ankura

A Cyber Threat Analysis of the Russia-Ukraine Conflict

February 28, 2021

Washington, DC
2000 K Street NW, 12th Floor
Washington, DC, United States 20006
+1.202.797.1111

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Ankura Cyber Threat Investigations & Expert Services (CTIX) team conducted a technical analysis of historical and ongoing adversarial activity associated with the current Ukrainian/Russian conflict. In doing so, the CTIX team leveraged proprietary sources of threat intelligence which were then enhanced with additional data points collected from various open and closed sources. This report showcases identifiable cybersecurity risks at the center of the Ukraine-Russia conflict and corresponding actionable threat intelligence.

Several of the most pertinent findings include:

- It is evident that Russia has been employing cyberattacks as a key strategy in the invasion of Ukraine, including destructive malware, Distributed Denial-of-Service (DDoS) attacks, and misinformation tactics
- There are key threat actor groups actively involved in executing cyberattacks on behalf of Russia – or at the very least sympathize with Russian endeavors – including Conti, The Sandworm Team, Ghostwriter, Energetic Bear, and Primitive Bear
- Techniques that will likely be used by Russian threat actors in the future include ransomware, DDoS, wiper malware, phishing, and cyber-espionage
- Malware that has been deployed and will likely be leveraged by Russian threat actors in the future includes WhisperGate, HermeticaWiper, Pterodo, Cyclops Blink, and SaintBot
- The widespread Log4j vulnerabilities exploited to wreak havoc on organizations across 2021 have likely been exploited by Russian threat actors before the start of the invasion, and the foothold gained will likely be used as an advantage in retaliatory attacks against Ukraine and its allies in the future
- It is difficult to predict how Russian attacks in the future might ensue; however, ransomware attacks will likely increase with a high possibility of cyberattacks targeting critical infrastructure of Russian adversaries

The report below includes a more comprehensive review of all medium/high confidence intelligence collected and analyzed by CTIX analysts. It is important to keep in mind that this conflict is extremely dynamic, and new developments are being identified in real-time. The Ankura CTIX team will continue to monitor this crisis and all of the actors involved to provide as much perspective as possible.

To stay up to date on the latest cyber threat activity, sign up for our weekly newsletter: the Ankura CTIX FLASH Update.

THE TACTICS, TOOLS, AND ACTORS INVOLVED

With the onset of the Russian invasion into Ukraine, this conflict gives insight into what a modern conventional war between near-peer adversaries looks like. More specifically, this conflict details the role of cyber warfare and how it affects the battlespace. Over the past two months, Ukraine has suffered multiple cyber-attacks ranging from disinformation campaigns to the largest distributed denial-of-service (DDoS) attack Ukraine has seen to date. While not every attack has been officially attributed, it can be said with high confidence that Russian state-sponsored threat actors and allies are responsible.

In this report, Ankura CTIX analysts paint a picture of the ongoing cyber warfare by providing detailed metrics surrounding the specific threat actors identified and/or suspected of attacking Ukrainian assets and infrastructure, as well as the tactics, techniques, and procedures (TTPs) employed by those attackers. The Russian threat actor known as Conti has officially voiced its support for the Russian invasion and has warned that any western nation conducting cyber warfare operations against Russian assets will suffer massive takedowns of critical infrastructure. The Sandworm Team attributed to Russia's General Staff Main Intelligence Directorate (GRU) has also been attributed to reintroducing the NotPetya wormable malware strain, as well as leveraging the Cyclops Blink Linux botnet, to target internet-of-things (IoT) devices to

execute distributed denial-of service (DDoS) attacks. The notorious Belarusian anti-North American Treaty Organization (NATO) threat actor UNC1151 has also been busy with the reimagining of their Ghostwriter campaign, a cyber-espionage and misinformation attack that sends spoofed emails to persons of interest, defaces government officials' private social media pages, as well as defaces both government and private websites. Finally, PrimitiveBear (AKA Shuckworm or Garmaredon), a hacking group attributed to the Russian Federal Security Service (FSB), has also been facilitating a cyber-espionage campaign targeting Ukraine.

A Recent Timeline of Cyber Threat Activity in Ukraine

Ukraine began to see cyber-attacks in January 2022, just two months after Russia began to amass troops along the Ukrainian border. The first cyberattack occurred on January 13th and was dubbed WhisperGate. Microsoft had identified that WhisperGate used malware designed to look like ransomware; however, it lacked a recovery key.[1] In other words, WhisperGate was intended to be destructive in nature by destroying data on infected machines without the chance of recovery, rendering critical devices, networks, and infrastructure completely useless. It is important to note that, at the time of publication, this attack has yet to be attributed to a specific threat actor.

Just one day after WhisperGate was made known, there were numerous attacks on various Ukrainian government websites. It was reported that "over 70 Ukrainian government websites were defaced with political imagery and a statement in Russian, Ukrainian, and Polish".[2] Based on our analysis, the intent of this attack appears to be an effort to destabilize and spread chaos among Ukrainian civilians. This follow-on attack has been attributed to Belarus' advanced persistent threat (APT) Group – UNC1151.[1]

The second series of attacks started in mid-February 2022, a little more than one week before Russian forces crossed the Ukraine border. On February 15-16th, Russia was attributed to "Ukraine's largest DDoS attack to date," which "impacted sites such as the Defense Ministry, and the two largest state banks."[1] On the same day, Ukraine saw a smishing disinformation campaign, where "customers of the largest state-owned bank received SMS messages about technical malfunctions of ATMs"[1] that were later confirmed by Ukrainian Cyber police to be false.

The final string of attacks occurred on the first days of the invasion of Ukraine. On February 23rd, Russia was attributed to another DDoS attack in which "websites such as the Ministry of Defense, Ministry of Foreign Affairs, Security Service and Cabinet of Ministers became inaccessible for several hours and faced latency outages for several days."[1] On that same day, Ukraine saw a new malware coined HermeticWiper that has yet to be attributed that led to "… numerous organizations in Ukraine have been hit, infecting hundreds of computers. This destructive malware is able to delete or corrupt data on the infected machine."[1] Shortly after that, the Kyiv Post reported that their site was "under constant cyberattack the moment Russia launched its offensive campaign".[1]

Threat Actors of Interest

CTIX analysts have determined that various threat groups associated with this conflict must be monitored while the war between Ukraine and Russia remains ongoing and global tensions continue to rise without a resolution in sight. With the following threat groups' historical targeting of the region, CTIX analysts predict that campaigns from these actors will continue to exploit the region with cyberattacks and cyber-espionage campaigns to create friction for Ukraine and its western allies. Indicators of compromise related to the threat actors of interest and their associated campaigns are listed below in the *Indicators of Compromise* section.

Conti

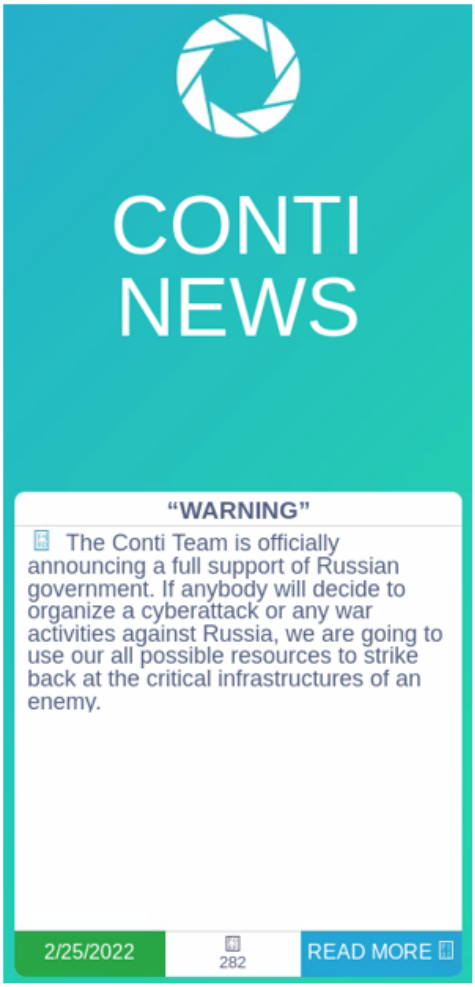
Looking back at the months prior to the invasion of Ukraine, the exploitation of the Log4j vulnerability by a wide array of threat actors was running rampant and led to more successful exploitations than any other vulnerability in 2021. The fallout from the Log4j exploits was monitored for months and even into the new year; however, CTIX analysts expected the outcome of such a widespread vulnerability to be much worse than it ended up being. In December 2021, the Russian ransomware gang Conti attempted to exploit Log4j,

[1] https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks

as an attack method for ransomware deployment. After the successful exploitation, the actors would move laterally across the target network with cobalt strike, which ultimately led to the execution of their ransomware payload. Log4j being utilized in the ransomware scene was very short lived as it did not prove viable enough as an attack vector. Ultimately, it did not provide Conti with the lateral movement they hoped to achieve, and the affected servers were deemed unworthy to exploit with ransomware from a financial perspective.

Conti utilizing Log4j as an attack vector indicates that the Russian government was/is aware of the exploit and had the capabilities to execute it successfully. Due to this, CTIX analysts can predict with high confidence that Russian threat actors have already exploited the Log4j vulnerability within Ukraine, laterally moved, and have been sitting dormant, waiting to strike against Ukraine and its allies when further sanctions are levied against Russia. Additionally, once the applied sanctions start to take a toll on the Russian economy , groups like Conti will likely have to return to conducting financially-motivated cybercrime and ransomware operations to keep supporting their activities.

In recent news, the Conti team also announced on February 25th that they are “officially announcing a full support of Russian government” and “If anybody will decide to organize a cyberattack or any war activities against Russia, [they] are going to use all possible resources to strike back at the critical infrastructures of an enemy.” Conti’s statement regarding this conflict confirms our analysts’ assumptions that attacks are imminent and on the rise.



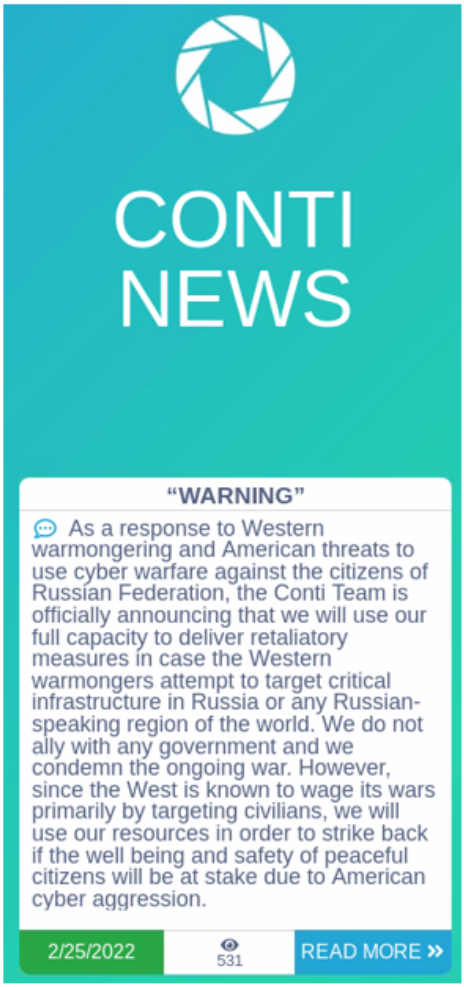


FIGURE 1: CONTI’S FEBRUARY 25TH ANNOUNCEMENT
FIGURE 2: CONTI’S UPDATED FEBRUARY 25TH ANNOUNCEMENT

Sandworm

The Sandworm Team (AKA Voodoo Bear) is one of Russia's most influential state-sponsored advanced persistent threats (APT).[3] Sandworm has been active since at least 2015 and is attributed to Russia's General Staff Main Intelligence Directorate (GRU). The team's first major attack utilized the BlackEnergy malware, a botnet used by cybercriminals and APTs alike, to target Ukrainian electricity infrastructure and media companies. They made a name for themselves by writing and executing the NotPetya malware in 2017. This malware attack targeted Ukrainian businesses and included a worm component that quickly spread across networks. The attack not only devastated Ukraine, but also spread across the world to many industry giants, causing over $1 billion in damages.[4] Sandworm's newest threat involves the use of the Cyclops Blink botnet. This Linux botnet has been active since June 2019 and targets small and home office devices. It is capable of large-scale DDoS attacks and grants the team initial access into many networks across the country. A technical analysis of this malware is included in the *Malware of Interest* section below. The Sandworm Team has shown they are capable of sophisticated, persistent, and destructive attacks against Russian opponents.

Ghostwriter

Ghostwriter, first discovered in July of 2020, started as a political misinformation campaign that targeted victims in Lithuania, Latvia, and Poland. Researchers have stated that this threat group has been actively targeting said countries since 2017 and has been involved with anti-NATO disinformation campaigns, cyber espionage, and political damage all throughout Europe.[5,6] According to FireEye, a portion of the Ghostwriter campaign involves gaining access to critical news sites' publishing systems, deleting stories, and replacing them with spoofed content that sought to undermine NATO's power in Eastern Europe through the spread of false information.[7] In an update, FireEye added that Ghostwriter's tactics mainly consist of defacing social media accounts that are associated with well-known Polish officials. The takeover of these high-profile social media accounts allows access to the users' email accounts, which can then reveal communications associated with potential campaign targets.[8] Misinformation is posted using these compromised accounts and enforces a negative stance on political officials as well as current events. Ghostwriter has been known to develop and run their own false news websites that appear to be legitimate for the purpose of regularly dispersing similar misinformation. While Ghostwriter is not the most technically sophisticated threat group, they are a force to be reckoned with regarding social engineering campaigns.[9] Ghostwriter is motivated by dispersing fear to the public, and the threat group is known to feed off current crisis events and national matters as well as take advantage of the chaos. Their aim is to target western audiences and promote a false narrative about Ukraine and its Western allies.

While Ghostwriter has not been active for some time, a group has been discovered that shares similar TTPs. In a report from Mandiant, the threat group named UNC1151 has been linked to Ghostwriter campaigns with moderate confidence.[10] This is notable as UNC1151 has conducted multiple operations since the start of the Russia-Ukraine conflict. Their first attack defaced multiple Ukrainian government websites, including the Ministry of Foreign Affairs, Education and Science, the Cabinet of Ministers, and the State Emergency Service.[11] They have continued their attacks by launching a phishing campaign against Ukrainian military personnel.[12] These attacks indicate that the operators behind Ghostwriter have not stopped their relentless attacks against Russian opponents. It is important to understand the TTPs of misinformation-spreading threat groups to better identify their motivations and future attack methods.

Energetic Bear

Energetic Bear (AKA Berserk Bear) is a Russian state-sponsored APT cyber espionage group. Known for a variety of campaigns in the last decade, including Dragonfly, Dragonfly 2.0, and Palmetto Fusion,

---

[2] https://attack.mitre.org/groups/G0034/
[3] https://resources.infosecinstitute.com/topic/apt-sandworm-notpetya-technical-overview/
[4] https://www.mandiant.com/resources/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity
[5] https://techcrunch.com/2021/09/24/european-council-russia-ghostwriter/
[6] https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf
[7] https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/unc1151-ghostwriter-update-report.pdf
[8] https://www.wired.com/story/ghostwriter-hackers-belarus-russia-misinformationo/
[9] https://www.mandiant.com/resources/unc1151-linked-to-belarus-government
[10] https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/
[11] https://thehackernews.com/2022/02/russia-ukraine-war-phishing-malware-and.html

Energetic Bear has repeatedly targeted government and industrial control system (ICS) networks in a series of attacks. This long list of affected industries includes electrical entities, fossil fuel infrastructure, education, pharmaceutical, aviation, and various levels of government networks.[13,14] An interesting and concerning aspect of these attacks is when Energetic Bear had access to control systems in these environments, they did not attempt to use them. In fact, they actively worked against inadvertently causing issues that would allow people to take notice of their activities on the server, such as avoiding the use of one of their older pieces of malware (Havex) in later attacks. [14,15] It is believed that the goal was to instead prepare for future attacks against these networks and industries, gather information, and prepare malware to take control in the future. Using a series of remote access tools combined with Energetic Bear's apparent push to gather legitimate credentials for later use, this appears to be more of a possibility.

Energetic Bear's technical prowess is well documented. A tried and tested method employed by the threat group includes heavily targeted phishing and spear-phishing attacks towards organizations and individuals. These could take the form of informative industry-related infographics or crafted resumes/job search postings to draw in certain individuals. Files using the tool "Phishery," when interacted with, inject resources that allow for network infiltration. Energetic Bear often paired this attack vector with one of their most popular methods, Watering Hole Attacks (WCS), and specifically utilized this combination in the attacks on recent aviation targets[13]. Specifically, in 2019, the TYPO3 Content Management System was compromised to modify JavaScript objects[16], usually "/typo3conf/ext/t3s_jslidernews/res/js/jquery.easing.js". This then prompts an external authentication attempt[14]. Using these techniques together, Energetic Bear could then attempt to gather legitimate credentials to leverage further access into an organization.

On top of WCS attacks, the use of multiple Microsoft vulnerabilities has also allowed the threat group to compromise networks. One specific vulnerability is CVE-2020-0688, which allows threat actors to remotely execute code on unpatched Microsoft Exchange Servers.[13] It was discovered that networks were being scanned specifically for this vulnerability. When found, they were targeted by Energetic Bear, allowing access to email servers and the ability to execute code with system privileges. Finally, one of the largest exploits employed by the threat group in recent years has been Zerologon (which is tracked as CVE-2020-1472). Using this vulnerability, threat actors can exploit Netlogon Remote Protocol to use unencrypted Netlogon sessions to brute force cryptographic keys. This is conducted in order to compromise authentication, which allows access to Microsoft Active Directory and then escalates their privileges.[13,17] This privilege escalation vulnerability has allowed Energetic Bear to compromise networks, and further use them to propagate attacks.[18] It is believed, at this time, that Energetic Bear is using compromised infrastructure almost exclusively to continue their expansion.[19] The use of compromised systems to further expand operations is an effective tactic that also helps to further obfuscate Energetic Bear. It has been discovered that the threat group used their privilege escalation and credential grabbing abilities to gain direct access to control systems. Energetic Bear has even been identified by researchers "screenshot[ing] control panels of circuit breakers."[15] This reconnaissance effort only further lends credence to the idea that Energetic Bear is simply waiting to activate plans and systems they have compromised when the command is given.

Primitive Bear

Primitive Bear, commonly referred to as Shuckworm and Garmaredon, are a cyber-espionage-driven threat group whose alliance falls within the Russian Federal Security Service (FSB) and primarily targets Ukrainian entities. Historically, Primitive Bear actors have been around since 2013 and focus on exploiting Ukrainian military and national security establishments in their campaigns, committing espionage, and relaying intelligence back to threat actor infrastructure. Techniques commonly used by the organization are exfiltration over command-and-control (C2), file copy and extraction, peripheral device discovery, credential harvesting, and gathering system hardware specifications. Operations conducted by these actors have significantly picked up since tensions between Russia and Ukraine have escalated. Recently, Primitive Bear

[13] https://www.cisa.gov/uscert/ncas/alerts/aa20-296a
[14] https://vblocalhost.com/uploads/VB2021-Slowik.pdf
[15] https://www.wired.com/story/berserk-bear-russia-infrastructure-hacking/
[16] https://twitter.com/drunkbinary/status/962689310855221248
[17] https://www.crowdstrike.com/blog/cve-2020-1472-zerologon-security-advisory/
[18] https://theintercept.com/2020/12/17/russia-hack-austin-texas/
[19] https://blog.gigamon.com/2021/10/25/bear-in-the-net-a-network-focused-perspective-on-berserk-bear/

again targeted Ukraine with a phishing campaign that deployed a customized set of Pterodo malware variants and persistence mechanisms.

Previous campaigns undertaken by Primitive Bear actors targeted Ukrainian users with government-themed phishing emails laced with scripts to determine the viability of the target for second-stage deployments. While threat actors favor sets of malicious programs, Primitive Bear actors have also incorporated living-off-the-land tactics in their espionage operations to further compromise their subjected targets. Payloads attributed to the group utilized self-extracting archives (SFX) to deploy the Remote Manipulator System access tool and batch scripts to execute the malicious code. Additionally, these payloads have been known to communicate with C2 endpoints to pull down additional payloads depending on the system.

Advanced spear phishing attempts have also been observed, carrying weaponized Office documents capable of deploying injectors to establish a remote connection to actor-controlled C2 servers. Once compromised, these actors have been known to establish system persistence and move to lateral targets within the compromised infrastructure. Recent campaigns carried out by Primitive Bear incorporate a variety of malicious techniques and applications to exploit their targets. These phishing campaigns targeting Ukrainians and high-level assets are loaded with modernized Pterodo/Pteranodom malware, Remote Manipulator System variants, and UltraVNC remote connection software. Compromise from these campaigns, which have targeted governments and companies throughout the region, would leave the victim's machine in the hands of espionage-hungry Primitive Bear actors and feed their ambition for Ukrainian intelligence.

Malware of Interest

CTIX analysts have determined that the malware strains utilized in the cyberattacks conducted against Ukraine are a combination of known strains already attributed to Russian threat actors, their allies, and new strains that are very similar to malware sets used in previous pro-Russian hacking campaigns. The most destructive malware campaigns so far have deployed wiper-based malware, sophisticated backdoor malware used to collect sensitive information for the purpose of cyber-espionage, and cutting-edge botnets used to conduct DDoS campaigns. Indicators of compromise related to the malware of interest are listed below in the *Indicators of Compromise* section.

WhisperGate

The Computer Emergency Response Team of Ukraine (CERT-UA) released a report on January 26th, 2022, stating that on the morning of January 14th, many Ukrainian government websites were targeted by malicious actors, which resulted in the websites having their content altered and systems destroyed.[20] The threat actors defaced websites by accessing legitimate accounts through a Tor connection. The attack, now known as WhisperGate, targeted government, non-profit, and information technology entities in Ukraine. Similar to the NotPetya wiper that targeted Ukraine in 2017, WhisperGate hid under the guise of ransomware but, once activated by the threat actor, would result in the destruction of the targeted systems. The malware is made up of three (3) separate components that work in conjunction:

1. **BootPatch:** The malware that destroys the Master Boot Record (MBR), renders a system unbootable, and creates a fake ransom note. This malware works in various directories, including "C:\PerfLogs", "C:\ProgramData", "C:\", and "C:\temp", under the name stage1.exe.
2. **WhisperGate:** A payload downloaded from Discord that drops additional dynamic link libraries (DLLs), one of which is a legitimate tool that allows all components of the malware to hide from Windows Defender.
3. **WhisperKill:** This component enumerates the connected drives and their content. When executed in memory, the malware locates files in predefined directories that match a list of predefined file extensions and corrupts them by overwriting the contents of the file with a fixed number of "0xCC" bytes. After the contents have been overwritten, the files are renamed with four-byte extensions.

WhisperGate abused the supply chain and two (2) different vulnerabilities to gain access to targeted organizations. The first vulnerability, Log4j, is a Java Naming and Directory Interface (JNDI) injection flaw

[20] https://cert.gov.ua/article/18101

that targets a widely used Java-based logging library and was first seen in early December 2021. The second vulnerability identified as a likely entry point was the OctoberCMS vulnerability, which gives an actor the ability to bypass authentication and take over a user account on OctoberCMS servers. On January 15th, 2021, Microsoft attributed the WhisperGate malware family to DEV-0586 APT group[21].

HermeticaWiper

On February 23rd, 2021, a wiper-based malware was discovered attacking hundreds of Ukrainian, Lithuanian, and Latvian computers. This malware, known as HermeticaWiper, was discovered shortly after a series of distributed denial-of-service (DDoS) attacks disrupted services to several Ukrainian governmental and banking websites on Wednesday. The affected sites include, but are not limited to, the online portals for the Ukrainian Ministry of Foreign Affairs, Cabinet of Ministers, and Rada (Ukrainian Parliament). First detected by ESET products as KillDisk.NCV, the data wiper was named HermeticWiper for the use of a genuine code signing certificate assigned to a company known as Hermetica Digital Ltd.

The malware, which targets primarily Windows systems, is comprised of two (2) components:

1. Targeting the Master Boot Record (MBR), similar to WhisperGate
2. Targeting disk partitions

The malware begins by gaining SeShutDownPrivilege, which allows for the code to shut down the endpoint once the drives are wiped, and SeBackupPrivilege, which allows for retrieval of file contents. Once the MBR is corrupted for every physical drive, HermeticWiper enumerates individual partitions as well as corrupts the data after destroying the shadow copy and other files required for system operations. The corruption occurs by abusing legitimate drivers from the EaseUS Partition Master software, specifically the "empntdrv.sys" driver.[22] The malware also modifies registry keys, such as the "SYSTEM\CurrentControlSet\Control\CrashControl CrashDumpEnabled" key, so that crash dumps are disabled. To complete the wipe, the malware forces a system reboot[23]. Researchers from ESET and Sentinel Labs have found that the malware's original compilation date was December 28th, 2021, despite first being seen in the wild on February 23rd. This indicates that HermeticaWiper was a long-planned attack; a theory supported by the possibility of the threat actors having access to at least one (1) affected victim's Active Directory from which the malware was dropped. HermeticWiper appears to be a more sophisticated version of the WhisperGate malware and uses similar TTPs to ensure compromise. Several different

[21] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
[22] https://twitter.com/ESETresearch/status/1496581903205511181
[23] https://twitter.com/juanandres_gs/status/1496581710368358400

analysts and threat actors have been sharing the following infographic that breaks down HermeticWiper in an easy-to-understand method.

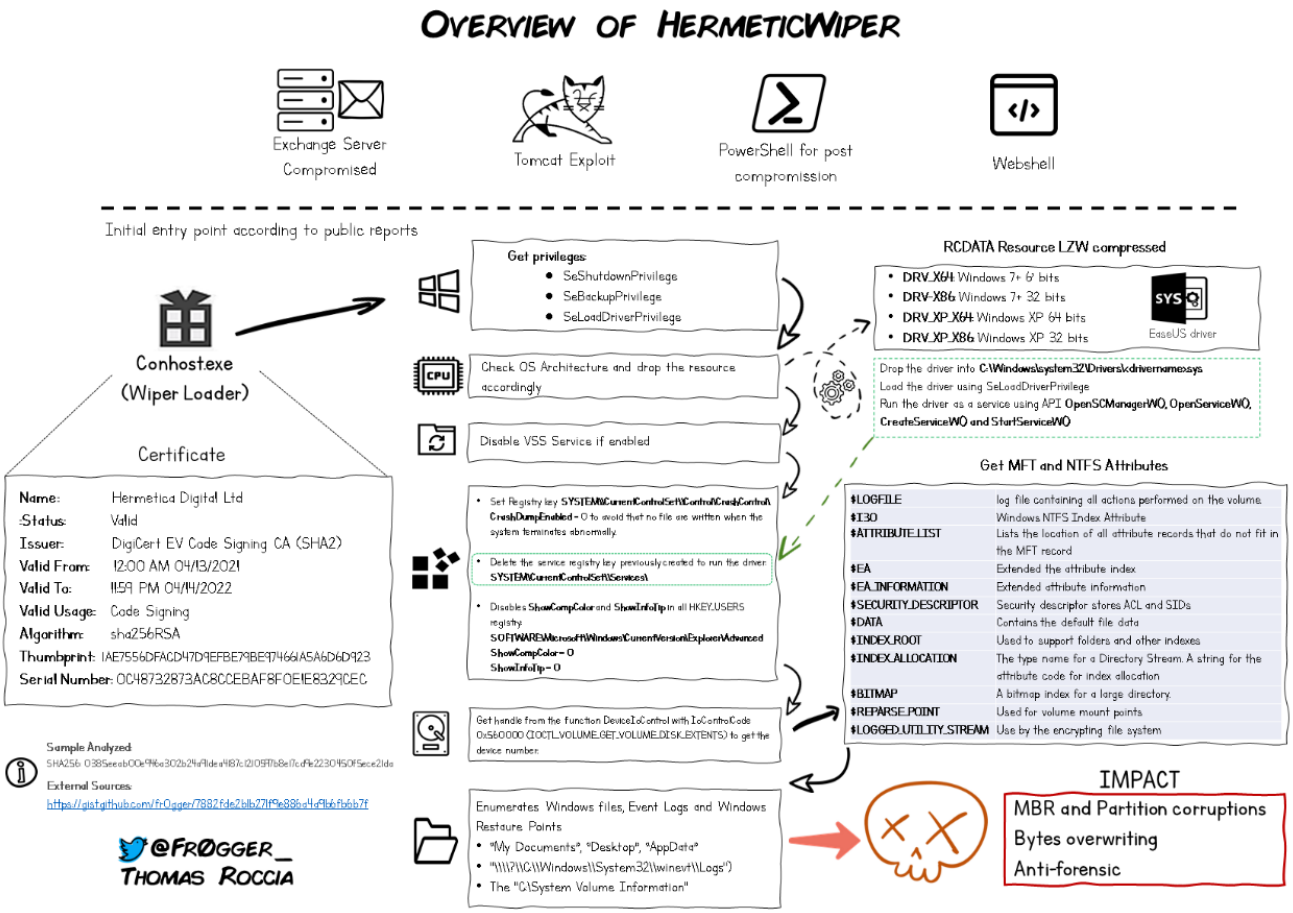


FIGURE 3: HERMETICWIPER BREAK DOWN SHARED ACROSS MULTIPLE MEDIAS[24]

Pterodo

Primitive Bear commonly deploys Pterodo malware onto the victim's device, which has evolved in its complexity over the past few years. Pterodo is historically a malicious Windows backdoor that has been modernized with the capability of generating a unique system URL that is based on the hard drive serial code, which will be utilized to establish a secure connection to a C2 endpoint. Once the link is established, threat actors analyze the infected device's communicated data, upload additional malicious scripts and files, and exploit the system further. The timeline of a Pterodo malware deployment is as follows:

1. User receives a phishing email with a malicious Microsoft Word document (.docx). Upon opening the file, embedded commands launch Pterodo from an infected Visual Basic Script (VBS) file named "depended.lnk".
2. Additional VBS scripts ("reflect.rar" and "deep-thought.ppt") are executed a short time later and a repeating system check module ("deep-thought.ppt") is executed every ten (10) minutes to verify actor persistence to the system.
3. Actors then utilize an HTA file in combination with the "mstha.exe" and "depended.exe" executables to bypass application control settings and browser security settings.
4. In parallel with the HTA file, a new variant of Pterodo is installed simultaneously from "depended.exe". Attackers continue to deploy new variants and system persistence module checks to ensure integrity.

[24] https://twitter.com/fr0gger_/status/1497121876870832128

5. Communications to the C2 server download additional collection scripts to the victim device. Programs then lay dormant (excluding module checks) until the threat actor access the system again.

Primitive Bear and its deployment of Pterodo are not to be underestimated, especially for organizations within the Ukrainian region. With rising tensions and the invasion of Ukraine territory, cyberattacks and other unconventional means of warfare will continue to be a rising threat.

Cyclops Blink

Cyclops Blink is a newly discovered large-scale malware botnet written and controlled by the Sandworm Team; a state-sponsored group affiliated with Russian intelligence. The malware targets small office and home office (SOHO) network devices. Cyclops Blink operators' initial attacks have consistently targeted the WatchGuard Firebox, a relatively cheap network firewall, though they will likely recompile the malware to a number of other devices.[25] The malware is a malicious Linux ELF executable file that runs as a core component with multiple modules spawned as child processes. The core component attempts to run as a process called "kworker", which is a legitimate process found on Linux machines. First, the malware modifies the "iptables" local firewall to allow TCP traffic to specific ports used for C2. It then starts four built-in modules that allow reconnaissance on the device, files to be uploaded and downloaded through the C2 server, store an up-to-date list of C2 server IP addresses, update Cyclops Blink, and maintain persistence. The core also handles communications with the C2 servers. For every beacon back to a C2 server, the malware selects a random destination from the list of addresses. Every message is encrypted with AES and has the encryption key randomly generated each time. The C2 network is tiered, with the clear net C2 servers routing information back to the main C2 interface on the dark web.

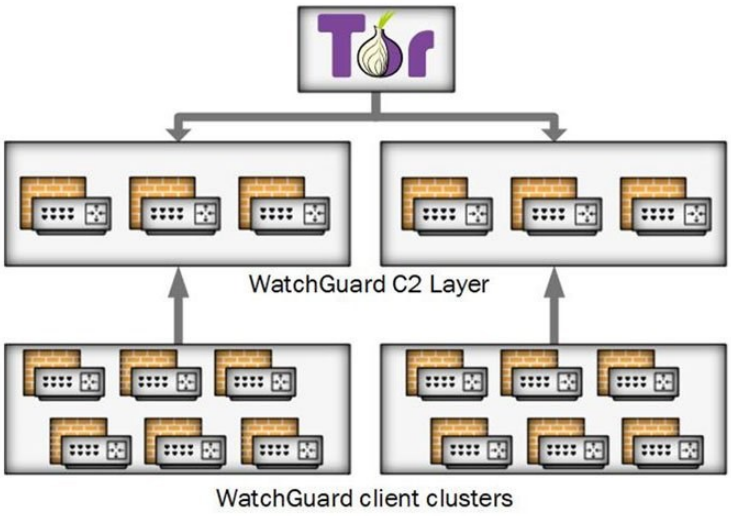


FIGURE 4: CYCLOPS BLINK C2 INFRASTRUCTURE[26]

This botnet has the potential to conduct destructive attacks against many well-protected targets. Distributed denial of service (DDoS) attacks have already been used, like with HermeticaWiper, to soften targets of more malicious attacks. In addition, this botnet provides the Sandworm Team with access to SOHO networks across the world. The Sandworm Team's previous use of the BlackEnergy botnet to devastate Ukrainian electric infrastructure has shown this group's strength and willingness to use botnets as a tool in their arsenal. WatchGuard has released a diagnosis and remediation plan along with three detection tools for businesses to utilize their Firebox firewalls.[27]

[25] https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
[26] https://thehackernews.com/2022/02/us-uk-agencies-warn-of-new-russian.html
[27] https://detection.watchguard.com/

SaintBot

SaintBot is a downloader botnet designed to infiltrate systems and then continue to deploy and execute different pieces of malware as directed by the C2 server. The primary method of deployment involves phishing emails. In January 2022, SaintBot was deployed using a phishing email impersonating the Ukrainian National Medical Service, and later in February as the Ukrainian Police.[28] This is especially concerning as it is spoofing trusted organizations in a time of crisis, leading to more people falling victim to these phishing emails. This malware is delivered via a zip file within the email and loaded with a PowerShell script which, when activated, downloads SaintBot from an embedded link. The process then downloads two (2) specific executables, "def.exe" and "putty.exe", and attempts to run them with elevated privileges.[29] "def.exe" disables Windows Defender and "putty.exe" is the main component of SaintBot. The main component is then copied into the Windows startup directory after it is renamed to a legitimate executable to avoid detection. During the first run, it injects itself into the "ehStorAurhn.exe" executable and connects to the C2 server. Currently, SaintBot is employing "locale identifier" (LCID)[30] to prevent from executing in Russia and some direct allies.[31] Oddly enough, Ukraine's LCID was on the exclusion list of the SaintBot attack in January, though this may have been a mistake. By impersonating these types of organizations and its versatile nature of being able to download and execute many types of malware, SaintBot poses a significant threat to a wide variety of organizations and networks.

PREDICTIONS FOR FUTURE CYBER THREAT ACTIVITY

With consideration that the United States and other powerful western allies levied substantial economic sanctions against Russia, it is inevitable that the conflict will put a strain on the Russian economy and there will likely be a surge in cyber-extortion tactics. With the ruble falling to the lowest price it has ever been compared to the US dollar, it is only a matter of time before the attacks are on the rise again. Due to the sanctions and other public retaliation from around the world, Russia has also begun to convey a victim stance - especially from a cyber perspective - and is using it to justify their offensive operations.

DDoS and ransomware attacks by Russian-associated threat groups are expected to be on the rise. These campaigns have been known to cripple entire networks for a substantial amount of time, rendering critical services inoperable until the flood of network packets subside, or a ransom is paid. Furthermore, should a company fall victim to ransomware attacks, there is a high likelihood that threat actors will not keep their integrity post-ransom payment and may continue to extort the victim with more payment demands or fence the stolen assets across forums and marketplaces. In addition to ransomware increases, critical infrastructure organizations must be prepared for cyberattacks against their industry and ensure that their technological infrastructure is secured and patched to limit access. The return of these attack vectors is inevitable and will be at the hands of ruthless threat actors whose alliances fall with the enemy.

Recommended Hardening Techniques

Below, CTIX analysts have documented actionable steps that organizations around the world should implement to harden their cyber resilience in the face of a heightened and ever-evolving cyber threat landscape.

[28] https://blog.trendmicro.co.jp/archives/30466
[29] https://blog.malwarebytes.com/threat-intelligence/2021/04/a-deep-dive-into-saint-bot-downloader/
[30] https://docs.microsoft.com/en-us/globalization/locale/locale-names
[31] https://blog.malwarebytes.com/threat-intelligence/2021/04/a-deep-dive-into-saint-bot-downloader/

Building cyber resilience will manage risk in today's threat environment.

Ankura CTIX urges organizations to implement the following hardening techniques to increase their cyber resilience.

1. Bolster threat intelligence capabilities to ensure awareness of this dynamic situation
2. Ensure that incident response plans and playbooks are up-to-date and ready for execution
3. Monitor email traffic for phishing links and malicious documents
4. Institute multi-factor authentication (MFA) on all user accounts enterprise-wide
5. Ensure backups are present and working in the case of data-wiping attacks
6. Follow the principle of least privilege for employees and third-party vendors
7. Verify integrity of Intrusion Detection & Protection Systems
8. Conduct monthly internal threat assessments and daily/weekly vulnerability management scans
9. Ensure that all server rooms, data storage locations, and IT closets are secured properly
10. Modernize security protocols and practices to combat new emerging threats and attack vectors

ankura

INDICATORS OF COMPROMISE (IOCS)

CTIX analysts conducted covert collections across a number of public, private, deep, and dark web sites to collect indicators of compromise for the threat landscape highlighted in the above analysis.

Indicator	Type	Description
fe6e84192da5c0210d4bd51e809792b28e60edb337917f903a7e9a31bc40cf86	Hash	Conti
fe1652f4b828c9f98ff4a37829f4a988ad3c1601fc0dff7f99fe941ae4e81864	Hash	Conti
fc783af396a1bd9c81613cd051db69e778c102953aec0d6f67743846f3b862e6	Hash	Conti
f99c69327a746f4fde02b7a550cf6c9f48e5e22fcb49bea0e3e4bc5a3efa605c	Hash	Conti
f99c69327a746f4fde02b7a550cf6c9f48e5e22fcb49bea0e3e4bc5a3efa605c	Hash	Conti
f7b83f07f6fec1df0fa73c935c96dc2ec8fbe0de3b17bb56f9963c92c22715c3	Hash	Conti
f20ed03ba228b36064517c1e5fff9ae40d957451a5c6d9a48f9bbe2c3dd881b7	Hash	Conti
f11724258acba02fa817e411878cd2506c09f4d00fcc47302f55dc7748d50fd9	Hash	Conti
f0a674f3a449561a102eac9ee445b18bb15536429dca0c0ee020054952dd4899	Hash	Conti
ef870eae64e28ebd71c8ad909af39ea9a072256bfd634210f4de24ded5a3304a	Hash	Conti
eae876886f19ba384f55778634a35a1d975414e83f22f6111e3e792f706301fe	Hash	Conti
d01e2c2e8df92edeb8298c55211bc4b6	MD5	Cyclops Blink
bbb76de7654337fb6c2e851d106cebc	MD5	Cyclops Blink
3c9d46dc4e664e20f1a7256e14a33766	MD5	Cyclops Blink
3f22c0aeb1eec4350868368ea1cc798c	MD5	Cyclops Blink
bbb76de7654337fb6c2e851d106cebc7	MD5	Cyclops Blink
3adf9a59743bc5d8399f67cab5eb2daf28b9b86	SHA1	Cyclops Blink
c59bc17659daca1b1ce65b6af077f86a648ad8a	SHA1	Cyclops Blink
7d61c0dd0cd901221a9dff9df09bb90810754f10	SHA1	Cyclops Blink
438cd40caca70cafe5ca436b36ef7d3a6321e858	SHA1	Cyclops Blink
50df5734dd0c6c5983c21278f119527f9fdf6ef1d7e808a29754ebc5253e9a86	SHA256	Cyclops Blink
c082a9117294fa4880d75a2625cf80f63c8bb159b54a7151553969541ac35862	SHA256	Cyclops Blink
4e69bbb61329ace36fbe62f9fb6ca49c37e2e5a5293545c44d155641934e39d	SHA256	Cyclops Blink
ff17ccd8c96059461710711fcc8372cfea5f0f9eb566ceb6ab709ea871190dc6	SHA256	Cyclops Blink
100.43.220[.]234	IP Address	Cyclops Blink - C2 Server
96.80.68[.]193	IP Address	Cyclops Blink - C2 Server

188.152.254[.]170	IP Address	Cyclops Blink - C2 Server
208.81.37[.]50	IP Address	Cyclops Blink - C2 Server
70.62.153[.]174	IP Address	Cyclops Blink - C2 Server
2.230.110[.]137	IP Address	Cyclops Blink - C2 Server
90.63.245[.]175	IP Address	Cyclops Blink - C2 Server
212.103.208[.]182	IP Address	Cyclops Blink - C2 Server
50.255.126[.]65	IP Address	Cyclops Blink - C2 Server
78.134.89[.]167	IP Address	Cyclops Blink - C2 Server
81.4.177[.]118	IP Address	Cyclops Blink - C2 Server
24.199.247[.]222	IP Address	Cyclops Blink - C2 Server
37.99.163[.]162	IP Address	Cyclops Blink - C2 Server
37.71.147[.]186	IP Address	Cyclops Blink - C2 Server
105.159.248[.]137	IP Address	Cyclops Blink - C2 Server
80.155.38[.]210	IP Address	Cyclops Blink - C2 Server
217.57.80[.]18	IP Address	Cyclops Blink - C2 Server
151.0.169[.]250	IP Address	Cyclops Blink - C2 Server
212.202.147[.]10	IP Address	Cyclops Blink - C2 Server
212.234.179[.]113	IP Address	Cyclops Blink - C2 Server
185.82.169[.]99	IP Address	Cyclops Blink - C2 Server
93.51.177[.]66	IP Address	Cyclops Blink - C2 Server
80.15.113[.]188	IP Address	Cyclops Blink - C2 Server
80.153.75[.]103	IP Address	Cyclops Blink - C2 Server
109.192.30[.]125	IP Address	Cyclops Blink - C2 Server
84ba0197920fd3e2b7dfa719fee09d2f	MD5	HermeticWiper
3f4a16b29f2f0532b7ce3e7656799125	MD5	HermeticWiper
d57f1811d8258d8d277cd9f53657eef9	MD5	HermeticWiper
bdf30adb4e19aff249e7da26b7f33ead	MD5	HermeticWiper
f49c0774f1ec84f33db771801eea1edf	MD5	HermeticWiper

b470903ecb076607dcd2b86a1ba9f94b	MD5	HermeticWiper
5d5c99a08a7d927346ca2dafa7973fc1	MD5	HermeticWiper
0e085a1d8aa8a4a3ed1cd9949f7100a3	MD5	HermeticWiper
b33dd3ee12f9e6c150c964ea21147bf6b7f7afa9	SHA1	HermeticWiper
87bd9404a68035f8d70804a5159a37d1eb0a3568	SHA1	HermeticWiper
f1848b3c4fceb3cb38cce30c23b40a19acc793e7	SHA1	HermeticWiper
be37ed968a0dca38f872dbb0239c6f3a3b9321bc	SHA1	HermeticWiper
ba6a2e5a5f7578429e86b262c2a370d6bac86b21	SHA1	HermeticWiper
189166d382c73c242ba45889d57980548d4ba37e	SHA1	HermeticWiper
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	SHA256	HermeticWiper
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	SHA256	HermeticWiper
fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d	SHA256	HermeticWiper
e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5	SHA256	HermeticWiper
b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd	SHA256	HermeticWiper
b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1	SHA256	HermeticWiper
96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84	SHA256	HermeticWiper
8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b	SHA256	HermeticWiper
2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d	SHA256	HermeticWiper
23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4	SHA256	HermeticWiper
b50fb20396458aec55216cc9f5212162b3459bc769a38e050d4d8c22649888ae	SHA256	HermeticWiper
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	SHA256	HermeticWiper
8d71d6e45183bc1390f0621e79a7ec1f1f664a252af7cfde2458de3b1c1a4f8e	SHA256	HermeticWiper
22f1d202cd3c902a5d813b0be8a3bc3e61af31a3dcd799e6a63139d6ea888382	SHA256	HermeticWiper
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	SHA256	HermeticWiper
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	SHA256	HermeticWiper
a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e	SHA256	HermeticWiper
4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382	SHA256	HermeticWiper
61b25d11392172e587d8da3045812a66c3385451	SHA1	HermeticWiper
912342f1c840a42f6b74132f8a7c4ffe7d40fb77	SHA1	HermeticWiper

a952e288a1ead66490b3275a807f52e5	SHA1	HermeticWiper
231b3385ac17e41c5bb1b1fcb59599c4	SHA1	HermeticWiper
095a1678021b034903c85dd5acb447ad	SHA1	HermeticWiper
eb845b7a16ed82bd248e395d9852f467	SHA1	HermeticWiper
arianat.ru	Domain	Primitive Bear
deep-pitched.enarto.ru	Domain	Primitive Bear
deep-toned.chehalo.ru	Domain	Primitive Bear
deer-lick.chehalo.ru	Domain	Primitive Bear
iruto.ru	Domain	Primitive Bear
http://68468438438[.]xyz/soft/win230321[.]exe	URL	SaintBot
http[:]//update-0019992[.]ru/testcp1/gate.php	URL	SaintBot
51e84accb6d311172acb45b3e7f857a18902265ce1600cfb504c5623c4b612ff	SHA256	WhisperGate
a2d60af7bebac9b299db109f8162ed6335fb5dda08f57f00e9dc809d4f138428	SHA256	WhisperGate
34ca75a8c190f20b8a7596afeb255f2228cb2467bd210b2637965b61ac7ea907	SHA256	WhisperGate
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745	SHA256	WhisperGate
17fc12902f4769af3a9271eb4e2dacce	MD5	WhisperGate - AdvancedRun.exe
5d5c99a08a7d927346ca2dafa7973fc1	MD5	WhisperGate - BootPatch
179.43.176 [.] 42	IP Address	WhisperGate - Discord Downloader
179.43.176 [.] 38	IP Address	WhisperGate - Discord Downloader
179.43.176 [.] 60	IP Address	WhisperGate - Discord Downloader
179.43.176.0/24	IP Address	WhisperGate - Discord Downloader
https: //cdn.discordapp [.] com / attachments / 928503440139771947/930108637681184768 / Tbopbh.jpg	URL	WhisperGate - Discord Downloader
http: //179.43.176 [.] 42: 8000 / index.php	URL	WhisperGate - Discord Downloader
http: //179.43.176 [.] 38: 8000 / index.php	URL	WhisperGate - Discord Downloader
14c8482f302b5e81e3fa1b18a509289d	MD5	WhisperGate - WhisperGate

0e16df6845cde1260087902f25842f79	MD5	WhisperGate - WhisperKill
fa23f43fa759f0f38cde2b703d98ba05	MD5	WhisperGate - WhisperKill
7de66b5c7d3ddae321fa6cfeeaa94819	MD5	WhisperGate - WhisperKill
78e941e780adc1a159fdc7090194c96d	MD5	WhisperGate - WhisperKill
363e2b62f93c58c177e58dbe0a247fa0	MD5	WhisperGate - WhisperKill
adcd23078da37d0054cc75fb45e9d095	MD5	WhisperGate - WhisperKill
b0e4a2cd59c4620b794ecda351c736a2	MD5	WhisperGate - WhisperKill
a02df1ad79381a269843c831fb8a48b0	MD5	WhisperGate - WhisperKill
f360827a30f1267a3170ad6f7c160730	MD5	WhisperGate - WhisperKill
3907c7fbd4148395284d8e6e3c1dba5d	MD5	WhisperGate - WhisperKill
101.99.93 [.] 49	IP Address	WhisperGate - WhisperKill
rmssrv2 [.] ru	Domain	WhisperGate - WhisperKill
rmssrv3 [.] ru	Domain	WhisperGate - WhisperKill
rmssrv4 [.] ru	Domain	WhisperGate - WhisperKill
https: //cdn.discordapp [.] com / attachments / 908281957039869965/937420906286952568 / d5aadb4ace8ffccb.zip	URL	WhisperGate - WhisperKill
http: // eumr [.] site / up74987340.exe	URL	WhisperGate - WhisperKill
http: // eumr [.] site / load74h74830.exe	URL	WhisperGate - WhisperKill
http: //185.244.41 [.] 109: 8080 / upld /	URL	WhisperGate - WhisperKill
http: // 8003659902 [.] space / wp-adm / gate.php	URL	WhisperGate - WhisperKill
http: // smm2021 [.] net / wp-adm / gate.php	URL	WhisperGate - WhisperKill
http: // 8003659902 [.] site / wp-adm / gate.php	URL	WhisperGate - WhisperKill
eumr [.] site	Domain	WhisperGate - WhisperKill
8003659902 [.] Space	Domain	WhisperGate - WhisperKill
smm2021 [.] no	Domain	WhisperGate - WhisperKill
8003659902 [.] Site	Domain	WhisperGate - WhisperKill
1000020 [.] Xyz	Domain	WhisperGate - WhisperKill
185.244.41 [.] 109	Domain	WhisperGate - WhisperKill
e61518ae9454a563b8f842286bbdb87b	MD5	WhisperGate - WhisperPack

Address		Phone
2000 K St. NW., 12th Floor, Washington, DC, 20006 United States	M	+1.202.797.1111