Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3 Threat Profile: Evil Corp

August 29, 2022 TLP: White Report: 202208291500

Threat Profile: Evil Corp (AKA UNC2165)

Executive Summary

Evil Corp (AKA UNC2165) is a one of the most capable cybercriminal syndicates in the world. They are based out of Russia and have been operational since 2009. They are responsible for the development and operations of several of the most powerful malware and ransomware variants, and maintain strong relationships not just with other powerful cybercriminal gangs, but also the Russian government. The U.S. federal government has indicted members of their gang and has an active bounty offered for information on their leadership. Evil Corp has been observed modifying their activities to circumvent U.S. federal government actions to stop them.

Impact to HPH Sector

Evil Corp should be considered a significant threat to the U.S. health sector based on several factors. Ransomware is one of their primary modus operandis as they have developed and maintained many strains. Many ransomware operators have found the health sector to be an enticing target as, due to the nature of their operations, they are likely to pay some form of ransom to restor operations. Healthcare organizations are particularly suceptible to data theft as personal health information (PHI) is often sold on the dark web to those looking to leverage it for fraudulent purposes. Foreign governments often find it to be more cost effective to steal research and intelliectual property via data exfiltration cyberattacks rather than invest time and money into conducting research themselves. This includes intellectual property related to the health sector. It is entirely plausable that Evil Corp could be tasked with acquiring intellectual property from the U.S. health sector using such means at the behest of the Russian government.

Overview

Evil Corp is a cybercriminal gang that has been exceptionally aggressive and capable in their more than decade of global hacking operations. According to the U.S. Treasury Department in 2019, “Evil Corp has used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft,” and also has, “caused millions of dollars of damage to U.S. and international financial institutions and their customers.” Seventeen members of the group have been sanctioned by the U.S. Treasury Department and two key members are under indictment by the FBI. Former Treasury Secretary Steven Mnuchin refered to Evil Corp as, “of the world’s most prolific cybercriminal organizations.” Former Assistant Attorney General Brian A. Benczkowski characterized some of Evil Corp's actions as having, “deployed two of the most damaging pieces of financial malware ever used and resulted in tens of millions of dollars of losses to victims worldwide" and being, “the perpetrators behind the world’s most egregious cyberattacks,” and having targeted victims across the globe in, “one of the most widespread malware campaigns we have ever encountered.” The State Department and FBI have a standing offer of $5 million for information leading to the arrest and conviction of their leader, Maksim Yakubets, which is the largest reward for a cybercriminal ever offered.

Evil Corp is known for their development and operation of Dridex (related to Cridex and Bugat), which is a multifunctional malware variant capable of impacting the confidentiality and availability of protected data and systems directly related to business operations. This has included banking and healthcare information. The Department of Homeland Security has called Dridex, “one of the most prevalent financial

Trojans." They are also known for developing and operating Zeus and several of its major variants, as well as a number of prevalent ransomware variants such as Doppelpaymer, Hades, Phoenixlocker and Wastedlocker.

Nomenclature and Associations/Affiliations

Evil Corp is also known as UNC2165, GOLD DRAKE and Indrik Spider. Please note that these associated threat group labels are presented as coassociated with a high degree of confidence, but are not 100% absolute as they represent intrusion clusters analyzed by a number of different research teams and organizations. It is also worth noting that there are open source assessments which associate Evil Corp with TA-505, however HC3 does not currently support that conclusion.

Leadership and Key Individuals

- Maksim Yakubets is Evil Corp's leader and is responsible for managing and supervising the group's operations as well as intefacing with the Russian government. He is known to have worked directly with Andrey Ghinkul in the operations of their Dridex malware program. Yakubets has also been responsible for recruiting and managing Evil Corp's money mules – individuals responsible for facilitating the movement of money illicitly gained through a series of accounts which make tracing these transactions a significant challenge to law enforcement. Yakubets was indicted by a federal grand jury in 2019 and charged with conspiracy, computer hacking, wire fraud, and bank fraud. This was related to the distribution of Bugat, a predecessor of Dridex. He was also charged in a separate criminal complaint that year with conspiracy to participate in racketeering, computer fraud and theft. Yakubets is also known for his relationship with the Russian government. Yakubets has also provided direct assistance to one of Russia's leading intelligence organizations, the FSB, who were sanctioned in December of 2016. Yakubets was known to be in the process of obtaining the equivalent of a security clearance to formally obtain permission to access classified information in support of the Russian FSB. Yakubets has been tasked to work on projects for the Russian government, which included the acquisition of protected data through agressive actions in cyberspace and conducting cyber operations on its behalf.
- Evgeniy Bogachev is a key member of Evil Corp who is currently wanted by the FBI for his management of several of the prolific Zeus malware variants (including Jabber Zeus and GameOver Zeus), used to target many sectors including healthcare in order to collect and further exploit sensitive data. He is the second significant member of Evil Corp to have been indicted in 2019, along with Yakubets. Bogachev is known to go by the online monikers "lucky12345" and "slavik". Similar to yakubets, Bogachev is considered one of the most wanted hackers in the world.
- Igor Turashev is another key memebr who is known to have served Evil Corp as an administrator, has had a role in targeting and has also maintained control over the Dridex malware project.
- Denis Gusev is another key member of Evil Corp whose role has included financial facilitator and logistics coordinator. Gusev operates six businesses based out of Russia including Biznes-Stolitsa, OOO, Optima, OOO, Treid-Invest, OOO, TSAO, OOO, Vertikal, OOO, and Yunikom, OOO.
- Other core members of the group that carry out critical activities include Dmitriy Smirnov, Artem Yakubets, Ivan Tuchkov, Andrey Plotnitskiy, Dmitriy Slobodskoy, and Kirill Slobodskoy. These individuals are involved in management of the Dridex malware program, supervising the targeting process as well as other technical, financial and logistical aspects of the group. These individuals were also named in the December 2019 indictment.
- Evil Corp is known to rely heavily on money mules. Eight Moscow-based individuals who have

served as financial facilitators for Evil Corp include Aleksei Bashlikov, Ruslan Zamulko, David Guberman, Carlos Alvares, Georgios Manidis, Tatiana Shevchuk, Azamat Safarov, and Gulsara Burkhonova. These individuals are ensure the illicit movement of stolen money in such a way to elude tracing by law enforcement. These individuals were also named in the December 2019 indictment.

Motivations

Evil Corp is primarily a cybercriminal group and as such, is financially motivated. This motivation often manifests itself in the form of digital extortion, such as ransomware attacks, as well as cyberattacks that facilitate sensitive information theft – financial or otherwise – which can then be sold on the dark web for a profit. However, where Evil Corp distinguishes themselves from many other threat actors is how they blur the proverbial lines between cybercriminals and state-sponsored activities. They are known to cooperate with Russian intelligence agencies, including but not necessarily limited to the FSB. While this doesn't make them unique, the extent to which their activities are driven by both personal greed and a state political agenda gives them one of the widest array of potential motivations of all the major cyber threat actors in the world. There is speculation that Evil Corp is simply a front organization for Russian intellgience, but it should be noted that they have stolen large sums of money from their victims over their history of operations.

Common Tactics, Techniques and Procedures (TTPs)

Evil Corp have oeprated a number of prominent malware and ransomware variants over their history and as such, the list of tactics, techniques and protecures (TTPs) they leverage is wide. They have a wide variety or technical capabilities due to both their in-house capabilities as well as the relationships they have with other cybercriminal groups. They often leverage the very common tactic of phishing as wll as the use of legitimate security tools and living-off-the-land techniques. A list of the tactics and techniques used by Evil Corp mapped against the MITRE ATT&CK framework can be found here. The company Crowdstrike has described some of their TTPs associated with "big game" targeting and BitPaymer in this report. Mandiant has also examined some of their TTPs asssociated with Lockbit ransomware.

Tools and Weaponization

Evil Corp has been known to operate and maintain a number of propriatary malware variants over time which include the following:

- Dridex: Dridex malware initially developed as one of the most powerful financial trojans. It has evolved into a very powerful, general purpose, information stealer which has dynamic command and control capabilities, backdoor tactics and other post-exploitation functionality including dropping additional malware. Dridex was previously known as Bugat.
- Zeus: Zeus is one of the oldest banking trojans, known to operate since at least 2007 (some report as early as 2005). Due to its source code having leaked in 2011, several variants have since been developed which have seen its sophistication improve. Original versions of Zeus can be prevented by any number of signature-based detection technologies, however the code continues to be publicly available and new variants continue to be developed.

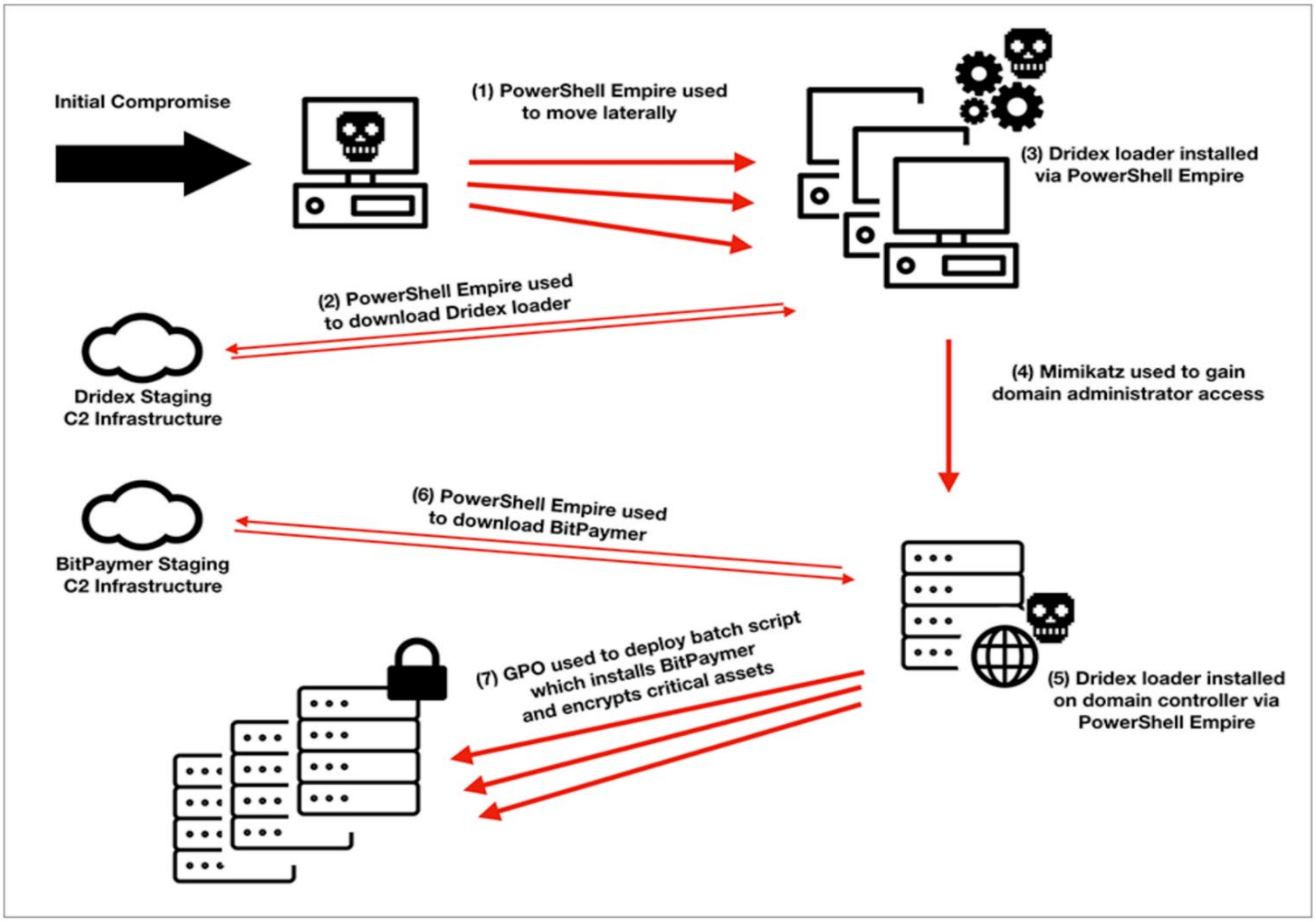
Initial Compromise
(1) PowerShell Empire used to move laterally
(3) Dridex loader installed via PowerShell Empire
(2) PowerShell Empire used to download Dridex loader
Dridex Staging C2 Infrastructure
(4) Mimikatz used to gain domain administrator access
(6) PowerShell Empire used to download BitPaymer
BitPaymer Staging C2 Infrastructure
(7) GPO used to deploy batch script which installs BitPaymer and encrypts critical assets
(5) Dridex loader installed on domain controller via PowerShell Empire

Figure 1: Diagram depicting Evil Corp cyberattack leveraging Dridex, several other tools and Bit Paymer ransomware, courtesy of CrowdStrike.

- GameOver Zeus: Gameover Zeus (or GOZ) is a Zeus variant (see above) that is built specifically to deliver ransomware as its payload. It is often spread via phishing campaigns.
- JabberZeus: Also known as AquaZeus, JabberZeus is a Zeus variant that includes a instant messenger plugin for the Jabber platform so that attackers can communicate and collaborate activity during an attack. JabberZeus operates from certain infrastructure, samples of which can be found here and here.
- Bitpaymer: Bitpaymer, also known as Doppelpaymer and FriedEx) is a ransomware that was developed by EvilCorp and has been known to be often dropped by Dridex and in operations since 2017. It has code similarities with Dridex.
- Hades: Hades is a ransomware variant that has been in operations since December 2020. Hades is believed to be a direct successor to Wastedlocker and is believed to have been deliberately developed by Evil Corp for the specific purposes of evading sanctions that were announced in 2019. It leverages TTPs that are distinct and despite many ransomware variants operating publicly and seeking affiliates and initial access brokers to partner with for attacks, Hades is operated privately.

- Phoenixlocker – Also known simply as Phoenix, Phoenixlocker is a ransomware variant developed by Evil Corp in 2021 and suspected to be part of their effort to evade sanctions issued in 2019. It's designed to look like another hacker group – Payloadbin.
- SocGholish – Also known as FAKEUPDATES, SocGhoulsih is a framework of social engineering toolkits used to drop malicious code by phony software updates as well as infected websites. Some of these phony updates are known to mimic browser, Flash and Microsoft Teams updates.
- Wastedlocker – Wastedlocker is a ransomware variant believed to be operational since May of 2020. It's often used in multi-stage attacks and is associated with ransom demands ranging from $500,000 to more than $10 million.

As previously mentioned, Evil Corp have a wide set of highly-capable tools at their disposal. These are developed and maintained in-house, but are often used in conjunction with commodity malware, living-off-the-land techniques and common security tools that were designed for legitimate and lawful security assessments. Common characteristics exist between Evil Corp's in-house tools and they are depicted by the Venn diagram below:

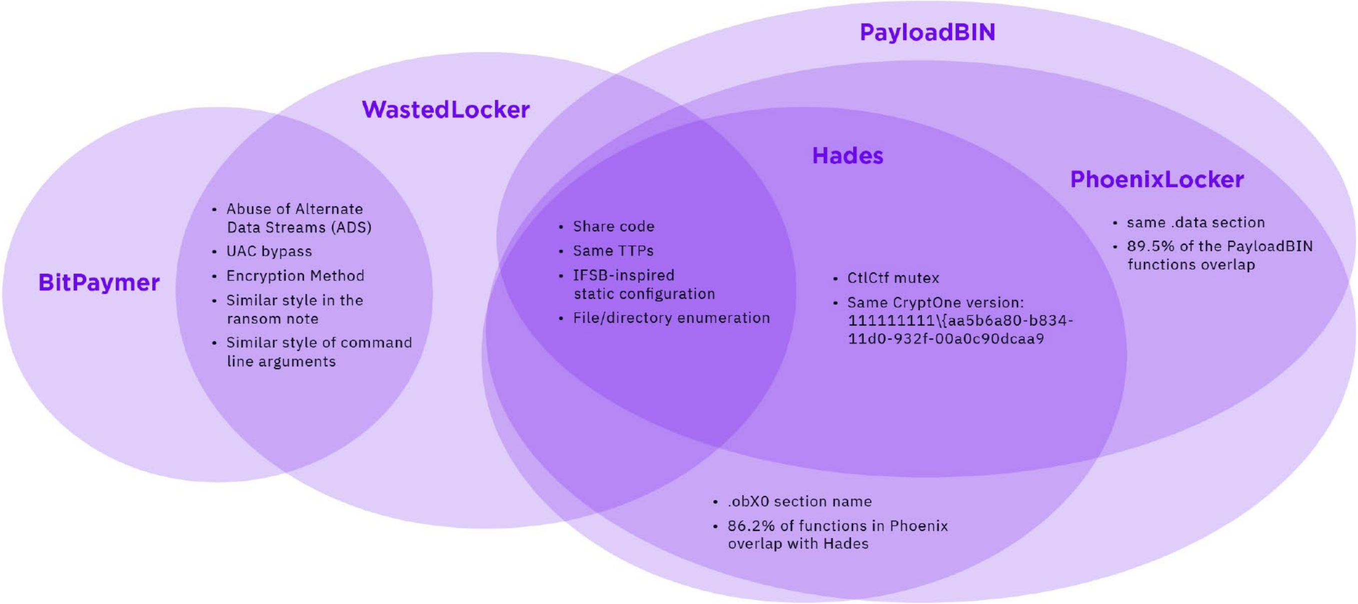
PayloadBIN
WastedLocker
Hades
PhoenixLocker
BitPaymer
• Abuse of Alternate Data Streams (ADS)
• UAC bypass
• Encryption Method
• Similar style in the ransom note
• Similar style of command line arguments
• Share code
• Same TTPs
• IFSB-inspired static configuration
• File/directory enumeration
• CtlCtf mutex
• Same CryptOne version: 111111111\{aa5b6a80-b834-11d0-932f-00a0c90dcaa9
• same .data section
• 89.5% of the PayloadBIN functions overlap
• .obX0 section name
• 86.2% of functions in Phoenix overlap with Hades

Figure 2: A Venn diagram depicting overlapping characteristics of Evil Corp's arsenal of cyber weapons, courtesy of Sentinel Labs.

Evil Corp has also been known to use other commodity malware variants as well as publicly-available tools in their attacks including:

- Cobalt Strike
- Covenant
- Donut
- Koadic
- Mimikatz
- Powershell Empire

- PowerSploit

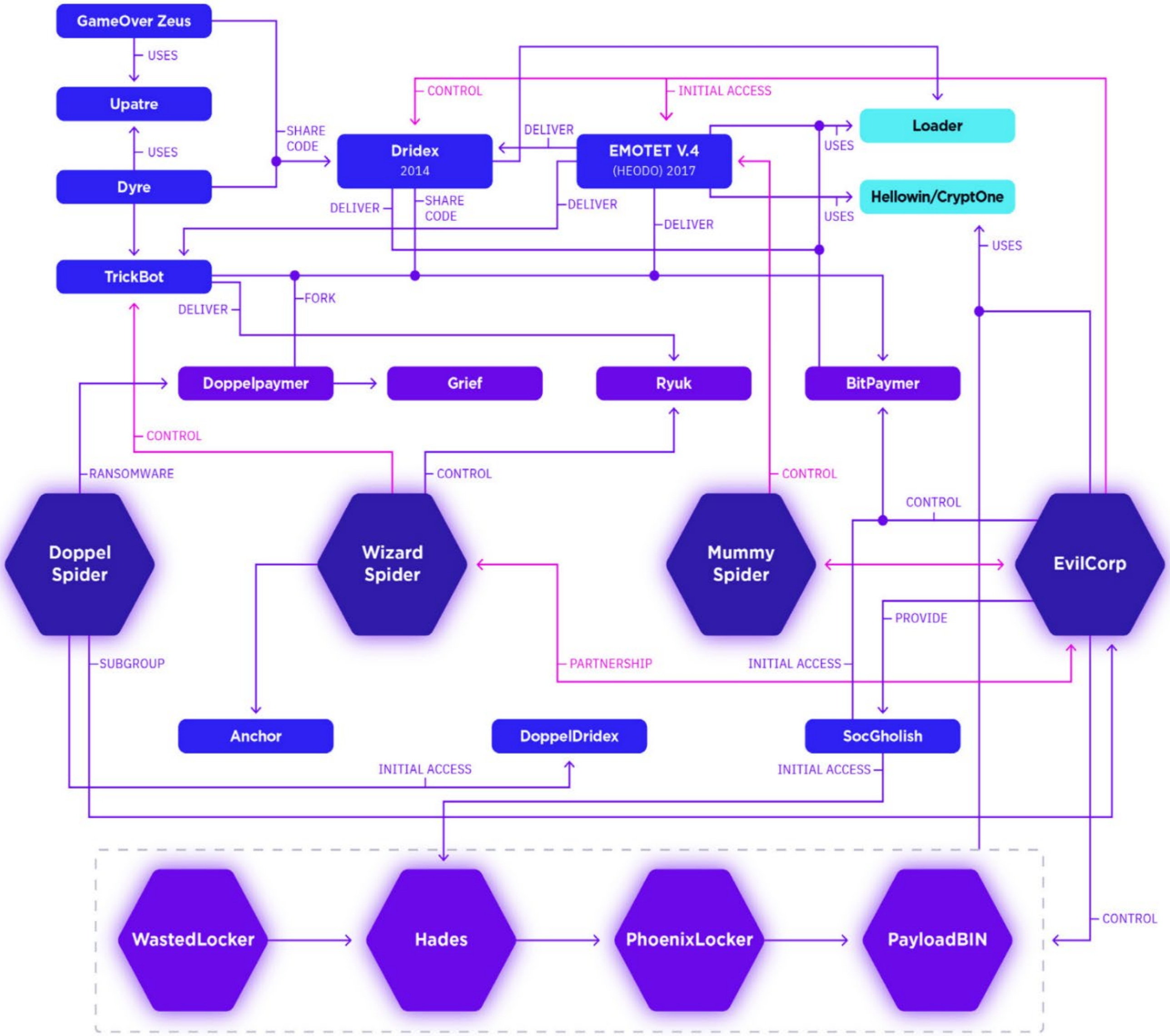

Figure 3: A diagram depicting the relationships between Evil Corp and other major cybercriminal ecosystem actors, courtesy of Sentinel Labs.

Relationships

Evil Corp has strong and enduring relationships with many of the most capable and notorious cybercriminal gangs around the world. These malware and ransomware operators include Doppel Spider, Wizard Spider, Mummy Spider – all suspected to have members primarily in Russia but also the Commonwealth of Independent States. In addition to Evil Corp's in-house cyber weapon arsenal, they also by virtue of these relationships have access to prolific malware variants such as Trickbot and Emotet, as well as major ransomware operations such as Ryuk. These relationships, along with Evil Corp's in-house capabilities make them one of the world's most powerful criminal gangs. Many of these groups and malware variants have all been known to target the U.S. health sector agressively.

Targeting and Scope of Attacks

Evil Corp does not appear to have any geographic limitations on their targeting. Like many financially-motivated cybercriminals, they are ostensibly motivated to attack targets of opportunity. They have been known to engage in big game hunting: targeting larger organizations with deeper pockets. However, georgaphically, they do have a tendency to attack targets in the United States and Europe. In terms of sectors, they target finance, government, healthcare, media, transportation, instance, manufacturing, non-profits, technology and education. One of their more well-known attacks against the health sector was the compromise of several Scottish hospitals that are a part of the NHS Lanarkshire board in 2017 with the use of BitPaymer ransomware. The United Kingdom's National Crime Agency (NCA) Metropolitan Police Service arrested multiple individuals who contributed to the activities of Evil Corp.

Defense and Mitigations

It is not practical to attempt to lay out a comprehensive list of defense and mitigations recommendations and data for a group such as Evil Corp, which maintains a wide array of custom capabilities that are continually being developed. Therefore, we will present a sample of mitigations, indicators of compromise, Yara rules and similar defensive information:

CISA Alert (AA19-339A) Dridex Malware
https://www.cisa.gov/uscert/ncas/alerts/aa19-339a

SANCTIONS BE DAMNED | FROM DRIDEX TO MACAW, THE EVOLUTION OF EVIL CORP
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp

CISA Ransomware Guide
https://www.cisa.gov/stopransomware/ransomware-guide

To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

DRIDEX and how to overcome it
https://www.symantec.com/connect/blogs/dridex-and-how-overcome-it

Appendix A: US Federal Government Announcements Related to Evil Corp

The following is a list of official actions taken by the U.S. federal government in an effort to counteract Evil Corp and their illicit activities:

Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware
https://home.treasury.gov/news/press-releases/sm845

Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware
https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens

DHS CISA, Alert (TA15-286A) Dridex P2P Malware
https://www.us-cert.gov/ncas/alerts/TA15-286A

FBI Most Wanted: EVGENIY MIKHAILOVICH BOGACHEV
https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

FBI Most Wanted: MAKSIM VIKTOROVICH YAKUBETS
https://www.fbi.gov/wanted/cyber/maksim-viktorovich-yakubets

THE MALWARE DRIDEX: ORIGINS AND USES
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

HADES ransomware operators continue attacks
https://www.accenture.com/us-en/blogs/security/ransomware-hades

Killing the Bear: Evil Corp
https://killingthebear.jorgetesta.tech/actors/evil-corp/

References

Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware
https://home.treasury.gov/news/press-releases/sm845

Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of “Bugat” Malware
https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens

To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

Dridex P2P Malware,” US-CERT Alert (TA15-286A)
https://www.us-cert.gov/ncas/alerts/TA15-286A

“Dridex Threat Profile,” New Jersey Cybersecurity & Communications Integration Cell
https://www.cyber.nj.gov/threat-profiles/trojan-variants/dridex

WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

Alert Logic, “Dridex malware has evolved to Locky Ransomware,”
https://www.alertlogic.com/resources/threat-reports/dridex-malware-has-evolved-to-locky-ransomware/

Dridex (Bugat v5) Botnet Takeover Operation
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

Cops Knock Down Dridex Malware that Earned 'Evil Corp' Cybercriminals At Least $50 Million
https://www.forbes.com/sites/thomasbrewster/2015/10/13/dridex-botnet-takedown/#2b883f00415b

Recorded Future - Dark Covenant: Connections Between the Russian State and Criminal Actors
https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf

DHS CISA, Alert (TA15-286A) Dridex P2P Malware
https://www.us-cert.gov/ncas/alerts/TA15-286A,

Dridex still active after takedown attempt
https://www.securityweek.com/dridex-still-active-after-takedown-attempt

How the Dridex Gang makes millions from bespoke ransomware
https://www.forbes.com/sites/geoffwhite/2018/09/26/how-the-dridex-gang-makes-millions-from-bespoke-ransomware/

Cybercrime Technical Desk Reference
https://www.cisecurity.org/wp-content/uploads/2018/09/MS-ISAC-Cyber-Crime-Technical-Desk-Reference.pdf

Dridex: Tidal waves of spam pushing dangerous financial Trojan
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf

FriedEx: BitPaymer ransomware the work of Dridex authors, welivesecurity by ESET, 26 January 2018,
https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/

Dridex Campaigns Hitting Millions of Recipients Using Unpatched Microsoft Zero-Day
https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day

High-Volume Dridex Banking Trojan Campaigns Return
https://www.proofpoint.com/us/threat-insight/post/high-volume-dridex-campaigns-return

Threat Actor Profile: TA505, From Dridex to GlobeImposter
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter

New year, new look – Dridex via compromised FTP
https://blogs.forcepoint.com/blog/security-labs/new-year-new-look-dridex-compromised-ftp

DRIDEX and how to overcome it
https://www.symantec.com/connect/blogs/dridex-and-how-overcome-it

URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-

linked-by-a-similar-loader/

Threat Spotlight: Spam Served With a Side of Dridex
https://blogs.cisco.com/security/talos/spam-dridex

SocGholish
https://redcanary.com/threat-detection-report/threats/socgholish/

Are Evil Corp Actually Russian Spies?
https://www.truesec.com/hub/blog/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies

FBI Most Wanted: EVGENIY MIKHAILOVICH BOGACHEV
https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

Dridex (Bugat v5) Botnet Takeover Operation
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

THE MALWARE DRIDEX: ORIGINS AND USES
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

FriedEx: BitPaymer ransomware the work of Dridex authors
https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/

ZeuS, Still Alive and Kicking in the Form of Jabber ZeuS?
https://circleid.com/posts/20210610-zeus-still-alive-and-kicking-in-the-form-of-jabber-zeus

Exposing a Currently Active "Jabber ZeuS" also known as "Aqua ZeuS" Gang Personal Email Portfolio - An OSINT Analysis
https://ddanchev.blogspot.com/2022/01/exposing-currently-active-jabber-zeus.html

Inside the Hunt for Russia's Most Notorious Hacker
https://www.wired.com/2017/03/russian-hacker-spy-botnet/

What Is GameOver Zeus (GOZ)?
https://www.proofpoint.com/us/threat-reference/gameover-zeus-goz

HADES ransomware operators continue attacks
https://www.accenture.com/us-en/blogs/security/ransomware-hades

Killing the Bear: Evil Corp
https://killingthebear.jorgetesta.tech/actors/evil-corp/

WastedLocker malware analysis
https://seguranca-informatica.pt/wastedlocker-malware-analysis/#.YfAaIRUITTY.twitter

Increase In Drive-by Attack: SocGholish Malware Downloads https://www.menlosecurity.com/blog/increase-in-attack-socgholish

SocGholish Campaigns and Initial Access Kit
https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback