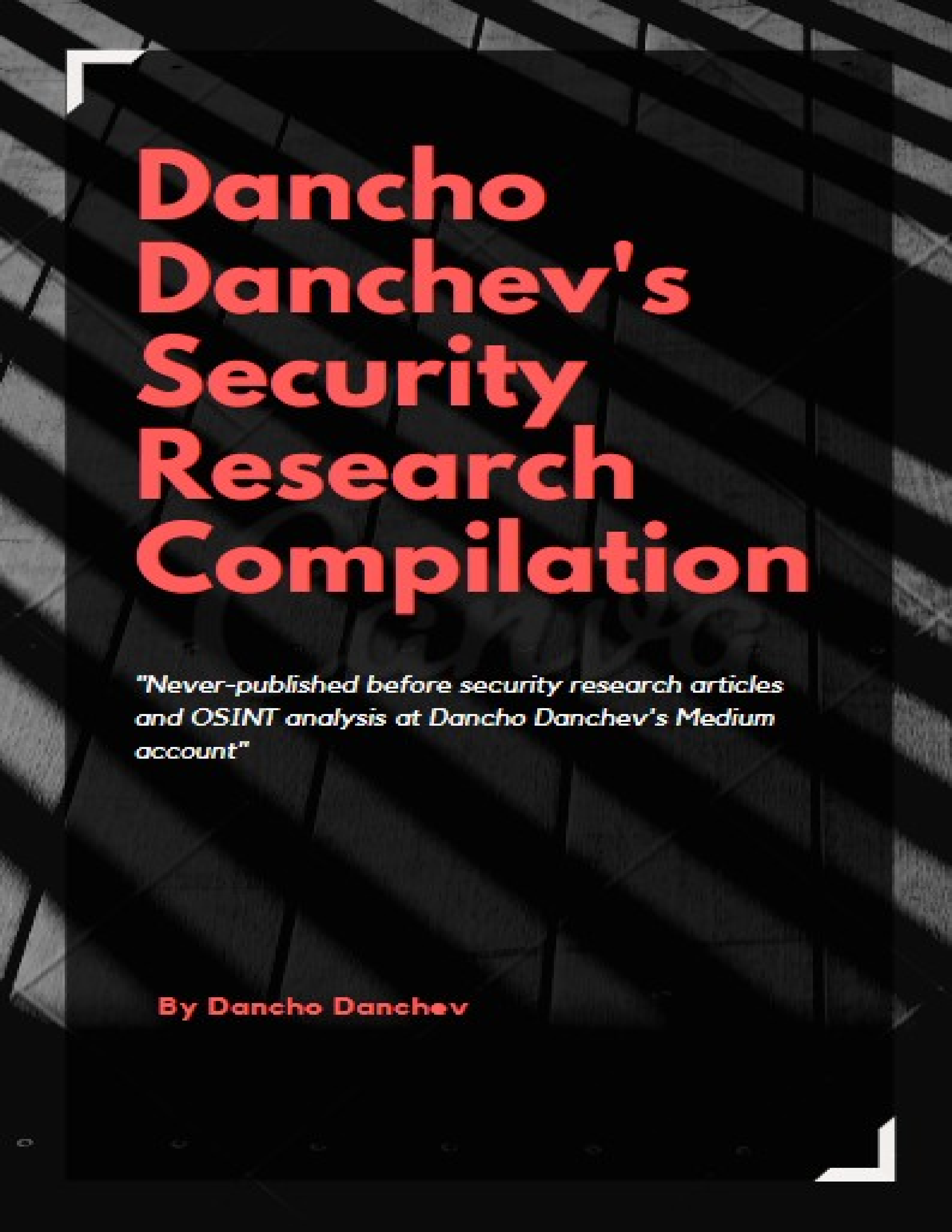

Dancho Danchev's Security Research Compilation

"Never-published before security research articles and OSINT analysis at Dancho Danchev's Medium account"

By Dancho Danchev

Article 1

Assessing U.S Military Cyber Operational Capabilities to Counter Pro-ISIS Internet Infrastructure

Dancho Danchev

Oct 20, 2019·8 min read

In a modern C4I-powered and Network-Centric Warfare-enabled digital battlefield the U.S fighting with the Chinese and the Russians for a “battle of the heart” including the overall disinformation including offensive clandestine and covert ops launched by Chinese and Russian Intelligence Agencies it should be noted that a both proactive and reactive Offensive and Defensive Cyber Warfare strategy on behalf of the U.S Government and U.S Intelligence Community should act as a prompt response for ensuring the global safety and prosperity of a vast network of computers known as the Internet further steaming National Growth and prosperity including Free Speech and major Innovation and Economic Growth boost Worldwide.

In this article I’ll discuss some of the currently active U.S Cyber Command including NSA Offensive and Defensive Cyber Warfare Initiatives through the prism of Anti-ISIS Join Task Force ARES including its practical execution and implementation in the face of Operation Glowing Symphony and offer in-depth discussion on some of the current Cyber Jihad and Cyber Terrorism recruitment and propaganda including active funding campaigns and tactics including actual URLs for currently active Pro-ISIS Cyber Jihad Forums and Community and the associated Network Reconnaissance Based Data.

It appears that the U.S government including the U.S Intelligence Community and U.S CYBERCOM have been busy launching and legally authorizing offensive cyber warfare actions and clandestine and covert operations against ISIS for the purposing of disrupting the Group’s access to Internet communications including the spreading of teaching recruitment and propaganda material through the execution of Operation Glowing Symphony which aims to to track down and shut-down Pro-ISIS online content including the active outreach to NATO-Member Allies whose infrastructure might have been abused in the process.

Based on publicly obtained classified documents courtesy of the U.S Government and the U.S Intelligence Community it appears that the U.S Government including U.S CYBERCOM managed to establish and actually executed a structured and systematic approach in the form of an offensive and clandestine Cyber Warfare operation against ISIS for the purpose of disrupting and undermining their access to Internet-based Communications.

In a campaign entitled Operation "Glowing Symphony" the U.S Military including the U.S Government which authorized the campaign with the help of U.S CYBERCOM appear to have established the foundations for a successful and systematic approach to counter Pro-ISIS online propaganda and recruitment efforts with the help of NATO-Allies through the "restoration of a supposedly claimed Cyberspace region" which inevitably prompted the use of Offensive Cyber Warfare force and actual prosecution of the individuals behind the ISIS-Group and actual recruitment and propaganda campaign.

A Proposed "Civilian Sector" Crowd-Sourced Approach and Methodology for Responding to and Reacting to Online Cyber Jihad and Cyber Terrorism Threats Propaganda and Recruitment Materials:

In the overwhelming sea of information it's becoming increasingly crucial to not only apply basic automated OSINT processing and enrichment methodologies but also actively introduce a manual based approach for tailored-based and a strategic and tactical based Technical Collection methodologies relying on public and proprietary tools for the purpose of collecting processing enriching and disseminating raw harvested and processed OSINT data for the purpose of presenting the bigger picture to a specific client or a general set of audiences.

In the section of the article I'll walk you through the process of Technical Collection gathering including the processing enriching and dissemination of actionable raw OSINT data for the purpose of presenting a big picture including the actual presentation of the data to a diverse set of audience and will also present a case study on the Current and Future State of the Cybercrime Ecosystem in the form of OSINT analysis.

Among the key concepts that should be taken into consideration in the initial Technical Collection phase includes active use of passive and active OSINT-based methodologies for the purpose of establishing the foundations for a successful Technical Collection program. Possible raw OSINT sources of information include the popular Pastebin.com including several of the most popular public search engines online including Google. Here are a few examples of active raw OSINT content that needs to be discovered acquired and disseminated including a possible enrichment which I manage to locate on Pastebin.com in terms of building an initial Technical Collection initiative on ISIS.

hxxps://pastebin.com/Xg5K3pt1 hxxps://pastebin.com/x9050k8h hxxps://pastebin.com/N9rPZ3Ar hxxps://pastebin.com/PS6RJEgP hxxps://pastebin.com/QuCGb0w3 hxxps://pastebin.com/2RHRgJwU hxxps://pastebin.com/3Hs3tBRe hxxps://pastebin.com/1dZWkDJs hxxps://pastebin.com/r9Tz7tC9 hxxps://pastebin.com/XxDtwzsa hxxps://pastebin.com/v4HFqddu hxxps://pastebin.com/jfF7yfT5 hxxps://pastebin.com/YBmEewMK hxxps://pastebin.com/DhcssPLn hxxps://pastebin.com/dZr780T0 hxxps://pastebin.com/bV49SzUL hxxps://pastebin.com/vYmW62eL hxxps://pastebin.com/cfeyKCTH

Sample Tools and Public OSINT Services that I'll discuss and use in this article including the associated Case Study include for the purpose of historical preservation of digital evidence namely the use of a basic Web Crawler to actually crawl and process a specific and newly launched Cyber Jihad and Cyberterrorism type of online community with the idea to historically and legally preserve a copy of the actual communication channel potentially reaching out to U.S Law Enforcement including the U.S Intelligence Community citing potential "new community discovery" and various other current and ongoing Cyber Threats posed by the Cyber Jihad and Cyberterrorism threats posed by the digitally preserved communication channel to be used for Historical OSINT purposes which is a basic Technical Collection principle that everyone that ever comes across to a newly discovered Cyber Jihad and Cyberterrorism type of Web site of community should take advantage of.

Web Crawler — hxxp://www.httrack.com/ Open Desktop Semantic Search — hxxps://www.opensemanticsearch.org Carrot2 — Open Source Search Results Clustering Engine — hxxps://project.carrot2.org/ Apache Solr Powered Local Yacy Search Engine — hxxps://yacy.net

hxxp://ahlamontada.com
hxxp://al-aqsa.org
hxxp://al-mustaqbal.net
hxxp://al-nahda.com
hxxp://al-rashedeen.info
hxxp://al-waie.org
hxxp://albadil.edaama.org
hxxp://albayanislamac.com
hxxp://albusyro.info
hxxp://albuxoriy.com
hxxp://alemara1.org
hxxp://alfajrtaqni.net
hxxp://alfidaa.biz/vb/
hxxp://alfurq4n.org
hxxp://alintibana.net
hxxp://almaqreze.net
hxxp://almobshrat.net
hxxp://almubarakradio.com
hxxp://alokab.com
hxxp://alqassam.ps
hxxp://alsomod-iea.info
hxxp://alsomod.com
hxxp://altarefe.com
hxxp://alweya.com
hxxp://an-najah.net
hxxp://anjemchoudary.co.uk
hxxp://ansar-alhaqq.net

hxxp://ansar.tv
hxxp://ansar1.info
hxxp://anti-majos.com
hxxp://arrahmah.com
hxxp://azzammedia.com
hxxp://azzammedia.net
hxxp://cageuk.org
hxxp://chechensinsyria.com
hxxp://cyberkov.com
hxxp://dakwahmedia.net
hxxp://darultavhid.com
hxxp://daulahisamiyah.net
hxxp://daulahislamiyyah.com
hxxp://dawaalhaq.com
hxxp://dawatehaq.net
hxxp://dhiqar.net
hxxp://dolatislam.blogspot.sg
hxxp://dr-algzouil.com
hxxp://eldorar.com
hxxp://elmanara.org
hxxp://enfalmedya.com
hxxp://faithfreedom.org
hxxp://fpi.or.id
hxxp://gimfmedia.com
hxxp://globalkhilafah.com
hxxp://gulf-up.com
hxxp://gurmad.info
hxxp://halabnews.com
hxxp://halifat.info
hxxp://heyetnet.org
hxxp://hizb-afghanistan.com
hxxp://hizb-america.org
hxxp://hizb-australia.org
hxxp://hizb-eastafrica.com
hxxp://hizb-pakistan.com
hxxp://hizb-russia.info
hxxp://hizb-turkiston.net

hxxp://hizb-turkiye.org
hxxp://hizb-ut-tahrir.dk
hxxp://hizb-ut-tahrir.info
hxxp://hizb-ut-tahrir.nl
hxxp://hizb-ut-tahrir.org
hxxp://hizb-ut-tahrir.se
hxxp://hizb-uzbekistan.info
hxxp://hizb.org.ua
hxxp://hizb.org.uk
hxxp://hizbut-tahrir.or.id
hxxp://hizbut-tahrir.org.my
hxxp://hizbuttahrir.org
hxxp://ht-afghanistan.org
hxxp://ht-bangladesh.info
hxxp://ht-tunisie.info
hxxp://htmedia.info
hxxp://invitetoislam.com
hxxp://invitetoislam.org
hxxp://isdarat.in
hxxp://isdarat.org
hxxp://isdarat.tv
hxxp://isecur1ty.com
hxxp://isis.zz.vc
hxxp://islaam.com
hxxp://islahhaber.net
hxxp://islam-iea.com
hxxp://islam-in-poland.org
hxxp://islamdaveti.com
hxxp://islamdin.com
hxxp://islamdin.net
hxxp://islamic-dw.com
hxxp://islamicstate.pro
hxxp://isnews.net
hxxp://issdaratj.appspot.com
hxxp://jabhtnosra.appspot.com
hxxp://jamatdawa.org
hxxp://jannatoshiqlari.net

hxxp://jehadway.7olm.org
hxxp://jhuf.net
hxxp://jihadica.com
hxxp://jihadmin.com
hxxp://joinalqarda.com
hxxp://kavkazcenter.com
hxxp://kavkazchat.com
hxxp://khabarpana.com
hxxp://khelafa.org
hxxp://khilafa.org
hxxp://khilafah.com
hxxp://khilafah.net
hxxp://liputan-kita.com
hxxp://maqrezeradio.net
hxxp://millatuibrahim.com
hxxp://mindspring.eu.com
hxxp://mnbr.info
hxxp://moqatel1.clod5.com
hxxp://muqawamah.net
hxxp://muvahhid.info
hxxp://opcharliehebdo.com
hxxp://qassam.ps
hxxp://radioalfurqaan.com
hxxp://radioandalus24.com
hxxp://radyotevhid.com
hxxp://salaf-us-saalih.com
hxxp://salafimediauk.com
hxxp://se-te.com
hxxp://shabakataljahad.com
hxxp://shahamat-arabic.com
hxxp://shahamat-english.com
hxxp://shahamat-farsi.com
hxxp://shahamat-movie.com
hxxp://shahamat-urdu.com
hxxp://shamikh1.info
hxxp://shoutussalam.org
hxxp://somalimemo.net

hxxp://soutalhaq.net
hxxp://sunnahonline.com
hxxp://suwaidan.com
hxxp://tajdeed.org.uk
hxxp://takvahaber.net
hxxp://tarani.info
hxxp://tawhed.ws
hxxp://tevhiddergisi.com
hxxp://tevhiddersleri.com
hxxp://tevhidigundem.com
hxxp://theshamnews.com
hxxp://toorabora.net
hxxp://turkhackteam.org
hxxp://turkiyevilayeti.org
hxxp://twelvershia.net
hxxp://uicforce.co.vu
hxxp://ummah.com
hxxp://ummetislam.info
hxxp://ummetislam.net
hxxp://uptotal.com
hxxp://vdagestan.com
hxxp://voa-islam.com
hxxp://wa3iarabi.com
hxxp://worldakhbar.com
hxxp://www.alokab.com hxxp://www.alsomod.com
hxxp://www.arrahmah.com hxxp://www.eramuslim.com
hxxp://www.expliciet.nl hxxp://www.hilafet.com
hxxp://www.islamdevleti.org hxxp://www.kalifaat.org
hxxp://www.khilafah.com hxxp://www.khilafah.net
hxxp://www.khilafah.org hxxp://www.khilafat.dk
hxxp://www.khilafat.org hxxp://www.kiblat.net
hxxp://www.kokludegisim.net hxxp://www.lasdipo.com
hxxp://www.lebensordnung.com hxxp://www.mykhilafah.com
hxxp://www.newcivilisation.com hxxp://www.ramadhan.org
hxxp://www.risala.org hxxp://www.sunnahcare.com
hxxp://www.waislama.net hxxp://zaidhamid.pk

What should be taken into consideration when obtaining access to and processing these communities would be raw OSINT data in terms of Email addresses and public IPs which could be used for possible attribution. The next logical step would be to ensure that a proper enrichment and colleration strategy is in place the eventual dissemination of the actionable intelligence to a variety of U.S Intelligence Community including international law enforcement agencies for the purpose of launching a possible track down and prosecution including various other clandestine and offensive cyber warfare including operational support type of activities.

hxxp://a3maqagency.wordpress.com
hxxp://abu-qatada.com
hxxp://abubaraa.co.uk
hxxp://abuicanimovic.blogspot.com
hxxp://abujibriel.com
hxxp://abuqatada.com
hxxp://abuqital1.wordpress.com
hxxp://al-busyro.org
hxxp://al-fidaa.com
hxxp://al-jahafal.com
hxxp://al-rashedeen.info
hxxp://albayan.co.uk
hxxp://albayanislamac.com
hxxp://albetaqa.com
hxxp://alboraq.info
hxxp://alfetn.com
hxxp://almaqdese.net
hxxp://almaqreze.net
hxxp://almubarakradio.com
hxxp://almuhajirun.net
hxxp://almuwahhidin.wordpress.com
hxxp://alokab.com
hxxp://alqassam.ps
hxxp://alquds.co.uk
hxxp://alsomod-iea.info
hxxp://alsunnah.info
hxxp://altarefe.com

hxxp://alweya.com
hxxp://anjemchoudary.co.uk
hxxp://ansa1.info
hxxp://ansar1.info
hxxp://anshoruttauhidwassunnahwaljihad.blogspot.com
hxxp://ar-royyan.com
hxxp://arrahmah.com
hxxp://as-ansar.com
hxxp://as-ansar.org
hxxp://at-tawbah.net
hxxp://azzamalqitall.wordpress.com
hxxp://azzammedia.com
hxxp://benmamun.wordpress.com
hxxp://cageprisoners.com
hxxp://chechensinsyria.com
hxxp://cyberkov.com
hxxp://dakwahwaljihad.wordpress.com
hxxp://daruhilafe.com
hxxp://darultavhid.com
hxxp://daulahislamiyah.net
hxxp://dawaalhaq.com
hxxp://dawla-is.cf
hxxp://diarysangterroris.blogspot.com
hxxp://dr-algzouli.com
hxxp://dr-mahmoud.com
hxxp://dwl-is.appspot.com
hxxp://eldorar.com
hxxp://fisyria.info
hxxp://fpi.or.id
hxxp://greenoptimus.blogspot.com
hxxp://halummu.wordpress.com
hxxp://hanein.info
hxxp://heyetnet.org
hxxp://invitetoislam.org
hxxp://iraqirabita.org.uk
hxxp://isdarat-tube.com
hxxp://isecur1ty.com

hxxp://ishobat.wordpress.com
hxxp://ishoomy.blogspot.com
hxxp://islamdaveti.com
hxxp://islamic-state.ga
hxxp://islamic-state.media
hxxp://islamicawakening.com
hxxp://islamicsupremecouncil.org
hxxp://islamqa.info
hxxp://jihad-sabiluna.blogspot.com
hxxp://jihadist-tuts.blogspot.com
hxxp://kafilahmujahid.blogspot.com
hxxp://kavkazcenter.com
hxxp://kavkazchat.com
hxxp://kavkazjihad.com
hxxp://khelafa.org
hxxp://khilafah.com
hxxp://kiblat.net
hxxp://majles.alukah.net
hxxp://maktoobblog.com
hxxp://manbar.me
hxxp://maqrezeradio.net
hxxp://millahibrahim.wordpress.com
hxxp://mo3sl3m.wordpress.com
hxxp://mtj.tw
hxxp://mujahiddin-islam.blogspot.com
hxxp://muslimdaily.net
hxxp://muslm.org
hxxp://muvahhid.info
hxxp://nepras.ps
hxxp://pecixputih.blogspot.com
hxxp://radioalfurqaan.com
hxxp://rumahjihad.blogspot.com
hxxp://shabakataljahad.com
hxxp://shahamat-arabic.com
hxxp://shahamat-farsi.com
hxxp://shahamat-urdu.com
hxxp://shamikh1.info

hxxp://sharia4indonesia.com
hxxp://soutalhaq.net
hxxp://suaraikhwanmuwahhid.blogspot.com
hxxp://sunnahonline.com
hxxp://suwaidan.com
hxxp://tajdeed.org.uk
hxxp://takvahaber.net
hxxp://tawhed.net
hxxp://tawhed.ws
hxxp://tevhiddersleri.com
hxxp://tevhididavet.com
hxxp://thoriquna.com
hxxp://thoriquna.wordpress.com
hxxp://uicforce.co.vu
hxxp://vdagestan.com
hxxp://voa-islam.com
hxxp://www.alfidaa.biz hxxp://www.alfidaa.info
hxxp://www.alfidaa.org hxxp://www.almaqreze.net
hxxp://www.chechensinsyria.com hxxp://www.dinhaqq.info
hxxp://www.dinhaqq.infosc hxxp://www.eldorar.com
hxxp://www.hanein.info hxxp://www.invitetoislam.org
hxxp://www.jarchive.net hxxp://www.mediaumat.com
hxxp://www.mhesne.com hxxp://www.muvahhid.info
hxxp://www.muwahhid.info hxxp://www.nokbah.com
hxxp://www.profetensummah.com hxxp://www.tawhed.ws
hxxp://www.tevhiddersleri.com hxxp://www.thoriquna.com
hxxp://www.thoriquwna.com hxxp://xalifati.wordpress.com
hxxp://yenidenislam.com
hxxp://zad-muslim.com

Prior to ensuring that a proper Technical Collection including a possible raw OSINT enrichment strategy is taking place a take-down and a possible Law Enforcement and U.S Intelligence Community outreach strategy should take place ensuring that the data is properly disseminated and properly attributed to a specific threat actor in this particular case the global Cyber Jihad community and ISIS in particular.

In terms of ISIS it should be noted that every then and now a commercial entity tries to actually monetize the ongoing Cyber Jihad and Cyberterrorism buzz with the idea to actually raise funds for an unknown set of cause most commonly funded and operated using basic marketing principles including the active creation and emergence of a popular brand in this particular case the commercial ISIS franchise. Is ISIS dangerous? It largely depends on what exactly is the group trying to achieve in terms of possible recruitment fund raising including active radicalization of online users for the purpose of spreading online Cyber Jihad and Cyberterrorism propaganda.

What should be worth pointing out in terms of ISIS is the fact that they actually managed to scale the brand in particular the introduction of franchise and multi-national and multi-lingual Network Based Asset Operators who further maintained and supported the ISIS campaign through the active production of propaganda material including the actual distribution and hosting of the propaganda material. It should be also noted that the very existence and creation of the ISIS brand directly intersects with the rise and popularity including growth of Social Media with tens of thousands of users who can actually support the brand through direct interaction with the group including the active sharing and distribution including actual hosting of Pro-ISIS based propaganda material for the purpose of enticing more users into participating in the campaign.

The actual modernization of what we commonly know as Cyber Jihad and Cyberterrorism online could be best described as a logical evolution of the active utilization of social media for the purpose of recruitment and the spread of online propaganda including actual recruitment and followers including actual supporters solicitation. This is where ISIS came into play for the purpose of positioning the group as the primary destination spot for Cyber Jihadists and Cyberterrorists online who might be interested in joining a “bigger cause” including the actual perhaps wrongly perceived approach of dominating a specific region of Cyberspace in terms of clustered conversation traffic generation and acquisition successfully positioning ISIS on the actual Offensive Cyber Warfare Map of U.S Government with the actual group aiming to claim a specific

Cyberspace region for Cyber Jihad and Cyber Terrorism purposes and rogue operations.

What could the U.S Government do in this particular case? Excluding the actual legal action which means directly approaching the U.S Intelligence Community including U.S CYBERCOM which is basically responsible for offensive and defensive Cyber Warfare operations including the NSA the U.S Government could easily issue an international warning for such type of groups with the idea to clearly demonstrate knowledge and true power of the Cyber Domain successfully claiming back and undermining the credibility of such type of campaigns.

Image courtesy of the National Security Archive .

Article 2

My Involvement in the Top Secret GCHQ “Lovely Horse” Program and the Existence of the Karma Police

Dancho Danchev

Oct 21, 2019·6 min read

Following a series of News Articles including publicly leaked information regarding the existence of a Top Secret GCHQ-sponsored program whose aim is to monitor public Twitter conversations of prominent hackers an Security Researchers including vendors and is a part of related legal surveillance and eavesdropping of various other Security Researchers and related Security Resources online including the actual owners of the Security Projects such as — HAPPY TRIGGER/Zool/TWO FACE eventually feeding data and information into another Top Secret Program known as the Karma Police including a possible involvement in what the U.S Intelligence Community is currently describing as “4th Party Exfiltration” or “outsourcing SIGINT” which basically describes a huge portion of today’s modern Security Industry in particular the Threat Intelligence market segment though the INTOLERANT program which basically aims to raise awareness on the process of raising awareness of new current and emerging Cyber Threats globally courtesy of the Security Industry.

I decided to post the following article detailing my involvement in the program using my old Twitter account — https://twitter.com/danchodanchev in particular the active legal measures taken to eavesdrop and put my account and Twitter activity under U.S Government surveillance next to a huge portion of my friends and colleagues at the time up to present day.

Want to find out how the GCHQ actually issues legal warrants and seeks legal authorization for people and communities of notice? Check out this document .

Sample Open-Source Modification of GCHQ’s Lovely Horse Open Source for Cyber Defense Program Referencing my Old Twitter

Account

It shouldn't be surprising that prior to vising the GCHQ back in 2008 with the help of the Honeynet Project I was pleasantly surprised to have made an important presentation on my way to properly secure the Internet's infrastructure from rogue and malicious actors successfully communicating my expertise experience and knowledge to a closed-group of knowledgeable people and Security People. It's been a decade following my disappearance and possible kidnapping attempt courtesy of local Bulgarian Law Enforcement with no clear clue as to what exactly happened at that time.

GCHQ's Top Secret "Lovely Horse" Program Twitter Account Participants Including My Old Twitter Account User ID @danchodanchev

Who was really involved in my kidnapping attempt ? Who really knew about it and who managed to actually track me down and find me? Long story short — I suspect a rogue operation courtesy of people that I know in an attempt to incriminate and undermine my reputation with an indirect help of people that I don't know that also includes high-profile cybercriminal take-down attempts — Koobface was my primary take-down and research priority at the time — including an active Hitman request for me posted on a high-profile cybercrime forum community worth $10,000 which appear to have successfully tracked me down while I was busy working in another town and successfully managed to kidnap and launch an discrimination and incrimination campaign including an attempt to damage my work and reputation which basically resulted in a major slow down of my research activities and actual working process with a high degree of probability that the campaign launched against me was Koobface and possibly Hillary Kneber-botnet related including a possible leak and potential OPSEC compromise in the context of working directly with a colleague — Xylitol including a possible search for me courtesy of an unknown set of individuals.

Sample Tweet Courtesy of Hilary Kneber — a Prominent Cybercrime-Friendly Enterprise Circa 2010

It should be worth pointing out that at the time I was also approached by a prominent U.S based company known as HBGary — and it seems that the actual communication made it to Wikileaks .

You can catch up with some of my latest research and analysis here .

Was I kidnapped and actually disappeared under the guidance of cybercriminals looking for ways to track me down and undermine my reputation and basically destroy and ruin my research activities or was I victim of a bigger operation courtesy of a foreign entity in this particular context a vendor or an organization who's not been so pleasantly and happy with some of my research? Back in the day the only campaign that I was actually busy monitoring and working on was the Koobface botnet in particular the active tracking down of one of its main operators including the actual take-down of the Koobface botnet courtesy of my active research at the time. Based on publicly obtained screenshots from the flagship Cybercrime Forum Community at the time — Darkode — I was able to portray a bigger picture in the context of having another researcher approach me at the time in this particular case Xylitol who offered direct access to the Darkode Cybercrime Forum Community which I basically used to take a peek for research purposes on a variety of occasions which at the time was parked on hxxp://81.27.98.152.

Sample Google Search Results For My Name Citing Possible Illegal Lawsuit Courtesy of Unknown Individuals

What really took place at the time? It appears that besides the usual "link love" courtesy of various cybercriminals whose activities I specialize in profiling — for instance the following C&C and client-side exploits serving URL circa 2010 — **hxxp://translate-google-cache.com/danchodanchev/load.php?spl=mdac&b=ie&o=xp&i=mdac** — 174.34.179.53 indirectly working with a variety of researchers and basically spending most of my time researching the Koobface botnet including an active campaign against Abuse.ch at the time including a prominent colleague of mine — Brian Krebs — following a series of typosquatted domains targeting him and a researcher colleague known as Xylitol including the active redirection of Facebook IP netspace to my personal blog the personal greeting referencing me and my personal https://ddanchev.blogspot.com including the active response to my "10 Things You Didn't Know About the Koobface Gang " article at the time within the actual C&C infrastructure of the botnet at the time a prominent "Top Ten Sexy InfoSec Geeks of 2009 " award including a prominent SCMagazine "Who to Follow on Twitter " award circa 2010. Did I somehow manage to attract the wrong attention through my research or did a become a prime target for the U.S Intelligence Community putting my old Twitter account — https://twitter.com/danchodanchev under legal surveillance? Long story short — I'd rather end up with having my name referenced in a major C&C infrastructure campaign courtesy of an unknown group rather than having most of my Intellectual Property (IP) and well-being robbed and stolen citing potential National Security issues courtesy of the U.S Intelligence Community.

The Scene the way we know it at the time was basically a variety of publicly accessible Hacking and Cyber Security Forum Communities including several other prominent invite-only fraud and illegal activity themed online communities to which I never really bothered obtaining access to citing potential OPSEC (Operational Security) violations and my passive OSINT processing methodology of cyber threats at the time

Sample Screenshots of Cybercrime Underground Forum Chatter Prior to my Disappearance circa 2010 Directly Referencing me and Commenting on my Disappearance:

Dancho Danchev Disappearance and Possible Kidnapping Attempt Circa 2010 — Cybercrime Underground Forum Chatter on the Actual Events that Took Place at the Time Dancho Danchev Disappearance and Possible Kidnapping Attempt Circa 2010 — Cybercrime Underground Forum Chatter on the Actual Events that Took Place at the Time Dancho Danchev Disappearance and Possible Kidnapping Attempt Circa 2010 — Cybercrime Underground Forum Chatter on the Actual Events that Took Place at the Time Dancho Danchev Disappearance and Possible Kidnapping Attempt Circa 2010 — Cybercrime Underground Forum Chatter on the Actual Events that Took Place at the Time

Go through a chronological order of the events including people that I know and used to work with at the time here .

In conclusion — I'm positive that I'll continue doing the research that I've been doing for over a decade now and that I'll continue publishing it at my extremely popular Security Blog with the idea to raise awareness on current and emerging Cyber Threats offer novel advice and new methodologies for processing and responding to current and emerging Cyber Threats and basically offer the big picture to thousands of loyal users across the globe including the necessary extra OPSEC (Operational Security) measures that I've recently implemented for the purpose of preserving my Intellectual Property and with the idea to continue conducting the type of research that everyone who's been reading my Security Blog since 2005 is familiar with.

Article 3

Kaspersky’s Antivirus Products the NSA and U.S National Security — An Analysis

Dancho Danchev

Oct 22, 2019·7 min read

Sample Presentation Slide from a Top Secret GCHQ Program Targeting Kaspersky Software

It has recently became evident that the U.S is further strengthening it’s position on the cyber warfare front by successfully tackling internal and external utilization of foreign products within it’s networks further banning the use of one of the World’s most popular antivirus solutions Kaspersky Antivirus on its networks in an attempt to ensure that proprietary and classified information remains properly protected and to ensure that the data doesn’t fall into the wrong hands by utilizing foreign antivirus solutions on proprietary and classified networks further “phoning back” potentially compromising proprietary and classified networks including data.

With Kaspersky’s cloud-based proprietary sand-boxing and data-aggregation platform it is becoming increasingly easier for proprietary and classified data to fall victim into the wrong hands potentially compromising OPSEC (Operational Security) including related intellectual property leaks leading to the exposure of proprietary and classified information. Despite the fact that users are given the option to opt-out it should become clearly evident that modern antivirus software cannot really prevent the usability and actual applicability offered by network-based IDS (Intrusion Detection Systems) including the active use of a properly secured and hardened end-point in particular a secured Web-browser through the prism of preventing possible data and information including identification leaks and the execution and actual exploitation of malicious code on the targeted host.

Sample list of Public Kaspersky Labs Netblock IPs:

hxxp://dnl-01.geo.kaspersky.com
hxxp://dnl-02.geo.kaspersky.com
hxxp://dnl-03.geo.kaspersky.com
hxxp://dnl-04.geo.kaspersky.com
hxxp://dnl-05.geo.kaspersky.com
hxxp://dnl-06.geo.kaspersky.com
hxxp://dnl-07.geo.kaspersky.com
hxxp://dnl-08.geo.kaspersky.com
hxxp://dnl-09.geo.kaspersky.com
hxxp://dnl-10.geo.kaspersky.com
hxxp://dnl-11.geo.kaspersky.com
hxxp://dnl-12.geo.kaspersky.com
hxxp://dnl-13.geo.kaspersky.com
hxxp://dnl-14.geo.kaspersky.com
hxxp://dnl-15.geo.kaspersky.com
hxxp://dnl-16.geo.kaspersky.com
hxxp://dnl-17.geo.kaspersky.com
hxxp://dnl-18.geo.kaspersky.com
hxxp://dnl-19.geo.kaspersky.com
hxxp://dnl-00.geo.kaspersky.com
hxxp://downloads0.kaspersky-labs.com
hxxp://downloads1.kaspersky-labs.com
hxxp://downloads2.kaspersky-labs.com
hxxp://downloads3.kaspersky-labs.com
hxxp://downloads4.kaspersky-labs.com
hxxp://downloads5.kaspersky-labs.com
hxxp://downloads6.kaspersky-labs.com
hxxp://downloads7.kaspersky-labs.com
hxxp://downloads8.kaspersky-labs.com
hxxp://downloads9.kaspersky-labs.com
hxxps://s00.upd.kaspersky.com
hxxps://s01.upd.kaspersky.com
hxxps://s02.upd.kaspersky.com
hxxps://s03.upd.kaspersky.com
hxxps://s04.upd.kaspersky.com
hxxps://s05.upd.kaspersky.com
hxxps://s06.upd.kaspersky.com
hxxps://s07.upd.kaspersky.com
hxxps://s08.upd.kaspersky.com
hxxps://s09.upd.kaspersky.com
hxxps://s10.upd.kaspersky.com
hxxps://s11.upd.kaspersky.com
hxxps://s12.upd.kaspersky.com
hxxps://s13.upd.kaspersky.com
hxxps://s14.upd.kaspersky.com
hxxps://s15.upd.kaspersky.com
hxxps://s16.upd.kaspersky.com
hxxps://s17.upd.kaspersky.com
hxxps://s18.upd.kaspersky.com
hxxps://s19.upd.kaspersky.com
hxxp://p00.upd.kaspersky.com
hxxp://p01.upd.kaspersky.com
hxxp://p02.upd.kaspersky.com
hxxp://p03.upd.kaspersky.com
hxxp://p04.upd.kaspersky.com
hxxp://p05.upd.kaspersky.com
hxxp://p06.upd.kaspersky.com
hxxp://p07.upd.kaspersky.com
hxxp://p08.upd.kaspersky.com
hxxp://p09.upd.kaspersky.com
hxxp://p10.upd.kaspersky.com
hxxp://p11.upd.kaspersky.com
hxxp://p12.upd.kaspersky.com
hxxp://p13.upd.kaspersky.com

hxxp://p14.upd.kaspersky.com hxxp://p15.upd.kaspersky.com
hxxp://p16.upd.kaspersky.com hxxp://p17.upd.kaspersky.com
hxxp://p18.upd.kaspersky.com hxxp://p19.upd.kaspersky.com
hxxp://downloads.kaspersky-labs.com
hxxps://downloads.upd.kaspersky.com hxxp://crl.kaspersky.com
hxxp://ocsp.kaspersky.com

It's been clearly noted that in the past the U.S Government is starting to express a very specific interest in the activities of Kaspersky Software in particular their presence of the software on U.S Government end-points citing potential cyber espionage and data-leaks. The ultimate question? Does the U.S Government really need a Russian-based including possibly internationally-based major anti-virus vendor solution residing on its end-points? It largely depends unless of course the person and organization responsibly for evaluating and implementing such type of solutions doesn't really fall victim into a possible "security through obscurity" example.

Sample Screenshot of SNORT IDS in action for Network-Based Intrusion Detection

How can this be achieved? There are several scenarios worth pointing out in terms of properly securing an end point in particular the introduction of anti-fingerprinting and off-the-shelf "stripped" browser whose primary purpose would be to prevent possibly data and information leaks including the identification and personal leaks courtesy of possible active and passive browser and online-identity fingerprinting campaigns and identification techniques which could not only compromise a host's OPSEC (Operational Security) but could also introduce possible malicious and fraudulent client-side execution flaws on the targeted host though the utilization of a popular and publicly accessible major Web browser release.

In should be noted that in the past the U.S Intelligence Community is known to have targeted Kaspersky including other anti-malware vendors though an active SIGINT campaign with the idea to "steal" and "bring back" a decent portion of new malware variants in a Top Secret Program known as "CAMBERDADA " which basically aims to eavesdrop on Kaspersky Infrastructure for the purpose of offering the U.S Intelligence Community a decent portion of malware-releases in terms of a possible “acquisition” of malicious software right from the source in this particular case Kaspersky Labs.

What can Kaspersky and other anti-virus vendors do in this particular case? It should be noted that basic network-based concepts such as perimeter defense at the network-infrastructure should be definitely taken into consideration including the active use of encrypted communication between an organization’s members including the use of basic Data Center encryption methodologies such as for instance basic Ethernet-based encryption which basically ensures that data-in-transit cannot really be decrypted for the purpose attributing the traffic to a particular event or Major Intelligence Program courtesy of the U.S Intelligence Community.

Sample Enthernet Data Center Site-to-Site Hardware appliance

You can find more information on possible Data Center and Traffic-Based Site-to-Site Encryption methodologies here — https://www.engageinc.com/Products2/BlackDoor.htm

Another possible methodology which could be implemented within any organization’s infrastructure for the purpose of ensuring that both external and internal communication channels remain properly protected from possible surveillance and eavesdropping attempts includes the use of basic traffic and communication obfuscation techniques which basically includes the use of “Whole Message Encryption” or basic PGP-Based Internal and External Communication Encryption strategy for the purpose of ensuring that an organization’s email communication work-flow remains properly protected from potential surveillance and eavesdropping attempts.

The overall reliance on foreign and custom-made Security Solutions can greatly contribute to a growing set of Cyber Espionage concerns in particular the leaking of classified and sensitive information to foreign entities without the actual knowledge of the user.

In a World dominated by a popular “security through obscurity” methodology where the Chinese and the Russians are actively attempting to compromise the Security of International organizations for the purpose of stealing and obtaining access to sensitive and classified “know-how” data information and knowledge it should be clearly noted that an important trend in the context of data mining and obtaining automated OSINT-based type of access to public U.S Government resources data information and knowledge for the purpose of stealing and actually piggybacking on on the actual "know-how" has been taking place for over a decade now in particular in a post 9/11 World. What exactly do I have in mind?

Basically what used to be once classified and sensitive research documents courtesy of the U.S Government and the U.S Intelligence Community in terms of offensive and defensive cyber warfare is today's modern Chinese and Russian Cyber Warfare doctrine with both countries including for instance Iran directly piggybacking on popular U.S Based research in the area of Offensive and Defensive Cyber Warfare Operations.

It should be also noted that a huge portion of today's modern advanced persistent threats in particular the active use of Remote access Tools (Rats) also known as DIY (do-it-yourself) Trojan Horses for the purpose of launching active Cyber Espionage campaigns can be best described as a re-surrection of a popular trend which used to take place during the 90's in this particular case the "lawful surveillance" and "lawful interception" of network-connected hosts through the use of publicly obtainable and easy-to-use Trojan Horse generating tools a tactic and a practice which throughout the 90's was largely used by Law Enforcement including hackers enthusiasts for the purpose of stealing confidential data or actually launching surveillance and eavesdropping campaigns against an unknown set of individuals for purely educational and research purposes.

Sample Screenshot of Spybot anti-telemetry Windows-based Solution in action

From the perspective of an Intelligence analyst — what every decent analyst should possibly consider is the use of "stripped" including hardened and secured devices including Workstations for the purpose of actively conducting research in a secure OPSEC (Operational Security) conscious environment which basically means a stripped OS (Operating System) including basic network-based perimeter defense mechanism such as for instance the use of Snot while running on the extremely popular PfSense hardware appliance.

Case in point is the recently released Emerging Threats Pro Telemetry Ruleset which basically prevents your host from “phoning back” to a pre-defined set of application-based C&C type of contact points which basically means it can get pretty difficult for an Intelligence agency or a competitor including a possible rogue or nation-state actor to actually launch passive or active infrastructure of network or host-based fingerprinting attack techniques.

What does this mean for Kaspersky an other Security Vendors looking for ways to protect their infrastructure from eavesdropping and possible surveillance attempts? Basically in a monocultural OS-dominated World it shouldn’t be surprising that vendors including Security Researchers often fall victims to basic OPSEC (Operational Security) mistakes which could possibly lead to a direct compromise of their research activities including the active stealing and use of their Intellectual Property (IP) for fraudulent or malicious purposes.

Sample U.S Government Supply Chain Management and Infiltration Cyber Espionage Risk Matrix

What the U.S can be better do to tackle the growing use including the active abuse of its Intellectual Property on a global scale through the systematic and persistent robbery courtesy of various rogue including nation-state actors looking for ways to obtain access to sensitive including classified information for commercial purposes? Pretty simple — it could definitely look to outsource some of its key National Security needs to the private sector in a possible private and government sector type of partnership. In terms of possible Supply Chain Management and Infiltration it should be clearly noted that basic precautions while travelling in the context of data-encryption at rest including basic OPSEC (Operational Security) principles while working and doing research should be definitely take into consideration for the purpose of preventing a wide-spread Intellectual Property theft including theft of “know-how” and technical experience while doing research.

Image courtesy of — The U.S-China Economic and Security Review Commission - “Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology ”.

Article 4

Assessment of U.S Intelligence Community Cyber Surveillance Programs and Tradecraft — Part One

Dancho Danchev

Oct 25, 2019·15 min read

Spooked by evil aliens? Did the Klingons did it again? Worry about your latest and very greatest porn collection leaking online? Thinking about your IP (Intellectual Property) as if it were U.S National Security? Want to find a meaningful way to contribute to a bigger cause — The U.S Intelligence community including your personal online privacy? Keep reading.

In this rather long analysis part of an upcoming set of Series on Current and Active U.S Intelligence Community Cyber Surveillance Programs I'll walk you though all the currently relevant U.S Intelligence Community Cyber Intelligence and Cyber Surveillance programs in non-alphabetical order with the idea to provoke a meaningful discussion on current tactics techniques and procedures courtesy of the U.S Intelligence community how you can protect yourself and most importantly how the U.S Intelligence community can "perform better" including practical software applications and services solution based recommendations for general users and organizations.

The data in this research has been obtained from Cryptome.org the Snowden archive and the Electrospaces.net research blog including the following archive .

The first program that I'll discuss in this analysis including the first part of the series includes "ABSOLINE EPILSON" which basically attempts to target iPhone users with client-side exploits including an active colleration of unique iPhone mobile device IDs for the purpose of infiltrating various internal and private networks for the purpose of exfiltrating private and personal data. I'll also offer practical advice and recommendations in terms of how to program really works how the U.S Intelligence Community can make it work better — for educational purposes only — including practical advice on how users can protect themselves from the CNO (Computer Network Operations) launched by the GCHQ.

The first part of these series of analysis will detail the workings of some of the most prolific U.S Intelligence Community and GCHQ Cyber Surveillance Programs including actual steps and practical recommendations on how end users and organizations can take proper measures to protect themselves from these widespread surveillance and eavesdropping Programs and techniques.

Program Name: ABSOLINE EPILSON — PDF — "*This paper describes standard analysis techniques that have been used to both discover iPhone target end point machines and implant target iPhones directly using the QUANTUM system. It shows that the iPhone Unique Device Identifier (UDID) can be used for target tracking and can be used to correlate with end point machines and target phone. It highlights the exploits currently available and the CNE process to enable further targeting.* "

Current status: The current status of the program is active in terms of possible collerations between iPhone user ID's including an end user's end point Internet user activities in terms of traffic and Web site cookie acquisition for the purpose of interception profiling and active monitoring potentially resulting in information and data including privacy-violations leak for a huge majority of iPhone users internationally unaware of the basic flaws exploited in this Top Secret GCHQ Program using an end user's iPhone as the "weakest link" to target their home-based or internal including private home-based end-point centric network.

Sample CVE Statistics for Apple's iTunes Software Throughout the Years

How exactly does the program work? With the iPhone continuing to occupy a large market share within the mobile device market segment — it shouldn't be surprising that malicious attackers will try to exploit both major iOS operating system flaws including the actual exploitation and use of iPhone-based client-side vulnerabilities potentially enticing a targeted user into interacting with rogue and potentially fraudulent and malicious Web site actually serving working and off-the-shelf client-side exploits to the targeted user for the purpose of compromising the confidentiality integrity and availability of the targeted device.

How it works: Every mobile has a unique ID? The problem? It tends to “phone back” to a manufacturers infrastructure and can be uniquely attributed to an end user including — possibly — to their end point potentially acting as the “weakest link” potentially exposing and end user’s end point Internet activities to the U.S Intelligence community. Prior to having a device “phone back” to a specific manufacturer’s infrastructure the data depending on the degree of OPSEC (Operational Security) applied — if any — can be easily eavesdropped on and put under active legal surveillance potentially compromising the actual confidentiality availability and integrity of the targeted mobile device including the end user’s home and internal network to a multi-tude of data-colleration attacks including active CNO (Computer Network Exploitation) campaigns and actual data leaks including high-profile privacy-violations.

How does the program actually work? Besides the general reliance on iPhone client-side vulnerabilities and exploits including the usual meta-data collection through the use of insecure and OPSEC-unware communication networks the program also attempts to exploit outdated and already patched iPhone including iTunes type of flaws and vulnerabilities in an attempt to trick users into falling victim into a possible social engineering type of fraudulent and malicious activity courtesy of the U.S Intelligence Community.

The digitally naughty part: Data colleration on a third-party device for the purpose of exposing the actual infrastructure behind the device including related end-points and related devices associated with the user in question — is nothing new. The digitally naughty part? It can be done — and the mobile device in question — an iPhone — in this particular case can be easily labeled as the “weakest link” in a possible corporate and end user private environment where it could result in the direct compromise of the actual internal infrastructure part of an ongoing legal eavesdropping and surveillance authorization campaign launched against a specific individual or an organization in question.

How you can make it work better: Shipping and delivery including supply chain infiltration tactics for the purpose of collerating unique mobile device IDs to a specific isn't new including possible "purchase-order-to-user-ID" colleration and data infiltration through basic social engineering and offensive CNO-based tactics. Potentially launching a targeted and geo-located phishing campaign on a per country city-basis could definitely lead to a positive results in terms of good old fashioned social engineering campaigns in terms of exfiltrating the necessary data including mobile device IDs including possible browser-based Web-based decoys for the purpose of further exposing an end user or an organization's private network and the necessary collerated end point devices.

Target application-isolation software and service solution providers and owners —What the GCHQ and the U.S Intelligence Community can definitely consider and actually implement on a short term and long-term basis is to launch a variety of malicious and fraudulent potentially disruptive type of attack campaigns which should be considered as as option for the purpose of ensuring that the project owner's time remains spend on fighting the malicious attacks including the eventual slowing down of the project development including the project's eventual shutdown. Possible portfolio of attacks might include online identity discrimination including spear phishing campaigns DDoS attack campaigns including possibly mail-flood attacks including possibly TDoS (Telephony Denial of Service attacks) against a variety of tailored and predefined project owner's contact points. Is this legal? It largely depends on who the U.S Intelligence Community and the GCHQ is targeting including the exact direct approach for the purpose of targeting the vendor or the project owner's individuals in question.

Develop an internal bug-bounty program for sand-boxing and application isolation software and service providers — It should be clearly noted that besides utilizing and using public sources crowd-sourcing the bug bounty through public and official channels including the possible outsourcing of the bug hunting process through third-parties while offering the necessary financial incentives might be the best approach to undermine the credibility of the project including the actual owner's credibility and reputation to maintain and operate the project. What exactly do I have in mind? Exploiting a popular flaw in a high market-share antivirus solution including a popular sand-boxing application such as for instance Sandboxie could greatly undermine the project's credibility in case the U.S Intelligence Community decides to launch a targeted and widespread malicious-software dropping and data exfiltration campaign.

Aim to wage disruptive warfare against private project owners — it's becoming increasingly evident that the U.S Intelligence Community including the GCHQ are attempting to launch a variety of discremination and impersonation including active and targeted DDoS (Denial of Service) attack campaigns including actual personalization of network assets for the purpose of disrupting the cyber operations of a huge number of project owners including hacktivist groups who might be interested in spreading data information and knowledge on current and emerging Cyber Threats including the actual launching of CNE (Computer Network Exploitation) attempts in the form of Web Site Defacements including related CNE type of campaigns online.

Randomly picking up a software owner — In the past it's been clearly evident that part of Top Secret U.S Intelligence Community and GCHQ Programs a random set of individuals could be easily targeted including the use of the Karma Police for the purpose of establishing a historical footprint in the context of an individual's or an organization's historical Web activities potentially triggering an alert to the current needs and requirements of the Top Secret U.S Intelligence and GCHQ Program in question. In need of a decent example on "on what really happened" is a good old fashioned Web site which I've been using and remember from the Scene for over a decade now — Matousec — which basically offers proactive and reactive Personal Firewall tests comparison and appears to have been recently targeted by an unknown set of individuals.

Sample Web Site Screenshot of the Matousec Web Site Including a Possible Mysterious Message Left Prior to the Web Site's Shutdown

Passively measuring and estimating product market-share for Targets of Opportunity — it's becoming increasingly evident in the past the U.S Intelligence Community and the GCHQ could easily attempt to measure the market share of a specific anti-virus and personal-firewall type of security solution using both public sources and SIGINT for the purpose of better launching individual or an organization based type of targeted CNE (Computer Network Exploitation) attack campaigns.

Sample Antivirus Products Market Share — 2018 — Courtesy of OPSWAT

How you can take measures to protect yourself: Consider obtaining one of the following "stripped" mobile devices in terms of hardened mobile OS offering in-depth and multi-layered security and privacy protection features for the purpose of bypassing wide-spread surveillance techniques and techniques. Ensuring that you possess a "stripped" mobile device is crucial for ensuring the necessary degree of personal privacy to stay ahead of current and emerging Cyber Threats including wide-spread privacy violations courtesy of the U.S Intelligence Community and various other nation-state and rogue actors including cybercriminals.

Sample Screenshot of a Highly Recommended Personal Firewall Net Firewall in Action Sample Recommended "Stripped" Commercial Mobile Device

Recommended "stripped" mobile devices to use potentially preventing widespread surveillance efforts including personal privacy violations:

https://necunos.com/ https://uhuru-mobile.com/ http://omprussia.ru/ https://secure-os.com/ https://www.encrypted-os.com/ https://copperhead.co/android/ https://www.confidentia.mc/phone/ https://www.darkmatter.ae/katim/katim-phone/ https://www.armadillophone.com/ https://securegroup.com/

Sample Recommended Nova Network Security Honeypot System in Action

The next logical step would be to ensure that the metadata on the device in terms of Web browsing including possible public and proprietary service use is properly obfuscated. Among the primary concerns whenever you choose to obfuscate a particular set of data would be possible supply-chain infiltration on behalf of the U.S Intelligence community in particular purchase orders that would further allow me to collerate and potentially identify a particular end user based on the actual supply-chain infiltration. One of the primary concerns in today's modern Internet world largely dominated by wide-spread surveillance courtesy of the U.S Intelligence Community including rogue and potentially malicious actors including nation-state and cybercriminals is the direct exposing of an individual's private network including possible collerated-based events that could potentially identify and track down a particular individual.

In terms of mobile device obfuscation the end user is largely advised to take advantage of personal firewall for the purpose of monitoring outgoing and incoming connections on the device in particularly blocking all-incoming connections and closely monitoring outgoing connections. Furthermore, what an end user can potentially do in terms of hardening their mobile device is to ensure that it does not leak back any internal IP addresses including possibly the device MAC address potentially exposing the device user's internal and private network potentially falling victim to "ABSOLINE EPILSON" type of end point and mobile device targeting type of attacks and campaigns courtesy of the U.S Intelligence Community including other rogue factors including nation-state actors and cybercriminals in general. How you should proceed in order to archive this process? Keep reading.

Next to the general use of "stripped" mobile devices end users should also consider the following highly recommended tactics techniques and procedures for the purpose of protecting their IP (Intellectual Property) including their mobile device and end point device's confidentiality availability and integrity:

WebCRT — Among the most common privacy-exposing scenarios in terms of "ABSOLINE EPILSON" remains the active utilization of unsecure browsing habits namely a misconfigured browser in terms or browser extension including the newly introduced "local IP exposing" WebCRT feature found in a variety of browsers. What should end users better do to protect their local IP including adding additional privacy and security features to their browser? Keep reading. The first thing a user should ensure from a network-based perspective is that their browser fingerprint remains as private as possible including the inability of the U.S Intelligence Community.

Sample WebRTC Local IP Exposing Online Test Results

Browser-Based Fingerprinting and Possible Information Leaks — In case an end user or an organization is interested in obfuscating their online presence it should be highly recommended that user takes basic precautions by installing the necessary browser-based privacy-enhancing addons and plugins for the purpose of ensuring that their Web-based activity can be easily obfuscated including the use of basic OPSEC (Operational Security) type of methodologies in this particular case the use of advanced and sophisticated VPN (Virtual Private Network) service provider. Case in point — would be active use of a “stripped” Web browser such as for instance — nDALANG — including Sphere — which basically operates in the user’s RAM further enhancing the individual’s and the organization’s Web-based privacy for the purpose of protecting the user from a variety of high-profile browser-flaw exploiting security flaws including the active reliance on high-profile privacy-preserving features making it harder for Web sites including the U.S Intelligence Community and the GCHQ to track you down and eventually attempt to profile your Web activities on a mass scale through the use of various current active Top Secret Programs.

Sample Screenshot of the nDALANG Privacy-Enhancing Browser’s Key Features

Personal Host Based Firewall — the first thing to look for in a personal firewall is a bi-directional firewall functionality allowing you to block all incoming traffic and successfully allowing you to allow all ongoing traffic based on a variety of rules including possible white-listing. The next logical step would be to implement basic ARP-spoofing prevention solution for the purpose of ensuring that your ISP including VPN provider cannot perform basic ARP-spoofing attack campaigns which could compromise the confidentiality of the targeted host and expose to it a multitude of network-based attack deception attack campaigns.

Sample Screenshot of XARP Anti-ARP Spoofing Free Tool

HIPS-based firewall — The next logical step would be to ensure that the end user including a specific organization in question remains properly secured and protected from a variety of both known and unknown threats through the use of host-based-intrusion-prevention solution which basically protects and ensures that the end user remains properly protected from a variety of unknown threats through the use of basic host-based hardening and security practices such as for instance Comodo's Personal Firewall which basically offers off-the-self HIPS-based host-based protection.

Sample Screenshot of Comodo HIPS in Action

Basic Network Deception — it should be fairly easy to assume that an end user or an organization could easily apply basic network-traffic and host deception mechanism in an attempt to detect and properly respond to including to disinform a potential attacker through the use of basic honeypot techniques applied on the targeted host.

Sample Screenshot of Canary Honeypot System

Privacy-Blocking online advertisements — The next logical step would be to ensure the use of an online advertisement blocking solution beyond the user's and organization's Web browser such as for instance the use of Pi-Hole which could be easily used to block a decent portion of third-party advertisement networks.

Sample Screenshot of Pi-Hole Online Advertisement Blocking Solution in Action

Custom-Based DNS-based DNSSEC-based servers with no logs policy — worry about the U.S Intelligence Community and your ISP eavesdropping on your traffic and Web browsing history potentially launching man-in-the-middle attacks? Consider utilizing basic free privacy-conscious DNS service provider with DNSSEC-enabled no-logs policy such as for instance — DNS Watch — which you can freely use without worry that your Web browsing history and DNS request history will be logged and potentially abused. A possible logical recommendation in the context of improving an end-point's in-depth security strategy might be the utilization of DNSCrypt which basically offers access to popular no-logs DNSSEC-enabled public and private DNS Servers for the purpose of ensuring that a user's including an organization's Web browsing activity remains hidden and properly protected from potential surveillance and eavesdropping attempts.

Sample DNSCrypt Public No-Logs DNSSEC-enabled Providers

Network-bases IDS (Intrusion Detection System) — it should be fairly easy to assume that the overall reliance on host-based end-point security solutions can be easily improved through the use of publicly obtainable Network-Based IDS (Intrusion Detection System) such as for instance Snort in combination with the use of a highly-popular and recommended host-based IDS and firewall solution such as for instance PfSense .

Sample Screenshot or SNORT IDS In Action

NordVPN — The next logical step would be to stay away from mainstream mobile devices citing potential Security and Privacy in mind including the use of a properly selected VPN service provider for the purpose of applying basic traffic obfuscation techniques including end-point network isolation in this particular context the end user and the organization should definitely look forward to implement a possible VPN provider actually "mixing" public legitimate jurisdiction-aware infrastructure with privacy-aware public or proprietary network technology — in this particular case VPN2Tor type of technology.

Windows-based users should definitely consider using and learning how to use the Advanced Tor Router application which basically offers a diverse set of unique privacy-enhancing and privacy-preserving featuring while utilizing the Tor Network further ensuring and offering a free solution for end users interested in preserving their Web browsing activities including possible network-wide Tor Network adoption on per OS and on per application-based basis. What does this application has to offer in terms of unique privacy-preserving features?

Basically it offers a variety of unique and never presented or discussed before type of Tor-Network and end-point privacy-enhancing or preserving features further ensuring that the end user will remain properly protected from sophisticated network-based and client-based type of attack campaigns potentially aiming to identify and expose their identity. What's worth emphasizing on in terms of the application is the unique set of privacy-preserving and oriented client-side feature in terms of possibly privacy-oriented and secure browsing experience.

Cryptohippie — Among the most popular and sophisticated vendors which I've been using for several years includes includes the Closed-Network Group offering courtesy of the Cryptohippie network which basically offers one of the most sophisticated privacy-conscious protection on the market in terms of privacy-enhancing technologies in the context of using a commercial VPN (Virtual Private Network) provider. What the provider basically does is to offer a pretty decent and sophisticated VPN type of commercial services whose featured perfectly match today's modern environment in terms of OPSEC (Operational Security).

Sample Managed and Corporate Closed-Network Communication Router Courtesy of Cryptohippie Inc.

In conclusion — stay tuned for an upcoming set of research analysis on some of the most prolific U.S Intelligence Community and GCHQ Cyber Intelligence and Cyber Surveillance type of programs — to be covered at my Medium account on a daily basis starting from today and continuing until a proper and structured response is offered to the majority of my readers in terms of some of the most prolific U.S Intelligence Community and GCHQ Cyber Surveillance currently in use on a large-scale basis today and how to protect against these type of Programs in terms of preserving your personal and your organization's Intellectual Property (IP) and technical "know-how" including the widespread prevention of large-scale and targeted cyber espionage campaigns and techniques.

Article 5

How the NSA utilized Iranian Cyber Proxies To Participate in the BOUNDLESS INFORMANT Program?

Dancho Danchev

Oct 27, 2019·4 min read

Sample Publicly Accessible Presentation Slide Showing the Actual IPs Known to have Participated in the BOUNDLESS INFORMANT Top Secret Program

Is there such a thing as free lunch? Think twice.

It appears that the NSA has been keeping itself busy utilizing rogue and fraudulent spread across various forum communities within Iran for the purpose of enticing Iranian-based users into using the rogue and often free VPN providers for the purpose of successfully eavesdropping on their communications in an attempt to feed the data into the BOUNDLESS INFORMANT Top Secret Data Collection Program including the active legal authorization to use various Top Secret Programs presumably targeting owners and individuals operating free and publicly accessible VPN providers in Iran including the active use of specially crafted and publicly accessible free VPN service providers for the purpose of enticing more users — in this case Iranian users into falling victim into the rogue VPN service provider offering with the idea to actively launch a legally authorized surveillance and eavesdropping campaign. How does this work? Keep reading.

Sample Rogue Free Iranian VPN Service Provider Which Appears to Have Participated in the Top Secret BOUNDLESS INFORMANT Program

Sample Rogue and potentially privacy-violating VPN-service providers known to have participated in the "BOUNDLESS INFORMANT" Top Secret Data Collection Program spread across various publicly accessible Iranian-based Web forums:

Vpn3.bluewebx.com
bluewebx.us
irs1.ga
iranianvpn.net
IRSV.ME
CISCO2.DNSSPEEDY.TK
ironvpn.tk
ironvpn.pw — Email: ironvpn@yahoo.com; Wegal@yahoo.fr
irgomake.win
make-account.us
make-account.ir
IRANTUNEL.COM
SSTP.JET-VPN.COM
accvpn1.newhost.ir — mokh98@gmail.com

Sample Facebook Post Detailing the Public Offering of a Free and Commercially Available VPN Service Targeting Iranian Users part of the Top Secret BOUNDLESS INFORMANT Program

Sample Responding IPs Based on Passive DNS Analysis of All the IPs Known to Have Participated in the Top Secret "BOUNDLESS INFORMANT" Program Acting as Rogue and Publicly Accessible VPN Service Providers:

hxxp://uk2.bluewebx.com
hxxp://hikemasat.dyndns.org
hxxp://sokrates.homeunix.net
hxxp://uk-server.vpnmakers.com
hxxp://uk.hidethisip.info
hxxp://uk.myfastport.com
hxxp://uk.vpnmakers.com
hxxp://ipsec.lon.witopia.net
hxxp://ipsec.london.witopia.net
hxxp://s17.worldserver.in
hxxp://ns1.dl.music30ty.net
hxxp://ns2.dl.music30ty.net
hxxp://ns3.music30ty.net
hxxp://ns4.music30ty.net
hxxp://dl.music30ty.net

hxxp://mrwan.dyndns.info
hxxp://mrwan.dyndns.info
hxxp://scatconnect.no-ip.biz
hxxp://revscape.no-ip.biz
hxxp://dibil.zapto.org
hxxp://windows.misconfused.org
hxxp://stats.uk-ln-002.privatetunnel.com
hxxp://us2.aseman-sky.in
hxxp://199–127–100–25.static.avestadns.com
hxxp://sucking.cc
hxxp://hadcoreporntube.com
hxxp://naughtyxxxtube.com
hxxp://erotixtubes.com
hxxp://www.sucking.cc hxxp://www.erotixtubes.com
hxxp://farzand.no-ip.org
hxxp://kaliou.dyndns.tv

Sample IPs known to have participated in the Top Secret "BOUNDLESS INFORMANT" Program:

146.185.26.163
176.249.28.104
212.118.232.104
212.118.232.184
212.118.232.50
31.6.17.94
37.130.229.100
37.130.229.101
37.220.10.28
80.84.63.242
84.45.121.218
85.237.211.177
85.237.211.198
85.237.212.52
94.229.78.58
184.154.95.24
198.105.215.147
198.144.105.223
198.144.107.244

198.144.107.45
199.127.100.25
216.172.135.105
216.172.135.136
37.72.168.84
50.115.118.140
50.115.119.172
64.9.146.208
65.49.68.162
68.68.107.164
68.68.108.69
69.175.29.74

Sample Screenshot of Iranian-Based Public and Free VPN Service Provider Known to Have Participated in the Top Secret BOUNDLESS INFORMANT Program

It should be clearly noted that in restrictive regimes such as for instance Iran the U.S Intelligence Community and the NSA might be interested in successfully tracking down potential hacktivists and their activities including possible “movements” activities for the purpose of launching legal authorization to eavesdrop and launch surveillance campaigns against the actual individuals including active traffic surveillance and basic eavesdropping techniques.

What can Iranian users to properly protect themselves from such type of attacks? Case in point is the use of foreign-managed sophisticated and market-relevant in today’s modern and sophisticated modern Internet where nation-state actors including various other rogue actors including the U.S Intelligence Community and the NSA actively try to launch wide-spread and mass surveillance and eavesdropping campaigns.

Sample Screenshot of Psiphon — A Popular Anti-Censorship Tool Which Could Be Used to Bypass Common Censorship Attempts and Could Actually Offer More Privacy and Security Compared to a Free VPN Service Providwer

Sample highly recommended tools or the purpose of bypassing common and rogue potentially fraudulent free VPN Service Providers include:

Psiphon — https://psiphon.ca

In conclusion — it should be clearly noted that the U.S Intelligence Community including the NSA and its partners will continue to successfully attempt to launch wide-spread surveillance and eavesdropping campaigns potentially targeting the actual project and product owners in the process including the actual users of the free VPN services in question.

What end users and organizations could possible do is to stay on the top of current and emerging cyber threats for the purpose of preserving their Intellectual Property (IP) including to protect their organization’s confidentiality availability and integrity through maintaining a decent situational awareness on current and emerging cyber threats.

Article 6

Exposing GCHQ’s Top Secret “GORDIAN KNOT” Cyber Defense Sensor Program — An Analysis

Dancho Danchev

Oct 28, 2019·9 min read

Sample Publicly Obtainable Top Secret “GORDIAN KNOT” Presentation Slide

In a previous post on Medium entitled “Assessment of U.S Intelligence Community Cyber Surveillance Programs and Tradecraft — Part One ” I offered practical security tips and actual advice for the purpose of setting up the foundations for an upcoming set of posts detailing some of the most prolific U.S Intelligence Community Cyber Surveillance Programs and how you can protect yourself from wide-spread surveillance and eavesdropping attempts including practical advice on how the U.S Intelligence Community can actually make them work better.

In this post I’ll discuss in-depth GCHQ’s “GORDIAN KNOT ” Top Secret Sensor for Cyber Defense Program which largely relies on Information Assurance Sensor development network including the “HARUSPEX ” Top Secret Program which collects malicious software based on specific signatures targeting U.K-based infrastructure in the context of malicious software and phishing including spam campaigns with the help of data and E-mail attack signatures produced to be utilized by MessageLabs E-mail monitoring infrastructure acting as a Sensor Network successfully protecting U.K based Email infrastructure including several other currently active Top Secret U.S Intelligence Community Programs actively collecting malicious software and collerating data using SIGINT for possible malicious cyber adversary attribution.

Sample Screenshot of MessageLabs Email Attack Signatures Configuration Interface

Program Name: “ GORDIAN KNOT” — The program is among the U.S Intelligence Community’s active malware spam and phishing emails collecting Sensor Networks which in combination with the "HARUSPEX" Top Secret Program aims to build the foundations for a successful Technical Collection of malicious software spam and phishing emails for the purpose of using active legal surveillance authorization measures including SIGINT for the purpose of establishing a successful cyber adversary attribution program efforts. How exactly does this work? Keep reading.

Current Status: This is a currently Top Secret U.S Intelligence Community Program aiming to collect malicious software spam and phishing emails for active Cyber Defense including the use of legal surveillance authorization measures for the purpose of using SIGINT for possible cyber adversary and attack attribution.

How it works: The program relies on both proprietary classified and public including commercial sensor networks used by the U.S Intelligence Community for Cyber Defense purposes including possibly cyber adversary attack attribution including the active use of U.K infrastructure implementations of MessageLabs Cloud-Based Security Solutions for the purpose of intercepting and responding to malicious software spam and phishing attack campaigns using active legal surveillance authorization measures including the use of SIGINT for possible cyber adversary attack attribution.

The targeted population? Pretty much everyone using MessageLabs Cloud Based Email Security Solution including various U.K Government bodies through a possible legal authorization to actually eavesdrop and put the E-mail traffic under active surveillance for the purpose of using SIGINT for possible attack attribution further protecting U.K based infrastructure.

Long story short — whenever a malicious attack reaches to any of the monitored users the U.S Intelligence Community and the GCHQ will feed the attack data using a specifically crafted set of E-mail signatures back to their "HARUSPEX" Top Secret program for the purpose of using SIGINT for attribution purposes.

How does the process actually work? It's fairly simple that once an attack is launched U.K based infrastructure and the attack falls victim into the E-signatures database developed by the GCHQ for the purpose of enhancing Cyber Defense through intercepting and feeding back into related SIGINT-based programs various malware-serving and phishing email campaigns for the purpose of using SIGINT for attribution purposes.

The digitally naughty part: Based on various legal surveillance authorization mechanisms the U.S Intelligence Community and the GCHQ can easily achieved a what can be best described a fully working public and private sector Monitoring Sensor for anticipating to and responding to malicious software phishing and spam campaigns with the U.S Intelligence Community and the GCHQ actively relying on SIGINT for cyber adversary and attack attribution in combination with MessageLabs relevant API-based data synchronization and export functionality which could possibly offer relevant colleration type of malicious data enrichment and processing for the purpose of using SIGINT for cyber adversary and cyber attack attribution purposes.

How you can make it work better: Long story short — taking under consideration that U.K based infrastructure is under the jurisdiction of U.K's GCHQ in terms of SIGINT and possible Information Assurance and Cyber Defense initiatives — it should be fairly easy to assume that based on a legal authorization surveillance and eavesdropping initiative the GCHQ can basically and practically monitor and respond to basically all the cyber attack incidents affecting U.K based infrastructure while possibly using SIGINT for active and passive cyber attack and cyber adversary attack attribution. Actively relying on public private sector API-based data-warehouse data information and knowledge including hundreds of thousands of active and potentially fraudulent and malicious IoCs (Indicators of Compromise) the GCHQ can be perfectly positioned to take advantage of U.K's vast Internet infrastructure and actually utilize it as a mainstream U.S Intelligence Community type of Sensor Network for Early Warning Systems including active Cyber Defense purposes.

Sample Screenshot of MessageLabs Email Security Cloud Based Solution Anti-Email Spoofing Mechanism in Action

How you can take measures to protect yourself: In case you're a major U.K based infrastructure provide or a private organization including a company that basically wants to preserve the confidentiality availability and integrity of its communication — it should be fairly easy to assume that basic “enforced encryption” type of communication both internally and externally should be taken into consideration including possibly the use of DKIM (Domain Keys Identified Email) for the purpose of establishing a decent degree of “security through obscurity” type of mentality including basic OPSEC (Operational Security) in terms of ensuring that basic email impersonation or email spoofing type of campaigns cannot really reach the targeted organization or an individual in question through basic implementation of various MessageLabs “security through obscurity” practices and mechanisms.

How does the attribution actually work? Pretty simple. Based on the publicly obtainable data from the “GORDIAN KNOT” and the “HARUSPEX ” Top Secret Cyber Sensor for Cyber Defense Programs the U.S Intelligence Community including the GCHQ is capable of collerating the obtained data from the original malicious software serving including phishing campaign to a particular individual or a set of individuals through the active use of SIGINT which means that the U.S Intelligence Community including the GCHQ can launch offensive including active legal measures in terms of surveillance and eavesdropping authorization for the purpose of establishing the true identity behind a particular malware-serving including phishing campaign including actual legal action next to the active hijacking or a specific set of malicious and fraudulent botnet that managed to targeted U.K based infrastructure.

Same Screenshot of a Publicly Accessible Top Secret U.S Intelligence Community Presentation Slide Discussion Public and Commercial Sensors for Cyber Defense

Among the next logical example would be to go through Lockheed Martin’s publicly accessible OSINT Fusion Project presentation slides which also details similar offensive and defensive SIGINT use for actual cyber adversary attribution through the reliance on public and private Internet-based Cyber Security Events Sensors. The research published within Lockheed Martin’s OSINT Fusion Project presentation slides is pretty similar to what I’ve been doing for over a decade now — namely raising awareness on current and emerging cyber threats through the direct publication of research material on my personal Security Blog using basic Technical Collection methodologies including a personally developed OSINT methodology in terms of attribution and actual discovery of current and emerging cyber threats globally.

Sample Publicly Obtainable Screenshot of a Top Secret U.S Intelligence Community Botnet Hijacking Program Known as QUANTUMTHEORY

Yet another currently active Top Secret U.S Intelligence Community Program whose purpose is to hijack and disrupt various currently active botnets including basic C&C (command and control) infrastructure courtesy of the U.S Intelligence Community is "QUANTUMTHEORY " which basically allows a U.S Intelligence Community offensive and defensive CNO (Computer Network Operation) Operator the ability to hijack and track down any currently active botnet which in combination with other Top Secret U.S Intelligence Community Programs can greatly result in the actual cyber adversary attribution of a specific malicious and fraudulent actor through the use of legally authorized and active basic SIGINT operations.

Sample Screenshot of a Publicly Obtainable Presentation Slide Detailing How the X-KEYSCORE System Could be Used to Track Down Conficker-Based Malware Infections

It should be also worth pointing out that the U.S Intelligence Community is also known to be actively utilizing the X-KEYSCORE system for active and passive SIGINT in terms of cyber attack adversary attribution including the active use of software and digital attack fingerprints and signatures developed exclusively to be used by the U.S Intelligence Community and X-KEYSCORE Top Secret Program users.

Sample Screenshot from a publicly accessible Top Secret Program Known as X-KEYSCORE Actively Looking for BackEnergy DDoS Attack Tool Including the Mujahideen Secrets 2 Encryption Tool

It appears that the same system has been also used to detect possible Mujahideen Secrets 2 type of network-based activity for the purpose of covering possible attribution a release which I originally covered in a research posted in 2007 including another analysis posted in 2008 at my extremely popular Security Blog .

Same Screenshot of a Publicly Obtained Top Secret EONBLUE Presentation Slide Detailing the Use of Sensor Networks for Cyber Defense

Yet another program including a possible Top Secret Program use of SIGINT for cyber attack attribution is the EONBLUE Program which relies on “deep packet inspection” using signatures for detection known and already profiled threats including possible network-based anomalies — an area where I’ve offered extensive technical background throughout the years at my extremely popular Security Blog successfully anticipating and proactively detailing the malicious and fraudulent activities of cybercriminals and nation-state actors.

Sample Publicly Obtainable Presentation Slide Discussing the Top Secret X-KEYSCORE Program Use and Reliance on Malware-Detecting Fingerprints

What the U.S Intelligence Community further attempt to do in an attempt to improve the overall utilization and use of passive and active OSINT for cyber adversary type of attribution including the combination of SIGINT part of some of the Top Secret anti-malware and anti-botnet type of Programs that I’ve discussed — is to rely on public and commercial sources further enhancing the use of OSINT for Cyber Defense including the reliance on SIGINT in terms of cyber adversary attribution.

Do you want to find out more about successful active and passive SIGINT cyber operations courtesy of some of the research that I conducted during the years and published at my extremely popular Security Blog ? Keep reading. On the majority of occasions I’ve managed to archive a decent degree of active communication between the actual campaign owners and malicious botnet operations who personally greeted me or used my name and personal blog as a reference within their C&C (command and control) infrastructure including for their actual domain registration purposes next to the active redirection of Facebook's entire IP space to my personal blog courtesy of the Koobface botnet circa 2009.

Case in point are the following cases where I've successfully managed to establish a direct connection between the botnet operations who successfully reached back and left messages referencing me and my research including active typosquatting of my name some of the actual domain registrations including the active redirection of one of the malicious domains involved in the U.S Treasury Department circa 2010 to my personal Blogger profile.

hxxp://mikkohypponen-suc.kz — is known to have been registered using my name — Danch Danchev
hxxp://seximalinki.ru/images/ddanchev-sock-my-dick.php
hxxp://seo.hostia .ru/ddanchev-sock-my-dick.php
hxxp://hidancho.mine .nu/login.js

In conclusion it should be clearly noted that the U.S Intelligence Community is perfectly positioned to track down disrupt and undermine a huge portion of today's modern trend including the active use of SIGINT for cyber attack and cyber adversary attribution. With the currently ongoing commercialization of what was once best known as Technical Collection — today's modern Threat Intelligence market segment — it shouldn't be surprising that the U.S Government including the U.S Intelligence Community is actively taking measures to keep track of and potentially undermine various cyber threats online including the active use of botnets and various other nation-state or rogue actors through the reliance on SIGINT for cyber attack and cyber adversary attribution.

Article 7

Exposing GCHQ's URL-Shortening Service and Its Involvement in Iran's 2009 Election Protests

Dancho Danchev

Nov 24, 2019·4 min read

In 2009 Iranian citizens participated in a widespread Election Protest online and it appears that the GCHQ's primary mission at the time was to launch a custom-made URL shortening service labeled — hxxp:// lurl.me part of the DEADPOOL Top Secret Surveillance and Eavesdropping Program part of GCHQ's Joint Threat Research Intelligence Group (JTRIG) department which is heavily involved in offensive and defensive cyber warfare online tactics including actual "dirty tricks" aiming to shut down or discredit a particular online organization or an individual and is pretty similar to what I've managed to successfully achieve throughout the years in terms of establishing the foundations for my own OSINT methodology which leads me to the publication of hundreds of high-qualily and never-published before OSINT cybercrime research and threat intelligence type of analysis at my personal blog including the following commercial portfolio of cybercrime and threat intelligence gathering including cyber warfare type of services .

Sample Currently Active Twitter Accounts Known to have Participated in the DEADPOOL Top Secret GCHQ Surveillance and Eavesdropping Program:

https://twitter.com/2009iranfree https://twitter.com/MagdyBasha123 https://twitter.com/TheLorelie https://twitter.com/Jim_Harper https://twitter.com/angelocerantola https://twitter.com/recognizedesign https://twitter.com/akhormani https://twitter.com/FNZZ https://twitter.com/GlenBuchholz https://twitter.com/enricolabriola https://twitter.com/katriord https://twitter.com/ShahkAm147 https://twitter.com/Pezhman09 https://twitter.com/jimsharr https://twitter.com/blackhatcode

The main purpose behind the use of this URL shortening service is to actually gather evidence that could be used to collerate and launch active CNO (Computer Network Operations) type of offensive or defensive cyber attack campaigns including actual Identification Targets identification for the purpose of feeding back the data through various other Top Secret GCHQ-themed Programs which appear to have been actually used by the GCHQ to track down and prosecute a LulzSec member and might have managed to intercept and actually trick a huge number of users into interacting with the rogue URL shortening service.

What users should keep in mind when using some of the most popular URL shortening services is to actually aim to prevent the leak of metadata and actual personally identifiable information which could be obtained from analyzing and processing the actual URL shortening service link statistics which on the majority of ocassions are publicly accessible. Yet another possible metadata obfuscation techniques which could be used to prevent such type of leaks includes hardware isolation including the use of an IDS (Intrusion Detection System) such as for instance Snort and the use of an advanced VPN (Virtual Private Network) type of service such as for instance Cryptohippie .

In terms of GCHQ's Joint Threat Research Intelligence Group (JTRIG) what the Unit basically does is pretty similar to what I've managed to achieve in my personal Security Lab throughout 2008–2013 for the purpose of fighting and responding to a growing set of cybercrime attack campaigns including never-published before type of threat intelligence type of research analysis in terms of offensive and defensive Cyber Assets and Virtual SIGINT type of cyber attack profiling and responding to a growing set of current and emerging cyber threats successfully positioning me and my research as a primary competitor back then now a proud member and partner of the U.S Intelligence Community as a "4th Party Exfiltration" partner basically representing the process of "outsourcing SIGINT".

Case in point is the Koobface botnet which basically represents a case study in "outsourcing SIGINT" including an actual Virtual SIGINT Journeyman perspective in terms of monitoring tracking down and eventually shutting down the actual botnet by exposing some of the primary botnet masters behind it.

The use of the rogue and potentially privacy and security compromising hxxp:// lurl.me URL shortening service courtesy of the GCHQ is similar to the NSA's use of Iranian Cyber Proxies to participate in the BOUNDLESS INFORMANT Top Secret Program and it should be highly recommended that end users including organizations take basic network and security precautions to stay safe and secure online.

Article 8

Introduction to Unit-123.org — The Primary Destination Spot for Intelligence Deliverables

Dancho Danchev

Dec 20, 2019·4 min read

It's been a while since I've last managed to properly launch a high-profile security or mainstream hacking and threat intelligence project following my disappearance back in 2010 and the most recently crowd-sourced OSINT Intelligence and Law Enforcement Operation "Uncle George " and I've decided to elaborate more on my most recently launched Security and Threat Intelligence type of project dubbed "Unit-123.org " — the World's Leading Cyber Threat Intelligence Products Portal with the idea to raise awareness behind the existence of the project and to elaborate more on what appears to have successfully matured into my day job — to produce share and disseminate high-quality and never-published before possibly sensitive and classified Intelligence Deliverables.

Sample Screenshot of Dancho Danchev's Most Recently Launched E-shop for Classified and Sensitive Intelligence Deliverables

What exactly is Unit-123.org ? The primary purpose behind the actual launch of the project is to properly reach out to the Security Industry including friends and colleagues including the U.S Intelligence Community through the proper distribution of personally-produced finished Intelligence Deliverable type of products OSINT research analysis malicious software research and analysis and actual OSINT artifacts including never-published before and released type of threat intelligence type of analysis to the general public.

Among the Key Categories of Intelligence Deliverables currently available as a Direct Download include:

Cyber Jihad Artifacts — which currently includes an actual copy of the **Mujahedeen Secrets Encryption Tool** and intends to cover various OSINT based type of Cyber Jihad and Cyber Terrorism type of research analysis findings which I've managed to collect or have actually processed and analyzed throughout the years.

Sample Screenshot of a Cybercrime-Friendly Affiliate-Based Network Featured in Unit-123.org's Official Cybercrime-Friendly Services Flash Advertisements Collection

Cybercrime Artifacts — which currently includes a never-published before type of Cybercrime Services type of Flash Advertisements Collection including a video demonstration of NASA's Phoenix Mars Mission Web Site Defacement including video demonstration of the cybercrime-friendly hxxp://5socks.net service including a video demonstration of a working DDoS attack against the popular h4cky0u.org cybercrime-friendly community including a video demonstration of the Poison Ivy RAT (Remote Access Tool) in action.

Sample Screenshot of the Cybercrime-Friendly h4cky0u.org Cybercrime Forum Community Currently Available as a Direct Download at Unit-123.org — The World's Leading Cyber Intelligence Products Portal

Cybercrime Forum Data Sets — which currently includes direct download access to the 2019 Cybercrime Forum Data Set including direct download access for the following Cybercrime Forum Communities — hxxp://aljyyosh.com which is an Arabic Cybercrime Forum Community including Darkcode , Ghostmarket , Carderplanet , ShadowCrew , Opensc.ws , Pay-Per-Install.org Malicious Software Artifacts — which currently includes access to malicious software RATs (Remote Access Tools) trojan horses malware crypters and binders including the actual source code and is targeting primarily Academic Institutions seeking to obtain access to such type of content for research analysis — Part 01 , Part 02 , Part 03 , Part 04 , Part 05 , Part 06 , Part 07 , Part 08

Sample Screenshot of Unit-123.org's — The World's Leading Cyber Intelligence Products Provider Video Compilation of Ashiyane Digital Security Team's Behrooz Kamalian

OSINT Artifacts — which currently includes and offers never-published before enriched OSINT analysis of Iran's primary hacking

groups including the Ashiyane Digital Security Team and in-depth analysis on some of the key members behind the group.
OSINT Products — which currently includes an in-depth analysis of **BakaSoftware** and **Anonymous Bulgaria** .
Technical Collection — which currently includes Technical Collection type of artifacts whose purpose is to ensure that an Intelligence Analyst is properly equipped with the necessary technical "know-how" to properly analyze process and enrich a vast majority of commercially and publicly available Cybercrime Forum and Cybercrime-friendly Data Sets online.

The project also aims to properly inform an educate a new generation of Cyber Threat Intelligence and OSINT Analysts through the daily publication of high-quality and never-published before type of content which currently includes:

France to Wage Offensive Cyber Warfare — Brace Yourselves! UAE — Where Money Pays — Do You Want to be a Cyber Warrior? Oops, White House National Cyberspace Strategy Acknowledges Information Warfare Operations Proactively Digging in the U.S Cyber Warfare Realm — And How You Can Perform Better? DoD's Cyber Strategy — 2018 — Shall We Play a Cyber-Retaliation Game? Exploring the Basics of Cyber Assets and Cyber Inventory Efforts Build-up — A Proposed Off-the-Shelf Methodology

It should be also worth pointing out that based on the growing threat of cybercriminals internationally I intend to post a variety of high-quality and never-published before finished Intelligence Deliverables and OSINT artifacts on Unit-123.org on a daily basis with the idea to empower a new generation of Cyber Warriors Intelligence Analysts and OSINT Analysts.

Article 9

FBI Most Wanted Cybercriminals — OSINT Checklist — An Analysis

Dancho Danchev

Dec 21, 2019·2 min read

I've been recently spending more time going through **FBI's Most Wanted Cybercriminals** Checklist and I've decided to elaborate more potentially reaching out to friends and colleagues including the Security Industry and Law Enforcement in an attempt to share and communicate valuable and recently produced OSINT analysis detailing the activities of several high profile Cybercriminals found on the FBI Most Wanted Cybercriminals Checklist including to provide actionable intelligence and personally identifiable information on some of the key cybercriminals and cybercrime groups listed in the FBI's Most Wanted Cybercriminals Checklist.

Sample Maltego Social Network Analysis Graph Covering ITSec Team and the Mershad Co. Company Currently Wanted for Prosecution by the FBI's Most Wanted Cybercriminals Checklist

Some of the key Cybercriminals and associated Groups which I've managed to profile and expose currently include:

The Syrian Electronic Army

The **Innovative Marketing** Scareware Affiliate-Network-based Franchise
Evgeniy Mikhaylovich Bogachev — a prominent member of the "Jabber ZeuS" Gang

Sample Personal Photo of Evgeniy Mikhaylovich Bogachev known to have participated in the "Jabber ZeuS" Malware Gang

Several high-profile **Iranian Cybercriminals** including actionable intelligence on ITSec Team and the Mersad Co. company which appear to have been most recently mentioned in the "**Cyber Deterrence and Response Act of 2019** "

Sample Personally Identifiable Photo Courtesy of Iran’s ITSec Team Group Member

I wanted to let everyone know that I’ll be soon posting an updated set of personally identifiable information including actionable intelligence on some of FBI’s Most Wanted Cybercriminals with the idea to assist the Security Industry an Law Enforcement in the process of tracking down and eventually prosecuting the individual behind these campaigns and malicious attacks.

Article 10

Astalavista.com — The Scene the Way We Know it — My Experience in Running the Portal

Dancho Danchev

Dec 22, 2019·5 min read

Official Astalavista.com — Astalavista Security Group Logo — Circa 2004

It’s been approximately 12 years since I’ve last touched based with Team Astalavista which basically represents Astalavista.com — The Underground or the World’s Most Popular Information Security Portal which I used to run for the position of Managing Director throughout 2003–2006 and managed to produce a high-volume high-quality Security Newsletter featuring exclusive interviews with people from the Scene including practical guides and articles on Information Security and various daily updated Security Tools and Security Document reviews and since I’ve recently touched based with the Team in a possible portal acquisition attempt I’ve decided to share some of my experience in managing and running the portal throughout 2003–2006 acting as Managing Director of hxxp://astalavista.com

Personal Photo of Astalavista.com Managing Director — Dancho Danchev — circa 2006 while running the portal

In this post I’ll describe The Scene the way we know it through the prism of my involvement as a hacker enthusiast throughout the 90’s and my primary position as Technical Collector of trojan horses for a variety of leading anti-trojans vendors including my participation in a variety of Scene-themed and oriented hacker groups at the time including the Netherlands-based Security Vendor - Frame4 Security Systems, TechGenix's WindowSecurity.com and ITSecurity.com where I was busy responding to general questions related to Information Security which led me to to pursue a career as a Managing Director at hxxp://astalavista.com - The Underground - The World's Most Popular Information Security Portal for a period of three years while I was busy studying in the Netherlands with my best friend and girlfriend at the time - Yordanka Ilieva - acting as Security Newsletter Proofreader and overly general support throughout the hxxp://astalavista.com journey.

Sample Screenshot of Astalavista.com — The Underground Under the Management of Managing Director — Dancho Danchev — 2006

Throughout 2003–2006 while I was busy running the portal while acting as Managing Director I was basically responsible for managing all the content including basically all the Security Directory and Security News updates on a daily basis including the production of an extremely popular monthly **Security Newsletter** where I managed to take detailed and in-depth Featured **Security Interviews** from the various folks across the Scene and the Industry including the active organization and production of Advertising Inventory type of assets including to bring on board a highly-popular and reputable provider of SSL Certificates with their Crypto Challenge namely **Thawte** including the actual communication and presentation of the Advertising Inventory to a diverse set of possible advertisers.

Sample Introduction Video for Dancho Danchev's Most Recently Launched "Security is Futile" Security and Hacking Forum Community

Among my key responsibilities at the time were also to ensure that the actual Cracks and Series Search Engines list remains properly formulated in the context of properly describing the existence of malicious code of spyware on the actual Web sites with the idea that the actual hxxp://astalavista.com domain was never really responsible and was never really hosting any cracks or serials on the actual hxxp://astalavista.com domain including to properly promote hxxp://astalavista.net which at the time was the Premium Membership based Security Portal part of the Astalavista Security Group brand.

Sample Photo of Dancho Danchev acting as Managing Director of Astalavista Security Group's Astalavista.com throughout 2003–2006 While Studying in the Netherlands

Sample Security Interviews which I took while working for Astalavista Security Group circa 2003–2006:

Proge — http://www.progenic.com/ — 2003
Jason Scott — http://www.textfiles.com/ — 2003
Kevin Townsend — http://www.Itsecurity.com/ — 2003
Richard Menta — http://www.bankinfosecurity.com 2004
MrYowler — http://www.cyberarmy.net/ — 2004
Prozac — http://www.astalavista.com/ — 2004
Candid Wuest — http://www.trojan.ch/ — 2004
Anthony Aykut — http://www.frame4.com/ — 2004
Dave Wreski — http://www.linuxsecurity.com/ — 2004
Mitchell Rowtow — http://www.securitydocs.com/ — 2004
Eric (SnakeByte) — http://www.snake-basket.de/ — 2005
Björn Andreasson — http://www.warindustries.com/ — 2005
Bruce — http://www.dallascon.com/ — 2005
Nikolay Nedyalkov — http://www.iseca.org/ — 2005
Roman Polesek — http://www.hakin9.org/en/ — 2005
John Young — http://www.cryptome.org/ — 2005
Eric Goldman — http://www.ericgoldman.org/ — 2005
Robert — http://www.cgisecurity.com/ — 2005
Johannes B. Ullrich — http://isc.sans.org/ — 2005
Daniel Brandt — http://google-watch.org/ — 2005
David Endler — http://www.tippingpoint.com/ — 2005
Vladimir, 3APA3A — http://security.nnov.ru/ — 2005

Sample Personal Photo of Dancho Danchev While Working for CBS Interactive's ZDNet Zero Day Blog Throughout 2008–2013

Prior to my involvement in the Astalavista Security Group brand and company I was also involved in several other projects throughout the 90's as a teenage hacker enthusiast such as for instance:

A Member to **WarIndustries** (http://warindustries.com List
Moderator at **BlackCode Ravers** (http://blackcode.com)
Contributor **Black Sun Research Facility** (http://blacksun.box.sk)
(BSRF)
List Moderator Software Contributor (**TDS-2 Trojan Information Database**)

(https://packetstormsecurity.com/files/25533/tlibrary.zip.html)
DiamondCS Trojan Defense (http://tds.diamondcs.com.au)
Contributor to **LockDownCorp** (http://lockdowncorp.com)
Contributor to **HelpNetSecurity** (http://forbidden.net-security.org)
A security consultant for **Frame4 Security Systems** (http://frame4.com)
Contributor to **TechGenix's** WindowSecurity.com (http://www.windowsecurity.com/authors/dancho-danchev/)
Security blogger for **ZDNet** (http://www.zdnet.com/blog/security/)
Threat intelligence analyst for **Webroot** (https://www.webroot.com/blog/).

Sample Personal Photo of Dancho Danchev While Working as a Security Blogger for Webroot Inc.

In its current state the project could be easily transformed thanks to a **VR for Hackers and Security Experts** crowd-funding platform which I've recently launched where you can actually check the Dark Web Onion using the following **Clearnet URL** including the overall availability of an ubiquitous **IoT** (Internet of Things) device shipped to millions of users or eventually a good old fashioned Security and Hacking Forum Discussion Community similar to my recently launched "**Security is Futile** " Hacktivism-type of Community including to actually go through my direct Project Investment Proposal using the following **Clearnet URL** .

I wanted to let everyone know that I will be definitely looking forward to re-lauching the official Astalavista Security Group hxxp://astalavista.com portal with the help of a growing set of Dark Web Onion visitors and that I will be definitely looking forward to sharing additional details on the official launch of the portal as soon as I manage to raise the necessary funds to officially launch the project in the form of a VR Application for Hackers and Security Experts or a good old fashioned Security and Hacking Forum Community.

Article 11

Exposing the U.S Intelligence Community and GCHQ's Use of "Dirty Tricks" Online — An Analysis

Dancho Danchev

Dec 23, 2019·8 min read

It should be fairly easy to assume that the prominent U.K's Intelligence Agency — the GCHQ — is both a master of offensive and defensive CNE (Computer Network Exploitation) tactics including the active use of network and Internet-host based including connected devices "dirty tricks" online. Largely relying on both an old-school set of espionage techniques successfully migrated in today's modern Internet-connected World including innovative and never-seen before type of technical and cyber espionage "know-how" and Cyber Assets SIGINT type of discovery including technical expertise the GCHQ continues to further master the Internet for the purpose of exfiltrating and targeting individuals and Communities-of-Notice internationally.

In this post I'll discuss in-depth the inner workings of GCHQ's Joint Threat Research Intelligence Group (JTRIG)'s use of "dirty tricks" online and the group's activities including the fact that what the group has managed to achieve is pretty much basically what I've managed to achieve in my Security Lab throughout 2008–2013 for both offensive and defensive Cyber Warfare purposes in terms of R&D and actually becoming a partner of U.S Intelligence Community in terms of " 4th Party Exfiltration" also known as "outsourcing SIGINT" including to provide active discussion on possible protection techniques and how the programs can actually perform better including an active discussion on various "Online Covert Operation" activities and actual cyber and good-old fashioned HUMINT in the context of the GCHQ's Joint Threat Research Intelligence Group (JTRIG) group activities online.

Sample Screenshot Indicating that I Was Featured as a Primary and Only EU-Based Individual As A Direct Competitor to the U.S

Cyber Threat Intelligence Market Segment Courtesy of Jeffrey Carr's Taia Global Presentation

Among some of the key good-old fashioned "Covert Cyber Operations" activities including good old-fashioned cyber HUMINT tactics and techniques include:

Establishing online aliases/personalities who support the communications or messages in YouTube videos, Facebook groups, forums, blogs etc. — as I've already discussed in a previous post detailing and actually exposing the GCHQ's use of "**sockpuppets** " type of fake and non-existent online aliases and personalities it should be also worth pointing out that the entire rogue bogus and potentially non-existent online and rogue account creation process can be easily outsourced using publicly accessible and obtainable DIY (do-it-yourself) type of rogue and bogus content generation tools. A sample similar service includes the automatic generation of "Fake Person" type of photos includes — http://thispersondoesnotexist.com which can be greatly used for the purpose of generating and basically creating fake online person accounts which can be greatly used to achieve the GCHQ's and U.S Intelligence Community's goals and objectives on their way to create "sockpuppet" type of accounts further spreading propaganda and disinforming in current and future-based propaganda and disinformation campaigns.

Sample Proposed "Fake Person" Honeytoken-Based Human-Layer Honeypot Deception Framework Graph

Establishing online aliases/personalities who support other aliases — the so called "establishment of sockpuppets" culture should be clearly considered as an automated way to spread propaganda disinform and actually compromise the OPSEC of a variety of individuals online that also includes reputable Security Researchers whose OPSEC and actually online privacy while doing online research can be greatly compromised and their opinion greatly influenced in the context of possibly "engineering cyber warfare tensions" or potentially disinform on "island-hoping" tactics similar to what I've been aiming to achieve with my "Fake Person" type of honeytoken-based type of rogue person-layer based deception framework.

Sample Proposed “Fake Person” Honeytoken-Based Human-Layer Honeypot Deception Framework MindMap

Sending spoof e-mails and text messages from a fake person or mimicking a real person (to discredit, promote distrust, dissuade, deceive, deter, delay or disrupt) — it should be clearly noted that modern spam campaigns and the actual malware that comes with it should be clearly treated as a form of economic terrorism with a handful of researchers out there who would take the necessary steps to ensure that such widespread campaigns remain properly “taken care” of in a bigger context of preventing widespread damage caused by malicious and fraudulent releases online.

Sample Personal Greeting Courtesy of the Koobface Gang Which Personally Thanks me for Exposing and Basically Attempting to Successfully Shut Down the Actual Koobface 1.0 C&CInfrastructure

Case in point is the **Koobface botnet** which I’ve extensively profiled throughout the years and I’ve successfully managed to prompt them to issue a response in the form of redirecting **Facebook’s entire IP space** to my personal blog including to actually issue a “**say hi** ” type of message within the actual command and control infrastructure personally greeting me for having successfully profiled and taken down a huge portion of the actual **Koobface 1.0** command and control infrastructure.

Sample “Exposing Koobface — The World’s Largest Botnet” Presentation Presented at CyberCamp 2016 Courtesy of Dancho Danchev

Providing spoof online resources such as magazines and books that provide inaccurate information (to disrupt, delay, deceive, discredit, promote distrust, dissuade, deter or denigrate/degrade) — some of these tactics can be basically described as good old-fashioned espionage campaigns in the context of utilizing cyberspace for the purpose of using basic HUMING and CYBERINT principles further positioning the campaign as a possible cyber espionage one with the actual orchestrator behind it successfully looking for ways to monetize access to malware infected hosts or to actually cause widespread damage internationally. These type of targeted attacks can be better attributed to good old-fashioned espionage techniques and tools of the trade which in the broader context of CYBERINT can include the active use of basic “engineering of cyber warfare tensions” including the active use of “island hoping” tactics making it for an analyst or Cyber Threat Intelligence to actually track down and properly attribute a specific malware-serving or malicious and fraudulent online campaign.

Providing online access to uncensored material (to disrupt) — these type of techniques should be clearly considered as an important milestone from a hacktivism type of perspective most importantly for the purpose of spreading data information and knowledge and to actually recruit Team Members and train and educate a new generation of Cyber Warrriors and potentially CYBERINT Intelligence Analysts on their way to properly attribute and track down a specific fraudulent and malicious online campaign.

Sending instant messages to specific individuals giving them instructions for accessing uncensored websites — unless the campaign is a widespread one it should be clearly noted that these type of attack campaigns can be potentially dangerous in the context of exposing a specific individual possibly in a restrictive regime to a regulated or forbidden type of content and then basically launch a privacy-violating Target Identificator type of campaign or to basically launch a basic client-side exploits serving campaign in a targeted fashion for the purpose of compromising the OPSEC of the individual in question and to actually track them down.

Setting up spoof trade sites (or sellers) that may take a customer’s money and/or send customers degraded or spoof products (to deny, disrupt, degrade/denigrate, delay, deceive, discredit, dissuade or deter) — these type of techniques can be best described as a possible form of financial and economic terrorism which basically aim to infiltrate the client or the target’s supply chain for the purpose of shipping them rogue and possibly modified products which could greatly undermine their OPSEC and potentially lead to some pretty serious privacy and security risks in case the orchestrator somehow managed to infiltrate the actual supply chain of the client or the actual target in question.

Interrupting (i.e., filtering, deleting, creating or modifying) communications between real customers and traders (to deny, disrupt, delay, deceive, dissuade or deter) — these type of campaigns can be best described as basic DDoS (Distributed Denial of Service) attack campaigns including the active use of TDoS (Telephony Denial of Service) attack campaigns which could eventually aim to properly disrupt the communication between a seller and a buyer.

Sample Screenshot of the Shenron DDoS Booter Kit in Action Which Basically Represents a Common Attack Technique in the Today's Modern Hacktivism-Driven World

Taking over control of online websites (to deny, disrupt, discredit or delay — these type of tactics directly include Web site Defacements and the use of DDoS (Denial of Service) attacks against a specific target for the purpose of stealing and compromising data or to actually deny a specific Web site's access to potential clients and customers include to properly spread a message potentially recruiting spreading data information and knowledge to millions of users globally.

Denial of telephone and computer service (to deny, delay or disrupt) — it used to be case where modern TDoS (Telephony Denial of Service) attacks used to be a highly restrictive and sensitive type of DoS (Denial of Service) attack techniques. However, thanks to the rise of commercial and on demand TDoS (Telephony Denial of Service) type of services courtesy of Russian and Eastern European cybercriminals that also includes capabilities currently offered and in use by the GCHQ and the U.S Intelligence Community it should be clearly noted that these type of attacks are prone to increase in terms of volume and sophistication. Case in point is BAT911.Worm which will basically attempt to call 911 with calls originating from the infected host's PC in case there's a modem present basically representing among the first distributed TDoS (Telephone Denial of Service) type of attack campaigns.

Hosting targets' online communications/websites for collecting SIGINT (to disrupt, delay, deter or deny) — as I've already pointed out in one of my previous analysis detailing and actually providing practical and relevant actionable intelligence on how the NSA utilizes rogue **Iran-based VPN** service providers to further eavesdrop and put under surveillance some of the actual users to further participate in the **BOUNDLESS INFORMANT** Top Secret Program.

Contacting host websites asking them to remove material (to deny, disrupt,delay, dissuade or deter) — it's fairly assume to assume that what the GCHQ's Joint Threat Research Intelligence Group (JTRIG) managed to achieve in terms of active online propaganda including terrorism and botnet type of shut-down activity online is pretty much similar to what I've managed to achieve in the context of shutting down and actually attempting to take down the Koobace 1.0's command and control infrastructure.

In future posts I'll continue to detail the inner workings of the GCHQ's Cyber Surveillance and Intelligence Programs in-depth including various other U.S Intelligence Community Programs similar to what I've managed to achieve throughout **2008–2013** in my Security Lab at by producing actionable threat intelligence at my extremely popular **Dancho Danchev's Blog — Mind Streams of Information Security Knowledge** including the active distribution of classified potentially sensitive type of content at my newly launched **https://unit-123.org** — feel free to go thought the actual **Project Introduction** post.

Article 12

How the GCHQ Used the Top Secret “ANTICRISIS GIRL” Program to Spy on Users — An Analysis

Dancho Danchev

Dec 30, 2019·3 min read

On the majority of occasions it appears that what the GCHQ managed to achieve in terms of “Passive SIGINT” namely to passively monitor and not interfere is pretty similar to what I’ve managed to achieve throughout the years in the field of cybercrime research and threat intelligence gathering namely to passively monitor a variety of newly born cyber threats including the emergence and actively profiling and tracking down of a variety of cybercriminals internationally.

Sample Screenshot of the Top Secret GCHQ “ANTICRISIS GIRL” Passive Web Traffic and Search Engine and Web Site Traffic Monitoring Program

Passive “SIGINT” also known as passively monitoring for cyber threats and the general approach of proactively monitoring for trends and anticipation of new and fraudulent and potentially malicious “event-based” activities and campaigns online can be best described as a proactive approach in terms of proactively responding to a growing threat posed by fraudulent and malicious cyber actors and fraudulent and malicious cyber attackers whose ultimately goal would be to launch and execute and orchestrate a variety of fraudulent and malicious campaigns online.

How exactly does the Top Secret “ANTICRISIS GIRL” “passive SIGINT” program work? It’s fairly simple to assume that basics “passive SIGINT” approaches similar to what I’ve manage to achieve while monitoring profiling and actually attempting to track down the Koobface 1.0 C&C infrastructure is pretty similar to what the Top Secret “ANTICRISIS GIRL” Program aims to achieve in the context of embedding basic Web Analytics tools on a variety of publicly-owned and private-sector type of automatically generated Blackhat

SEO and rogue and potentially fraudulent and malicious content-farms for the purpose of trends monitoring and the eventual direct intersection with Target Identifiers for the purpose of launching a variety of legal surveillance and eavesdropping campaigns against a multi-tude of targets.

Sample “Exposing Koobface — The World’s Largest Botnet” Video Presentation Discussing In-Depth the Use of OSINT Methodologies Including “Passive SIGINT” To Actually Track Down and Monitor and Eventually Shut Down the Koobface Infrastructure Botnet

Based on the “passive SIGINT” obtained in that particular case that also includes the direct and potentially malicious attempt to actually inject Web Analytics code and monitoring analytics type of tools on legitimate Web Properties whose visitors might fall victim into a possible legal surveillance and legal eavesdropping attempts such as for instance Wikileaks or Piratebay users including basically anyone who falls victim and actually visits an automatically generated and on purposely created rogue and fraudulent including potentially malicious Blackhat SEO themed online “content-farm”.

Key topics that might attract the GCHQ’s and the U.S Intelligence Community’s attention:

Rogue and Bogus Clearance Jobs and Resources Type of Portals and Materials
Rogue and Bogus Lyrics and other traffic acquisition tactics and techniques
Publicly Accessible Statistics for Major Online Properties that also includes URL Shortening Services whose visitors can be easily geolocated and Target Identifiers easily applied to further track down the individuals behind the actual use of these URL Shortening services

Sample Koobface 1.0 Infrastructure Web Site Referrers Obtained from Publicly Accessible Statistics

Case in point is the Koobface 1.0’s infrastructure which successfully redirected Facebook’s IP Space to my personal blog the active use of publicly accessible Web statistics tracker which at certain point made it possible to actually track down where most of the Koobface 1.0’s infrastructure traffic was coming from.

Sample Koobface 1.0 Infrastructure Originating Countries Traffic Obtained from Publicly Accessible Statistics

What end users and Web site owners should keep in mind is to preserve the privacy of their Web analytics including possibly the URL shortening service of use in the context of limiting access to publicly obtainable statistics which could be easily used for “passive SIGINT” including to eventually apply Target Identifiers to the visitors of a particular Web site or a Social Media Account and eventually violate the privacy and put under legal surveillance and eavesdropping a specific set of users or specific visitors to a specific Web site.

Article 13

The 2016 U.S Presidential Elections and Russia’s Active Measures in Terms of Cyber Espionage

Dancho Danchev

Dec 30, 2019·3 min read

It’s becoming increasingly evident that major U.S-based mainstream Security News providers are increasingly becoming victim of a growing trend in the face of “blame it on Russia“ including China and Iran in terms of good old fashioned espionage tactics and techniques known as Active Measures and are therefore proceeding to take down profile and shut down a variety of newly emerged “Fake News” type of online outlets which basically represent nothing more than a good-old fashioned Blackhat SEO (Search Engine Optimization) tactic capable of attracting hundreds of thousands of new visitors to a particular Web site on the basis of generating rogue and potentially malicious and non-existent type of content including the active establishment of what can be best described as a wrongly perceived online threat in the face of cyber personas which became increasingly popular following the 2016 U.S Presidential Election in the face of the Guciffer 2.0 supposedly Russian-powered enterprise responsible for leaking key data on the 2016 U.S Presidential Election.

Sample Detection Rate for Russia’ GRU Custom Made X-Agent Legal Surveillance Malicious Software

In this post I’ll provide actionable intelligence on the rogue and potentially fraudulent Guciffer 2.0 supposedly Russian-sponsored enterprise and offer an in-depth technical and OSINT-based type of analysis on the actual events that took place during the 2016 U.S Presidential Elections in terms of Russia’s active measures and cyber espionage campaigns.

Sample Bitly URL-Shortening Service Statistics and Actual Spear Phishing URL and Domain Used in the 2016 U.S Election Cyber

Espionage Campaign Courtesy of Russia's GRU Directly Targeting John Podesta

Sample Bitly URL-Shortening Link Used in the Actual 2016 U.S Election Cyber Espionage Campaign Courtesy of Russia's GRU Targeting John Podesta:

hxxp://bit.ly/1PibSU0

Sample Personal IP Used to Access John Podesta's Personal Gmail Account:

hxxp://134.249.139.239–34–249–139–239-gprs.kyivstar.net

Sample Personal Emails and Personally Identifiable Information of Guccifer 2.0 Enterprise Including a Personal IP Address:

Email: guccifer20@aol.fr — 208.76.52.163
Email: guccifer20@gmz.us

Sample VPN Service Provider Used by the Guccifer 2.0 Enterprise:

hxxp://fr1.vpn-service.us — Email: sec.service@mail.ru; vpn_support@mail.ru — 95.130.15.34

Fake Name-Based Personalities used by Russia's GRU in the 2016 U.S Election cyber espionage campaign:

Mike Long
Ward DeClaur
Daniel Farrell
Jason Scott
Richard Gingrey
Alice Donovan
Den Katenberg
Yuliana Martynova
Karen W. Millen
James McMorgans
Kate S. Milton

Sample Passive DNS Reconnaissance on all the Currently Active Domains Used in the 2016 U.S Election cyber espionage campaign courtesy of Russia's GRU:

hxxp://accounts-qooqle.com — Email: annaablony@mail.com — 87.236.215.99
hxxp://www.account-gooogle.com
hxxp://mail.myaccountsgoogle.com
hxxp://account-gooogle.com
hxxp://accounts.google.com-sl.com
hxxp://googl-login.com
hxxp://com-sl.com
hxxp://accounts.pass-google.com
hxxp://www.pass-google.com
hxxp://myaccountsgoogle.com
hxxp://pass-google.com

Sample Passive DNS and Responding IPs for the actual spear phishing campaign:

hxxp://www.myaccount.google.com-changepasswordaccount.cf
hxxp://www.myaccount.google.com-changepasswordaccount.gq
hxxp://www.myaccount.google.com-changepasswordaccount.ga
hxxp://www.myaccount.google.com-changepasswordaccount.ml
hxxp://www.myaccount.google.com-changepasswordaccount.tk
hxxp://com-securitysettingpage.ml
hxxp://com-securitysettingpage.tk
hxxp://com-securitysettingpage.cf
hxxp://myaccount.google.com-securitysettingpage.ga
hxxp://myaccount.google.com-securitysettingpage.ml
hxxp://myaccount.google.com-securitysettingpage.tk
hxxp://myaccount.google.com-securitysettingpage.cf
hxxp://myaccount.google.com-securitysettingpage.gq
hxxp://com-securitysettingpage.gq
hxxp://195.20.46.133
hxxp://80.255.12.237

Sample command and control server IPs used in the actual 2016 U.S Election Cyber Espionage Campaign Courtesy of Russia's GRU:

hxxp://linuxkrnl.net
hxxp://misdepatrment.com — frank_merdeux@europe.com

hxxp://5.135.183.154
hxxp://45.32.129.185

It should be clearly noted that spear phishing campaigns will continue to actively propagate and eventually target hundreds of thousands of users in a targeted fashion that also includes U.S Intelligence Community and Law Enforcement analysts and members of the U.S Intelligence Community.

Article 14

How the GCHQ and the NSA work on intercepting and infiltrating Virtual Private Networks?

Dancho Danchev

Feb 2, 2020·6 min read

Sample Screenshot of DARKSUNRISE Top Secret VPN Surveillance and Eavesdropping Program

It a modern cybercrime ecosystem driven and motivated by financial gain and actual fraudulent and malicious activities on a large scale it should be noted that modern nation-state adversaries are basically always there to "take care" in terms of launching offensive both passive and active SIGINT and metadata harvesting and interception campaigns this time against VPN users and VPN service providers potentially matching the traffic flow coming out and going out of the Virtual Private Network (VPN) service providers and actually launching targeted and client-tailored attack campaigns against VPN users and vendors of VPN service providers.

In this post I'll discuss in-depth some of the currently circulating VPN eavesdropping including possible man-in-the-middle and actual metadata harvesting type of attack campaigns launched by nation-state actors targeting users of VPN services and the actual users of the VPN service part of the Top Secret **DARKSUNRISE** Program including the **TURMOIL** , **TURBULENCE** , **PINWALE** , including the activities of the U.S Intelligence Community's **OTP VPN Exploitation Team** .

Passive SIGINT — incoming traffic estimation — entry points — in this particular case pre-defined set of information could be easily obtained for the purpose of undermining the effectiveness of the VPN service provider including to actually target a specific user in this particular case by utilizing already used Target Identificators for the purpose of establishing the foundations for a successful end user's "entry point" monitoring which could have severe consequences for the actual user which could come under active and legal surveillance including the actual VPN provider whose “entry points” and actual network could become victim of possible network-based eavesdropping and legal surveillance attempts.

Active SIGINT — outgoing traffic estimation — exit points traffic estimation and passive or active monitoring— the primary point here would be to monitor a VPN service provider’s outgoing traffic in the context of finding possible gullible and unaware of today’s modern nation-state and rogue adversaries risks such as for instance various off-the-shelf de-anonymization tactics techniques and approaches in the context of collerating outgoing VPN service provider’s traffic and actually using a Target Identifier for a specific user in the context of having them log in and actually use a major Web 2.0 property including social media to further establish the foundations for a successful monitoring operation of the VPN service provider or an actual user of the VPN service provider.

Session-matching techniques — in this particular case possible Target Identifiers based on already harvested and collected data and possible traffic estimation based on gullible and VPN service provider gullible an unaware users could be used to do active “traffic measurement” and potentially launch sophisticated traffic and end-user “de-anonymization” tactics and techniques which could potentially undermine the usefulness of the VPN service provider and potentially offer a fake feeling of privacy and security for the end user who could easily end up as a victim of legal surveillance and eavesdropping attempts courtesy of the U.S Intelligence Community.

Going on the offensive — in this particular case and as I’ve previously profiled and discussed before the U.S Intelligence Community could easily launch and position and on purposely supply rogue and basically **wiretap-ready** VPN service providers in third-party countries such as for instance Iran ultimately having the VPN service provider’s users participate in the Top Secret BOUNDLESS INFORMANT Program.

Public Key Credentials Harvesting — in this particular case the U.S Intelligence Community could easily start to execute potential traffic “de-anonymization” and measurement activities to actually attempt to launch a legal surveillance and eavesdropping program against a specific VPN service provider potentially exposing the VPN

service provider user’s to a variety of legal surveillance and eavesdropping including passive and active SIGINT attempts.
VPN Providers internal passive SIGINT research procedures — in this particular case the U.S Intelligence Community would attempt to actually infiltrate and begin to benchmark the actual VPN service provider in question including possible launching a variety of Target Identifier campaigns against its users including possible a variety of “dirty-tricks” similar to the ones which I’ve already discussed in the context of **virtual HUMINT** .

Practical Tips for VPN service users in terms of protecting against nation-state adversaries:

consider looking for double-VPN or triple-VPN service providers whose connections are basically routed using multi-jurisdiction aware type of connections in order to establish rogue mixed and crowded sessions using mixed and crowded exit nodes and stay away from high-profile high-trafficked Web 2.0 major Web properties including the active use of off-the-shelf ad-blocking tools and services such as for instance **Pi-hole** .

Sample multi-jurisdiction aware proprietary and highly-secure and privacy-conscious VPN server provider — Cryptohippie Inc.

ensure that you should always come up with a way to obtain access to the actual accounting data for your VPN service provider in terms of doing so from an unknown and potentially secure network-location that doesn’t necessarily have to belong to you including to properly research the actual VPN service provider of choice using a third-party network location including to possibly use an alternative payment method to actually avoid being tracked down for using it in the first place.
consider using a possible off-the-shelf privacy-conscious anti-fingerpriting enabled Web browser such as for instance **nDalang** which basically has the capacity to hide your real-identity and actually prevent browser-fingerprinting attack campaigns especially in cases where the user is using a highly-secured and privacy-conscious VPN service provider such as for instance **Cryptohipppie** .
consider applying basic common sense in terms of OPSEC namely

consider using basic “hardware isolation” techniques which could for instance mean that you’re fully protected from possible network-based information leaks through the use of an “always-on” type of “hardware isolation” based VPN service provider by using for instance the **GL-AR750S** VPN Router which is extremely handy and properly secured in terms of using an “always-on” VPN service and is fully compatible with the **Cryptohippie** VPN service provider which also has a highly secure and off-the-shelf secured and privacy-conscious company-based professional **VPN router** which you can use in combination with **pfSense** in terms of applying basic network-based “hardware-isolation” techniques for the purpose of protecting your network security including the use of the necessary security and privacy-conscious VPN service provider which in particular case is the highly recommended Cryptohippie Inc. VPN service provider.

Practical Tips for VPN providers in terms of protecting their networks from nation-state adversaries and spreading awareness on how to properly use the VPN service among their clients:

the first and perhaps most single issue for VPN service providers is to come up with in-depth technical including possibly user-friendly guides and manuals on how to use and not to use the service in the context of preventing wide-spread abuse of the service including possible “false feeling of security” where the actual user might end up being exposed to a variety of nation-state and rogue actor techniques which despite the use of a professional and commercial-grade VPN service provider could easily pose risk to their online activities and might eventually end up exposing the gullible and unaware end-user’s online activity to a nation-state actor including rogue and potentially fraudulent rogue and malicious actors

properly educate your users on how to use and how not to use the service in terms of its sophisticated technical features including hands-on experience with actual and realistic threat scenarios such as for instance the use of popular Web 2.0 commercial and social media services which could easily result in a possible “de-anonymization” attempt on the actual user and might eventually lead to a possible legal surveillance and eavesdropping including possible use of Target Identifiers

It should be clearly noted that by outsourcing the responsibility for your online activities to a third-party in this particular case — a commercial or a proprietary VPN service provider the user should do their homework in terms of assessing the degree of privacy and security features offered by the VPN service including possibly to inquire about existing off-the-shelf features similar to what **Cryptohippie Inc.** has been doing for quite a while now.

Article 15

Who’s Behind Iran’s flagship Hacking and Web Site Defacement Group — Ashiyane Digital Security Team?

Dancho Danchev

Feb 2, 2020·4 min read

With the growing cyber warfare tensions between the U.S and Iran it should be clearly noted that a proactive response to the growing threat posed by Iranian Hacking Groups including lone Iran-based hackers should be properly and both technically and qualitatively assessed for the purpose of estimating and measuring the current state of the Iranian Hacking Scene further attempt to bring down key properties of Iran’s leading and major and most prominent Hacking Groups including Personal Web Sites belonging to Iran-based lone hackers for the purpose of ensuring that a proper response can be easily formulated further empowering the Security Industry and the U.S Intelligence Community with the necessary data information and knowledge to stay on the top of its game.

Sample Brochure of Dancho Danchev’s Most Recently Released Report on Iran’s Hacking Scene

In this post I’ll discuss in-depth the inner workings of Iran’s most famous and notable Hacking Group — The Ashiyane Digital Security Team and provide actionable intelligence including a Social Network Analysis Graph of some of the key members of the group including to discuss in-depth the actual findings of my most recently released research **report** on Iran’s Hacking Scene — “A Qualitative and Technical Collection OSINT-Enriched Analysis of the Iranian Hacking Scene Through the Prism of the Infamous Ashiyane Digital Security Team” which is a complimentary Second Edition of the original 2015’s “Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran” **report** and discuss in-depth the actual workings of the group including an in-depth discussion on their Social Media account activity and technical experience and expertise with the group currently responsible for thousands of successful Web site defacement campaigns across the globe.

Sample Personal Photo of Ashiyane Digital Security Team's Leader — Behrooz Kamalian

An excerpt from the actual report:

"*In a cybercrime ecosystem dominated by fraudulent releases and nation-state actors including possible high-profile "sock-puppets" and cyber proxies type of rogue and potentially superficially engineered cyber warfare tensions it should be clearly noted that a modern OSINT and virtual HUMINT actionable threat intelligence analysis of major and prominent cyber actors should take place for the purpose of setting up the foundations for a successful cyber actor monitoring including possible offensive and couter-offensive tactics techniques and procedures for the purpose of profiling and acting upon the gathered and monitored intelligence should take place through the automated and systematic Technical Collection and OSINT enrichment of the gathered data for the purpose of empowering the necessary decision-makers and third-parties with the necessary data information and knowledge including hands-on tactical and strategic intelligence to work with and act upon.* "

Sample Personal Photo of Ashiyane Digital Security Team's Leader — Nima Salehi

Whether it might sound awkward or strange it appears that Iran's flagship and most popular Hacking Group originally started as an online marketing agency managed and operated by the group's current leaders — Behrooz Kamalian and Nima Salehi including Alireza Baghbani including as an online "Check Your Yahoo ID Status" type of free online service known as Xeeber.

Sample Logo of the Original "Check Your Yahoo ID Status" Service which basically represents the origins of Iran's Flagship and Most Popular Hacking Group — The Ashiyane Digital Security Team

Proposed Counter-Offensive Methodology In Terms of the Ongoing Cyber Tensions Between the U.S and Iran:

Publicly disclose all the Iranian Hacker Group's Hacking Tools for the Industry and the general public to profile and research

Publicly disclose all the Iranian Hacker Group's personal photos in an attempt to identify track down and prosecute them

Approach the Persiangig.com Hosting Provider in an automated fashion in an attempt to automatically take-down and shutdown all the active Iranian Hacker Web Sites currently hosted there in a short-period of time

Publicly disclose all the Iranian Hacker Group's Personal Emails in an attempt to assist international and U.S Law Enforcement on their way to track them down and prosecute them

Publicly disclose all the Iranian Hacker Group's Personal Web Sites in an attempt to provoke more people from the Industry to get hold of their tools-of-the-trade and possibly profile and analyze the tools

Publicly disclose all the Iranian Hacker Group's Personal Web Sites Data Set in an attempt to provoke more people to enrich and study the actual Data Set

In case you're interested in obtaining access to the 2020's research on Iran's Hacking Scene feel free to approach me and I'l be happy to send you a personal copy including a copy of the research for your Team or Organization.

Article 16

The Inside Story Behind the Life of ex-Bulgarian Hacker Dancho Danchev

Dancho Danchev

Nov 25, 2020·27 min read

Sample Personal Photo of ZDNet's Zero Day Blogger Dancho Danchev. Imagery courtesy of Dancho Danchev

Dear Medium readers,

This is Dancho (https://ddanchev.blogspot.com) and I've decided to share my personal real-life story circa the 90's when I was a prominent ex-Bulgarian hacker during the infamous hacker spree during the 90's when Astalavista.box.sk and Progenic.com were my primary and daily visit type of bookmarks which greatly provoked me to pursue a basically 20 year long career as an information security specialist today's world's leading expert in the field of cybercrime research and threat intelligence gathering that's been maintaining one of the security industry's leading and most popular security publications since December, 2005 which is my personal blog which I originally launched while working as a Managing Director for https://astalavista.com which at the time was one of the world's most popular and high-traffic visited information security portals in the world where I had the privilege to work as a Managing Director while studying in the Netherlands.

Sample Photo of a Surveillance Camera. Image Courtesy of Dancho Danchev

Do you want to know about my real-life story as an ex-Bulgarian hacker during the 90's? Are you interested in learning more about how we set up the foundation of the Technical Collection market segment including today's modern threat intelligence market segment and how we set them straight using data information and knowledge which was produced and disseminated? Keep reading.

The story takes place in a small town in Bulgaria during the 90's in a post Soviet and post Communist country where modern technologies slowly start to take place prompting a local whiz kid to gather as much information from a network of connected computers known as the Internet for the purpose of seeking a global domination through active and persistent information sharing exchange with colleagues from across the globe including exclusively the United States and members of the U.S Security Industry the Scene and prominent members of the U.S Intelligence Community including hundreds of independent contractors in a post and pre 9/11 World which is where Dancho Danchev originally began his career as a hacker enthusiast today's leading expert in the field of cybercrime research and threat intelligence gathering.

Sample Personal Photo of Dancho Danchev's Hometown in Bulgaria — Troyan. Image courtesy of Dancho Danchev

While I was in Bulgaria during my teenage hacker years I was busy freelancing as an information security consultant while working with international security portals where I was busy offering advice and practical information security advice and practical solution recommendations including my work with CIO.bg where I once contributed with an article on Cyberterrorism and Cyber Jihad including a series of publications for HiComm.bg where I was running a popular information security rubric and participated with several articles in several of the magazine's issues.

At a later stage I somehow decided to go corporate an in a way find a way to enter the commercial information security industry with my knowledge potentially beginning to contribute with knowledge and information using my personal contacts at various information security portals on my way to land a possible job preferably as a writer security blogger or a journalist which I apparently succeeded in doing as I've been actively contributing with my own research and knowledge on a variety of h/c/p/a (Hacking/Cracking/Phreaking/Anarchy) portals at the time.

Sample Personal Photo of Dancho Danchev While Visiting Sofia Bulgaria. Image Courtesy of Dancho Danchev

At some point in time Dancho decide to approach the primary operator of one of his favorite security Web sites at the time — https://net-security.org for the purpose of contributing with an article for their newly launched forbidden.net-security.org project. His idea was to contribute with a security article for their recently launched Newsletter and the article in question was a good old-fashined “How to use trojan horses” manual. The article eventually got accepted and Dancho felt proud of himself for making a contribution to the project and having his article published so that eventually more people will read it and send him an email with questions about trojan horses and the actual article. The primary Webmaster of net-security.org at the time was Berislav Kucan and the project still remains one of Dancho’s favorite and most popular visited security Web site on a daily basis.

Sample Photo of Sofia Bulgaria. Image Courtesy of Dancho Danchev

At a later stage I decided to establish a working relationship with Frame4 Security Systems which is a Dutch-based company for the purpose of writing an improved version of the original “How to use trojan horses” paper which later on became the “The Complete Windows Trojans Paper” which quickly became one of the Scene’s most popular and highly read paper on modern trojan horses and how to use them and how to protect against them.

Sample Personal Photo of Erasmus Bridge Rotterdam. Image courtesy of Dancho Danchev

With the summer coming to an end Dancho got an offer to begin to work at the local office of his ISP (Internet Service Provider) which at the time was Digital Systems for the position of office assistant where he was responsible for introducing new clients to the ISP’s service offering and for processing invoices. Among the key benefits for working at the local ISP office was the actual bandwidth that he got access to allowing him to access the Internet without any sort of limitations which he used to visit some of his favorite Top50 and Top100 security and hacking Web sites where he eventually downloaded some of the most recently released hacking and security tools including trojan horses which he copied on a floppy disk and eventually brought back home during the lunch break for the purpose of exchanging the information with his second employer at the time which was an anti-trojans vendor using a publicly accessible FTP server for the purpose of helping his employer improve the detection rate for these type of programs and trojan horses. Dancho would then receive a payment for having collected and actually shared these programs and trojan horses which he would use to pay the bills at the time and actually pay for using his ISP's service.

Sample Directory Listing of Dancho Danchev's Repository of Technically Collected Trojan Horses for his Employer at the time LockDownCorp

At some point in time he eventually got approached by a guy known as HeLLfiReZ who was interested in working with him and actually sharing his collection of trojan horses which he would then also share with his employer which at the time was LockDownCorp and earn revenue in the process. It would later come to his attentio that the guy that approached him was actually one of the key members of the infamous Sub7 trojan horse group which at a particual point in time was responsible for launching a DDoS (Distributed Denial of Service) attack against the researcher Steve Gibson who extensively profiled the campaign and actually had a conversation with HeLLfiReZ and his team members for the purpose of finding out how launched the attack and how it took place.

He would eventually run a personal hacking and secutity Web site archive using hosting courtesy of his employer LockDownCorp and run a popular Hacking and Security Web site which he would then feature on Progenic.com's Top100 Hacking and Security Web sites including to actually offer paid security consultations in terms of finding out ways to help people protect their home PCs from trojan horses and teaching them how to use a firewall and how they can secure their home PCs.

Sample Screenshot of Dancho Danchev's Employer LockDownCorp Flagship Anti-Trojans Scanner Circa the 90's

At a later stage in his early Information Security career he would visit and join https://itsecurity.com's Security Clinic where he would have his personal biography featured and actually respond to common security questions which users of the Web site will submit and have his response featured on the front page potentially driving traffic to his employer at the time which was Frame4 Security Systems and actually improving his knowledge and understanding of Information Security in general.

Dancho was also known for having participated in the Blackcode Ravers hacking group which was running the popular https://blackcode.com Web site at the time and actually participated with two issues of a popular Security Newsletter at the time which were featured on the home page of the portal.

Sample Screenshot of Dancho Danchev’s Personal Modem which he used to rock the board during the 90's

During the glorious years of IRC (Internet Relay Chat) where Dancho was busy hanging on several IRC networks including DALNet and his local country’s IRC network he managed to obtain the /etc/shadow password file for his entire ISP (Internet Service Provider) which at the tim was Digital Systems and shared a copy of it with his best friend at the time George Kadiyski for the purpose of using several popular and high-profile Wordlists including John the Ripper password cracker potentially obtaining access and brute-forcing the entire password list for hundreds of active dial-up Internet based accounts at the time. Over a period of several days the results at the time were outstanding in the context of actually succeeding in the brute-forcing process potentially allowing Dancho and his friend to easily access free Internet based dial-up accounts which at the time cost money allowing them to use the Internet for free.

Sample Screenshot of Dancho Danchev’s Personal Hacking Page Called “Security is Futile” Circa the 90's

At a later stage Dancho also managed to obtain access to his local town’s competing ISP (Internet Service Provider) which was known as BIANet /etc/shadow which was send to him by a friend and he also once again shared it with his friend who would once again begin brute-forcing the password file using a variety of Worldlists and the infamous John the Ripper passwor cracking tool at the time potentially allowing Dancho and his friend easy access to unlimited Internet based dial-up connectivity.

Sample Screenshot of Dancho Danchev’s Personal Hacking Site Circa the 90's

The time has come to play a game. Dancho quickly powered his 16-bit Pravetz PC 2MB RAM and a screen full of computer game choices quickly appeared prompting him to choose a game. While loading a relatively known game known as Scorch Dancho decided to play two hours and then proceed with meeting his friends and start a discussion with his grandma. A huge fan of strategy games Dancho decided that he didn’t have the time to dedicate to play his favorite game — Sid Meier’s Civilization and instead he figured that he would eventually play the game later throughout the day. Playing Scorch was quite an experience and he took a few hours of his precious learning time to interact with the game. He then decided to approach his best friend at the time and co-conspirator in the World of UFO’s the Soviet Union and computer games including the hacking Scene for two hours of extensive game play where we would strategize on how to best “approach” the Soviet Union in terms of invasion actively and carefully planning every move on our way to invade the Soviet Union and eventually all the surrounding countries. While I was busy preparing for our several hour game play George was supposed to be busy going through a CD which was basically a mirror of Packetstormsecurity in particular the E-Zine section so that we can prepare to have a conversation in terms of working out our technological and military strategy on our way to achieve global domination in the original Sid Meier’s Civilization. What we basically did in the beginning was to strategize and actually get a better view of the technology tree of the game and while I was busy moving the Empire along George was busy keeping notes on our way to keep track and advance out military strategy on a “first come first serve” basis.

Sample Screenshot of Dancho Danchev’s infamous “The Complete Windows Trojans Paper” Publication Circa the 90's

Provoked by the need to reach out to a vast network of computers known as the Internet — Dancho quickly decided that the time has come to get connected — so that he decided to seek a proper connection provider in his local home-town. Back in the day the primary connection providers in the time were Bulgaria's Digital Systems BIA Net and the country's leading mobile connectivity provider — Mtel's pre-paid dial-up cards. Times were different in terms of connectivity and DSL and ADSL were a dream come true in the face of corporate networks properly utilizing and using ISDN type of based connectivity. Keeping it simple — Dancho decided to quickly acquire the necessary dial-up modem — which he would eventually fall in love with potentially reaching out to a vast network of computers known as the Internet using the help of a local dial-up provider known as Digital Systems. Back in the day — hourly based dial-up access meant think twice about what you do and how you do it online which means that I would have to basically prepare a plan for the things that I'll do online including Web sites which I would have to visit including a set of emails which I would have to send to a set of people including friends and colleagues.

It's been years since he prepared to acquire a personal computer and get connected meaning that he managed to prepare a list of Web sites and newsgroups on the topic of hacking and computer security including general Web sites that he would eventually visit. Among the first Web sites that he visited was NBA.com where he would quickly learn about the latest developments on his favorite team including daily going through photos and possibly video material to showcase his favorite team at the time. Among the most venerable experienced he first discovered prior to getting connected is to search for UFO photos and information on the KGB including the active reproduction of sound using his external speakers in a MIDI-dominated World at the time. The most venerable and unforgettable experience at the time was the fact that he had access to an email which he used to keep in touch with the Internet Service Provider's system administrator so that he could keep in touch with him including the active sharing of new Web site links for him to visit and exchange communication.

Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.

Among the first groups which I really joined at the time was Toxic Crisco which basically represented a group of individuals involved in a variety of online activities including possibly hacking including the SCR Project which was basically a social engineering driven hacking group where I was proud to be a member of in particular my active involvement in reading various high-profile psychology books at the time.

For the purpose of using IRC in particular DALnet Dancho quickly gathered a copy of the popular mIRC including several War Scripts ICQ Bombers Nukers and Mail Bombers including trojan horses and quickly decided that he should start getting experienced in the world of hacking for the purpose of gaining knowledge and impressing his friends. Among the first channels that he actually joined at the time were #gay and #lesbian where he was basically portraying himself as another person who was basically seeking to offer a new and novel photos-based screensaver to a variety of individuals for the purpose of tricking them into executing the screensaver on their home PCs ultimately gaining access to their PCs using a popular trojan horse client at the time such as for instance Sub7.

It would be fairly easy to assume how things got complicated with Dancho quickly obtaining access to Internet Relay Chat’s primary mIRC application including a variety of IRC-based “War Scripts” including a dozen of mail-bombers and various other ICQ-based type of Nukers and Flooders on his way to demonstrate a proper technical know-how to his friends and peers in the shady world of hacking. Among the first channels he tried to access were #hacker #hackers #hacking and the infamous #hackphreak on EFNet including to actually open several personal channels on the local IRC networks including #drugs #KGB and #linuxsecurity. At a later stage he actually managed to ask a friend for a possible operator status on the local town's IRC channel where he was basically running a 24/7 online protection bot known as xploit including the active use of a Socks5 server which at the time was offered by his employer LockDownCorp where he was busy acting as Technical Collector of trojan horses/worms/viruses and VBS scripts for the purpose of improving the anti-trojan software's signatures-based detection rates.

Sample Photo of 3G USB Modem which Dancho used for work while travelling

Among the first thing that Dancho decided to do in his spare time is to actively research the local Webmaster of his hometown's official Web site for the purpose of attempting to launch a social engineering attack against his local town's official Web site which basically succeed and resulted in a "greeting" message being posted on the official Web site with no actual data destruction and data removal taking place in what would appear to be a professional approach when compromising a legitimate Web site for the purpose of greeting his personal friends and spread a message on behalf of "Trojan Hacking Group" which at the time basically consisted of one of his closest friends and another fellow hacker enthusiast.

Among his responsibilities the time included the active collection of trojan horses/worms/viruses and VBS Scripts with the idea to share them with his employer which at the time was LockDownCorp one of the world's leading anti-trojan vendors for the purpose of improving the detection rate for these publicly accessible trojan horses in what would later on mature into a successful Technical Collection operation which basically paid his bills and actually offered him a decent financial incentive to continue getting involved in security as a hacker enthusiast and actually improved his employer's overall detection rate for some of the most prolific trojan horses at the time.

Sample Photo of Dancho Danchev while travelling. Image courtesy of Dancho Danchev

The actual contractual agreement had to do with Danchousing a private FTP server where he would spend hours uploading collected trojan horses using his home-based dial-up connection and eventually earning a revenue in the process using Western Union where he was happy to have established direct working relationship with one of the world's leading anti-trojans vendors which at the time was located at — http://proxy2.stealthedip.com/maniac/incoming/

Whenever Dancho would attempt to reach out to his friends he would attempt to find out whether they are online using a popular trojan horse including to actually check his email account for their recently changed passwords and other related information including their current IP so that he can properly connect to their home PC for educational purposes.

Being the World's most notable cybercrime researcher security blogger and threat intelligence analyst the researcher quickly gained fame by systematically and efficiently profiling and analyzing a decent snapshot of malicious nation-state and fraudulent activity online leading him to pursue a successful career as the World's most popular cybercrime researcher security blogger and threat intelligence analyst.

Sample Personal Photo of Dancho Danchev. Imagery Courtesy of Dancho Danchev

In an early Monday morning the researcher quickly gathered a set of research materials of the primary botnet that's he's been monitoring the infamous Koobface botnet using passive and active virtual SIGINT methodologies which basically include active sampling of the botnet's malicious online activities using a daily set of intercepted malicious and fraudulent campaigns launched managed and operated by the Koobface botnet for the purpose of providing the necessary technical operational and strategic OSINT type of intelligence including the daily batch of money mule recruitment domains and campaigns which he was busy profiling with the idea to assist U.S Law Enforcement on its way to track down and prosecute the cybercriminals behind these campaigns.

Sample Photo of GCHQ’s “Lovely Horse” Program to monitor Hackers on Twitter where Dancho Danchev Participated

The Koobface botnet was the primary botnet propagating over social media at the time in particular Facebook and has already managed to affect tens of thousands of users globally potentially enticing them to interact with rogue and visual social engineering based type of malicious and fraudulent campaigns in the form of Fake Adobe Flash Players and fake YouTube videos where the ultimate goal would be to attempt to affect their friends on Facebook by sending automated and legitimately looking messages including links to rogue and malicious content.

Sample Screenshot of Dancho Danchev’s Security Newsletter for Blackcode.com Circa the 90's

It’s been years since he prepared to acquire a personal computer and get connected meaning that he managed to prepare a list of Web sites and newsgroups on the topic of hacking and computer security including general Web sites that he would eventually visit. Among the first Web sites that he visited was NBA.com where he would quickly learn about the latest developments on his favorite team including daily going through photos and possibly video material to showcase his favorite team at the time. Among the most venerable experienced he first discovered prior to getting connected is to search for UFO photos and information on the KGB including the active reproduction of sound using his external speakers in a MIDI-dominated World at the time.

Sample Screenshot of Dancho Danchev’s Trojan Analysis Database which he did for his employer DiamondCS’s Trojan Defense Suite Circa the 90's

The most venerable and unforgettable experience at the time was the fact that he had access to an email which he used to keep in touch with the Internet Service Provider’s system administrator so that he could keep in touch with him including the active sharing of new Web site links for him to visit and exchange communication.It’s been years since he prepared to acquire a personal computer and get connected meaning that he managed to prepare a list of Web sites and newsgroups on the topic of hacking and computer security including general Web sites that he would eventually visit. Among the first Web sites that he visited was NBA.com where he would quickly learn about the latest developments on his favorite team including daily going through photos and possibly video material to showcase his favorite team at the time. Among the most venerable experienced he first discovered prior to getting connected is to search for UFO photos and information on the KGB including the active reproduction of sound using his external speakers in a MIDI-dominated World at the time. The most venerable and unforgettable experience at the time was the fact that he had access to an email which he used to keep in touch with the Internet Service Provider's system administrator so that he could keep in touch with him including the active sharing of new Web site links for him to visit and exchange communication.

Sample Personal Screenshot of Dancho Danchev's Personal Hacking Web Site Circa the 90's

Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.

Sample Screenshot of a Sample Ethical Web Site Compromise Circa the 90's. Image Courtesy of Dancho Danchev

Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I

was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.

Sample Screenshot of a Private Psychedelic Trance Party in Second Life. Image Courtesy of Dancho Danchev

Among the next most prominent and key features of the Internet which I used at the time was ICQ in particular the fact that the messages from my hometown traveled to the capital of the country in real-time which was particularly impressive in particular the fact that I was receiving immediate responses to my messages. It was fairly logical to conclude that the active exchange of messages on ICQ and actual contacts was crucial to becoming popular and actually attempting to own the Scene. What I practically did at the time was to request several of my friends which were known to have been involved in the Scene at the time to forward and exchange a decent set of ICQ contacts of fellow members of the Scene which quickly empowered me with the necessary contacts to join several hacking groups in particular HackHouse and the Social Engineering Project where I was proud to be a member of.

Sample Screenshot of Dancho Danchev’s Personal External Battery which he used for travelling while working for ZDNet

Among the first groups which I really joined at the time was Toxic Crisco which basically represented a group of individuals involved in a variety of online activities including possibly hacking including the SCR Project which was basically a social engineering driven hacking group where I was proud to be a member of in particular my active involvement in reading various high-profile psychology books at the time.

For the purpose of using IRC in particular DALnet Dancho quickly gathered a copy of the popular mIRC including several War Scripts ICQ Bombers Nukers and Mail Bombers including trojan horses and quickly decided that he should start getting experienced in the world of hacking for the purpose of gaining knowledge and impressing his friends. Among the first channels that he actually joined at the time were #gay and #lesbian where he was basically portraying himself as another person who was basically seeking to offer a new and novel photos-based screensaver to a variety of individuals for the purpose of tricking them into executing the screensaver on their home PCs ultimately gaining access to their PCs using a popular trojan horse client at the time such as for instance Sub7.

Among the first groups which I really joined at the time was Toxic Crisco which basically represented a group of individuals involved in a variety of online activities including possibly hacking including the SCR Project which was basically a social engineering driven hacking group where I was proud to be a member of in particular my active involvement in reading various high-profile psychology books at the time.

On a beautiful Thursday afternoon Dancho decided to play a decent computer game while his mother was busy ironing in the kid’s room and decided to take a journey successfully getting the World rid of hostile aliens. The game called Duke Nukem basically took Dancho on a journey to another World where he spend most of his afternoon getting rid of evil aliens while he led a discussion with his mother on his whereabouts during the day including active next-day class preparation and the eventual dinner conversation. While mom was busy ironing Dancho took on another journey to a distant World where he took care of and protected the Earth from evil aliens and decided that the time has come for a rest.

Some of the most memorable memories of Dancho back in the time have to do with playing full-time one of the best strategy games during the 90’s that’s Sid Meier’s Civilization. Spending a decent portion of his time basically four hours on a daily basis Dancho quickly acquired the necessary skills to take his civilization to a new level by waging wars developing and exchanging new technologies and by waging wars with competing and adversary civilizations.

Having already mastered the power of the Civilization game Dancho quickly fell into a World of politics technologies and wars and successfully mapped and left a foothold in the World the way he knew and mastered having successfully spend a decent portion of his time playing the best strategy game during the 90’s that’s Sid Meier’s Civilization. Game World is something different. Whenever Dancho decided to play a game the World came to a halt with Dancho playing and learning the basics and inner workings of every game that he managed to get his hands on throughout the 90’s.

Pushing the boundaries of the game at some point Dancho decided to take a deeper look at how you can actually make the computer’s player become more advanced and sophisticated and actually tried to train the AI of the game and potentially figured out a way to teach to use advanced warfare tactics.

It would be fairly easy to assume how things got complicated with Dancho quickly obtaining access to Internet Relay Chat’s primary mIRC application including a variety of IRC-based “War Scripts” including a dozen of mail-bombers and various other ICQ-based type of Nukers and Flooders on his way to demonstrate a proper technical know-how to his friends and peers in the shady world of hacking. Among the first channels he tried to access were #hacker #hackers #hacking and the infamous #hackphreak on EFNet including to actually open several personal channels on the local IRC networks including #drugs #KGB and #linuxsecurity. At a later stage he actually managed to ask a friend for a possible operator status on the local town’s IRC channel where he was basically running a 24/7 online protection bot known as xploit including the active use of a Socks5 server which at the time was offered by his employer LockDownCorp where he was busy acting as Technical Collector of trojan horses/worms/viruses and VBS scripts for the purpose of improving the anti-trojan software’s signatures-based detection rates.

Sample Socks5 Commercially-available servers courtesy of LockDownCorp one of Dancho’s current employers at the time which he used to increase his reputation on the local IRC Network and to actually hide his real IP

Among the first thing that Dancho decided to do in his spare time is to actively research the local Webmaster of his hometown’s official Web site for the purpose of attempting to launch a social engineering attack against his local town’s official Web site which basically succeed and resulted in a “greeting” message being posted on the official Web site with no actual data destruction and data removal taking place in what would appear to be a professional approach when compromising a legitimate Web site for the purpose of greeting his personal friends and spread a message on behalf of “Trojan Hacking Group” which at the time basically consisted of one of his closest friends and another fellow hacker enthusiast.

Sample Web Site Defacement courtesy of Dancho throughout the 90’s which basically resulted in a personal message and a personal greeting to all of his friends at the time courtesy of “Trojan Hacking Group”

Among his responsibilities the time included the active collection of trojan horses/worms/viruses and VBS Scripts with the idea to share them with his employer which at the time was LockDownCorp one of the world’s leading anti-trojan vendors for the purpose of improving the detection rate for these publicly accessible trojan horses in what would later on mature into a successful Technical Collection operation which basically paid his bills and actually offered him a decent financial incentive to continue getting involved in security as a hacker enthusiast and actually improved his employer’s overall detection rate for some of the most prolific trojan horses at the time.

The actual contractual agreement had to do with Dancho using a private FTP server where he would spend hours uploading collected trojan horses using his home-based dial-up connection and eventually earning a revenue in the process using Western Union where he was happy to have established direct working relationship with one of the world’s leading anti-trojans vendors which at the time was located at — http://proxy2.stealthedip.com/maniac/incoming/

Whenever Dancho would attempt to reach out to his friends he would attempt to find out whether they are online using a popular trojan horse including to actually check his email account for their recently changed passwords and other related information including their current IP so that he can properly connect to their home PC for educational purposes.

Being the World's most notable cybercrime researcher security blogger and threat intelligence analyst the researcher quickly gained fame by systematically and efficiently profiling and analyzing a decent snapshot of malicious nation-state and fraudulent activity online leading him to pursue a successful career as the World's most popular cybercrime researcher security blogger and threat intelligence analyst.

Sample Brochure created by Dancho Danchev for an upcoming research paper on Iran's Hacking Ecosystem

Back in 2007 I got a direct invitation to attend a private and invite-only conference event held by the Honeynet Project at the U.K's GCHQ which I actually attended and presented on a variety of topics including current and emerging cybercrime trends and actually got the opportunity to meet with the folks from the Honeynet Project.

Sample Screenshot of Dancho Danchev's Presentation Held at U.K's GCHQ in 2007. Image Courtesy of Dancho Danchev Sample Cartoon Created by Dancho Danchev for a presentation. Image Courtesy of Dancho Danchev

In 2008 I got a surprise invitation to join the team at ZDNet a web site portal which I greatly admired while I was busy working for https://astalavista.com and I was in fact visiting on a daily basis where I spend a highly professional and productive 4 years as a security blogger at ZDNet's Zero Day blog leading to me to thousands of publications including an actual award-winning Jessy H. Neal Award for working on ZDNet's Zero Day blog.

Sample Screenshot of ZDNet's Zero Day Blog. Image Courtesy of Dancho Danchev

Working for ZDNet greatly shaped my professional well-being in a way that I was basically working with top-notch technology experts from across the globe and actually had the chance to contribute with personal content and research for a period of four years which was an unforgettable experience and it’s still a pleasure and a honor to touch base and actually find a way to contribute and say hi to the people that I used to work with back in 2008.

At some point in time I eventually got invited to attend a private and invite-only conference where I presented on money mule recruitment practices and eventually got the privilege to meet most of the people that I work with on a face-to-face basis where we hang out and actually socialized and discussed various hot topics and cybercrime trends internationally.

Sample Personal Screenshot of a Private Dinner. Image Courtesy of Dancho Danchev

Dancho began his career in the world of Intelligence Studies greatly provoked by research published and distributed by a U.S based company known as iDefense which basically specializes in profiling online hacktivism activity and is basically capable of producing high-quality and never-published before threat intelligence and general intelligence briefs. Among the key reports that Dancho was able to get his hands on was the U.S/China skirmish which basically consisted of various U.S and Chinese based groups actively interacting online by launching DDoS (Distributed Denial of Service) attacks against their infrastructure and participating in Web site defacement campaigns. He would then research and actively visit the CIA.gov’s official Web site including FAS.org and NSA.gov seeking manuals and research material on Open Source Intelligence (OSINT) which would later on greatly contribute to help him become one of the World’s leading experts in the field of cybercrime research and threat intelligence gathering.

Sample Personal Photo of Dancho Danchev’s Business Card circa 2012. Image courtesy of Dancho Danchev

In an early Monday morning the researcher quickly gathered a set of research materials of the primary botnet that’s he’s been monitoring the infamous Koobface botnet. His main motivation behind tracking down and monitoring one of the most prolific botnet that was spreading across Facebook at the time was to assist the Security Industry and researchers internationally including U.S law enforcement on their way to keep track of the botnet’s activities and eventually attempt to take it offline and actually attempt to track down some of the authors behind it.

Sample Vinyl Cover of Dancho Danchev's Album Released Online by a Canadian Industrial Artist

Dancho's daily routine consisted of checking the most recent campaigns launched by the gang and actually offer in-depth technical analysis on the latest campaigns publicly disseminating and profiling the campaigns at his personal blog leading him to a specific set of detailed and in-depth analysis of the Koobface botnet one of the few publicly accessible analysis resources on the topic at the time.

Sample Screenshot of Dancho Danchev's Presentation on Koobface Presented at CyberCamp 2016

The botnet masters at the time were basically known to keep track of Dancho's research and eventually left a message embedded in the actual C&C infrastructure basically greeting the researcher for his research including a second and a third message during the Christmas season including an actual point-by-point response to his "Top 10 Things You Didn't Know About the Koobface Gang" article which he published at ZDNet's Zero Day blog.

Sample Photo of Dancho Danchev Presenting at RSA Europe 2012

At a later stage he would present his findings in a Keynote Presentation at CyberCamp 2016 on the topic of "Exposing Koobface — The World's Largest Botnet" in front of a high-quality audience and actually discuss in-depth how he tracked it down and eventually attempted to take it offline.

Sample Brochure of Dancho Danchev's Flagship Second Edition of his Report on Exposing Iran's Hacking Ecosystem

While he was busy studying in the Netherlands he became familiar what appeared to be one of the most popular Web sites for hackers on the Web known as Astalavista.com where he managed to actually find the real company behind the portal and actually approached.

In 2021 I can be reached at ddanchev@cryptogroup.net including my personal blog — https://ddanchev.blogspot.com including the infamous — https://astalavista.box.sk where I’m currently running a high-profile hacking and security project.

Yours sincerely,

Dancho Danchev