World Watch

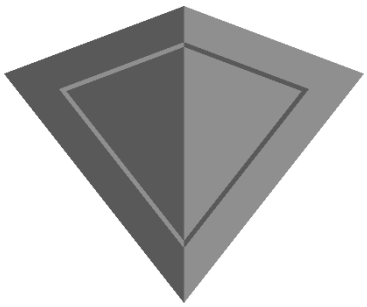
War in Ukraine Cyber Observations

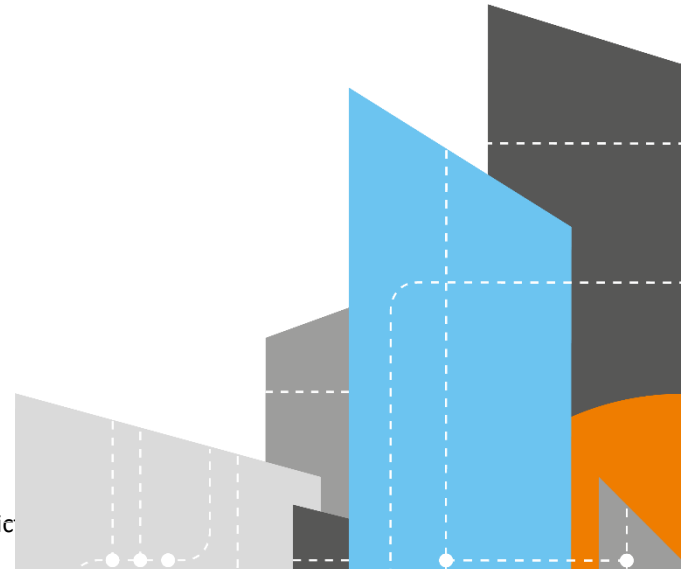
News alert

Confidentiality: unrestricted

First seen 2022-01-17

Last update 2022-03-02





Versions

Version	Date	State
Initial alert	2022-01-17, 10:00 CET	OK
Update 1.0	2022-01-27, 10:30 CET	OK
Update 2.0	2022-02-01, 12:00 CET	OK
Update 3.0	2022-02-07, 10:00 CET	OK
Update 4.0	2022-02-15, 10:00 CET	OK
Update 5.0	2022-02-16, 10:00 CET	OK
Update 6.0	2022-02-24, 10:00 CET	OK
Update 6.1	2022-02-24, 11:30 CET	OK
Update 7.0	2022-02-24, 17:00 CET	OK
Update 8.0	2022-02-25 14:00 CET	OK
Update 9.0	2022-02-27 12:00 CET	OK
Update 10.0	2022-02-28 11:00 CET	OK
Update 11.0	2022-03-02 10:00 CET	OK

Index

Title: Cyberwarfare

ID: 584848

First_seen: 2022-01-17

Last_update: 2022-03-02

Threat_type: Cyberwarfare

Defcon_level: 4/5

1 War in Ukraine: Cyber Threat Activity

Analysis

Reminder:

On February 23, Russia launched a full-scale war against Ukraine, and we track the latest geopolitical evolutions of this conflict here.

You will find below the specific information related to the cyber incidents identified in this hybrid warfare.

Update 11, 02/03/2022 10:00 CET

ESET discovers a new malware, retaliation by hacktivists against Russian groups

Following the February 27 release by a Twitter user called #Contileaks, a new batch of files has been published containing **all of Conti's source code**, as well as a large amount of data including malware, information about victims, their modus operandi... Our experts are currently analyzing the various documents, but the amount of information requires several days of work.

In addition, **ESET researchers** have published a report in which they provide more information about the **HermeticWiper** operation. In it, they announce that they have discovered a new wiper that attacks Ukrainian organizations and a worm component that propagates in local networks.

The worm sample, dubbed **HermeticWizard**, is a DLL file developed in C++ that allows attackers to deploy the HermeticWiper malware on local networks that have been compromised. To do this, it tries to find other machines on the local network using different Windows functions such as NetServerEnum, GetTcpTable, GetIpNetTabl, etc. When this is done, it tries to connect to the collected IP addresses to deploy the different tools required to run the HermeticWiper malware. However, it simply uses the SMB and VMI protocols to deploy it, so it is not a very complex malware, unlike worms such as EternelBlue or EternelRomance.

The second malware identified as **IsaacWiper** is a wiper that was deployed on February 24 during a second destructive attack against a Ukrainian government network. It is a malware that resides in a Windows DLL or EXE without Authenticode signature. According to researchers, it has **no code similarity** with HermeticWiper and is much less sophisticated than the latter. IsaacWiper aims to erase the contents of Windows devices. It is important to note that when it erases the hard drives of the compromised device, it recursively deletes the files in a single thread, so the time to erase a large disk is increased.

At this stage, there is no indication that these malwares have been used against any other country other than Ukraine. However, there is still a risk that the threat actors could decide to further use it against countries that support the Ukrainian government or sanction Russian entities.

In addition, the domain registrar, **Namecheap**, announced that it would stop providing services to customers registered in Russia. The company added that all affected domains would be automatically configured to display prohibited HTTP 403 errors.

More hacktivists cyberattacks against Russia **in retaliation** for the war against Ukraine are being reported but it is hard to confirm the accuracy of these claims. For instance, an affiliated group with Anonymous has claimed a successful attack against the Control Center of the Russian Space Agency "**Roscosmos**". They claim that Russia has lost its control over its satellites as a result of this attack. Another major cyberattack was claimed by AgainstTheWest targeting the major, state-owned, Russian financial institution **Sberbank**. The hackers say they will soon leak DNS infrastructure data, private keys for SSL, Sberbank API, CLI and SDKs.

Update 10, 28/02/2022 11:00 CET

Hacktivism increases, Conti chats leaked

On February 27, a member of the **Conti ransomware** group, believed to be Ukrainian of origin, has **leaked numerous gang's internal chats** following the aggressive pro-Russian message released by a group representative on their official site.

The leaked data contains 339 JSON files, with each one consisting of a full day's log. Conversations from January 29, 2021 to February 27, 2022 have thus been leaked as this Conti member has likely participated and/or hacked the gang's internal Jabber/XMPP server. This content, already indexed in a public database and translated in English, is thus now analyzed by many Threat Intel analysts (on top of Law Enforcement agencies). The LockBit ransomware has taken a different and more careful stance, announcing in an **apolitical message** it would not pick a side between Ukraine and Russia, and that for them all that matters is business (i.e making money).

Cyber hacktivism operations are still increasing and the latest to date was conducted by the Belarusian group **"Cyber Partisans"** against the country's train network, in order to disrupt Russian troop movements into Ukraine. These hackers may have effectively **damaged a railway control system**, forcing trains to halt in Minsk, Orsha & Osipovichi.

Another cyberattack has targeted a **Ukrainian border control station** while thousands of people are trying to flee the country because of the war. This attack has been caused by a wiper, although it is still unknown if it is HermeticWiper which has targeted several Ukranian entities recently (see our Update n°6&7 below).

Moreover, ProofPoint said it has identified a suspected compromised ukr[.]net account sending an evacuation themed **malicious Excel document** to a European government. This malicious document is sent via phishing emails to Ukrainian military personnel. ProofPoint added that the malicious document communicate to 84.32.188[.]141 but no further details were provided as of now. All relevant IOCs were added to our Datalake CTI repository, proposed as a standalone service (called Managed Threat Intelligence) and used by our Managed Threat Detection teams.

Different groups have indeed choosen a side in this conflict and are currently fighting in the cyberspace, a list of these actors has for example been shared here by an anonymous account dubbed CyberKnow. This one previously shared unverified (and most probably wrong) claims such as one regarding the origin of Log4shell. But their list of participating groups seems credible, as most of them mentioned publicly being involved indeed.

More DDoS attacks keep happening, as thousands for example already joined the "IT Army of Ukraine" we mentioned yesterday, and easy-to-use guides are being shared online on how to take part. The Moscow Stock Exchange, under heavy pressure because of the sanctions already affecting severely the country's currency, which delayed its opening hour this morning, seems for example down at the moment.

Update 9, 27/02/2022 12:00 CET

Hacktivism increases, Ukraine launching an IT Army to combat Russia on Internet

Hacktivism keeps growing with more DDoS attacks, defacements or data leaks.

Some leaks of military information on both sides was for example announced by hacktivists, including 200Go from a Belarusian defense contractor.

But the main concern came yesterday from the **Conti ransomware** operation, that announced siding with Russia and threatened to attack critical infrastructure if Russia is targeted by any cyberattack. They later softened their message, and turned it into a plea against US and also against war. On Twitter, a security researcher reacted by leaking the Conti back-end infrastructure Tor addresses, before deleting quickly his message.

This information may also be related to Ukraine authorities launching these last years many operations against ransomware groups (and cybercriminals in general). But RaaS gangs based in Russia might indeed enjoy an even more "golden age" of cybercrime now, as Russian authorities might let them act freely in response to the Western sanctions. Even if Russia presumably took a harsher stance against ransomware in the latest weeks by arresting som REvil members.

Ukrainian authorities have indeed decided to create an **"IT Army",** to "fight in the cyber front" with targets including Russian banks, companies, and public organizations. As explained by Kevin Beaumont, the Ukrainian government has praised the actions of the Anonymous hackers collective, which could well be a milestone moment, as for the first time a democratic government **publicly supports such an hacktivist group**. On Internet, "cyber patriots" could escalate the fight against Russia, which in return could try to get help from cybercriminal organizations such as Conti. This scenario is not a reality yet, and it is hard to guess as of now what impacts may be felt worldwide if it happens.

Another unanticipated actor has also rushed to help the Ukrainian people, Elon Musk. Indeed, he announced that **SpaceX's Starlink satellites** had been activated in Ukraine, with more terminals en route, following a request from Ukrainian Vice Prime Minister Mykhailo Fedorov. Musk's SpaceX has thousands of Starlink satellites in orbit, which allow the company to beam broadband services around Earth, without the need for fiber-optic cables. The satellites could keep Ukraine maintain their presence online, if its Internet infrastructure is damaged by Russia's attacks.

On the other side, Russia announced partial **restriction of access to Facebook** over the American platform's ban of Kremlin-backed media capability to send ads. The website of the state-run TV channel Russia Today -or RT—was inaccessible for hours these last days. The media said that it was a victim of a DDoS cyberattack launched by Anonymous. Attacks against Russian organizations have increased during the weekend as **Russian TV channels have been hacked** to

broadcast pro-Ukrainian messages and songs. Hacktivism even affected unexpected resources such as defacing vessel tracking platform, with Russian yachts location and name being modified.

Netlab360 provided some more information on the botnets behind the various attacks (against Ukraine and Russia) that happened in the past days.

The cyber threat level remains nonetheless unchanged and is still rated at a 4 out 5 level. The World Watch team is monitoring the situation in the cyber and geopolitical world and will update this alert once more information will be available.

Update 8, 25/02/2022 14:00 CET

More hacktivism expected as cyber conflict escalates

On February 24, reactions increased in the hacking community. A DDoS attack attempting to **disrupt the Kremlin.ru** and Mil.ru websites, was identified by systems capturing amplification malicious traffic. The Russian authorities reacted and "geofenced" it to only authorize Russian IP addresses to connect to it. The attackers remain unconfirmed as of now, but it may probably have involved hacktivists from the old "**Anonymous"** collective. Indeed, they announced on Twitter launching campaigns to combat Russian government, and claimed credit for the DDoS attacks, including **against Russian ISPs and major local banks**.

The famous RaidForums underground cybercriminals forum administrator also announced he would ban accounts connecting from Russia. Furthermore, the Ukrainian authorities asked local hackers to help them protect critical infrastructure and conduct cyber espionage missions.

This means the conflict will most probably continue to escalate in the cyber world, with more data leaks, defacements and DDoS attacks in particular.

Europe has agreed to provide some cyber defence forces to Ukraine as per the PESCO framework. The Polish cybersecurity Secretary of State announced cyberattacks have increased against their government systems, as did the CEO of PGE, the top power utility in this country. And the CERT of Ukraine shared on Facebook an ongoing phishing attack targeting .ua email accounts, presumably from the Belarus threat actor UNC1151.

We added the host- and network-based IOCs provided in this phishing campaign to our Datalake repository. The hostnames have been already blocked by CloudFlare now. Furthermore, GreyNoise, a US security vendor with many sensors in the world, started sharing list of IP addresses they identify as targeting specifically Ukraine. We've implemented their feed in our Datalake CTI platform under the source ID: "greynoise_ukraine".

Finally, a bit more information is available regarding the trojan attack in preparation we discussed yesterday. Dubbed OutSteel by Ukrainian authorities (or LocrecDocStealer by NSFOCUS), it is part of a bigger campaign affecting Ukraine since months. The attackers (i.e. named TA471, Lorec53 or UAC-0056 by the Ukrainian CERT) have relentlessly targeted at least 50 email addresses belonging to Ukrainian government, military or state-owned organizations. The TTPs involve sending phishing emails embedded with malicious attachments with decoy documents written in Ukrainian. It

leverages mostly LNK or CPL files, and domains ending in ".site" to host the payloads or C2. The end goal of the payloads is to steal documents, thus is espionage oriented.

We remain committed to help all our clients, and will keep sharing any evolution of the cyber threat level through this advisory. ***But for now, the cyber risk landscape has not changed for most non-Ukrainian/Russian organizations according to us.***

Update 7, 2022-02-24 17:00CET

Analysis of HermeticWiper and other malware used against Ukraine

Following ESET and SentinelLabs initial analysis of the second wiper attack ongoing in Ukraine since yesterday, Symantec has also published a report on this malware strain called **HermeticWiper**. The latter aims to erase content from Windows devices, after deleting snapshots and manipulating the MBR after reboot.

According to the researchers, the attackers gained network access to one Ukrainian victim on December 23, 2021, via malicious SMB activity against a Microsoft Exchange server. This allowed the attackers to steal credentials, then also install a web shell on January 16, before the wiper was finally deployed on February 23.

The wiper, signed by a legitimate -probably stolen- digital signing certificate, use legitimate resources to execute the most damaging components of the attacks. For instance, it uses a partition management driver identified as "empntdrv.sys" from the **EaseUS Partition Manager** application, to directly access physical disks, as well as obtain information about the partitions. Using this access, the malware corrupts entirely the hard drives. It is important to note that the malware embeds different versions of the legitimate driver (x86, x64, x86 for WinXP and x64 for WinXP), allowing him to run on most Windows versions.

Finally, the wiper does not seem to have any additional functionality beyond its destructive capabilities. According to Symantec, the campaign tied to HermeticWiper also deploys a ransomware strain against affected organizations. The file names used by the ransomware included client.exe, cdir.exe, cname.exe, connh.exe or intpub.exe. It seems likely that this ransomware was used as a decoy or distraction from the wiper attack.

Symantec has observed this wiper in an organization in Lithuania on top of Ukraine, after hacking it since last November using as initial vector a Tomcat vulnerability. Another rumor mentioned it was also seen in Latvia, without much further evidence to confirm it so far. The attacker relied a lot on scheduled tasks and PowerShell scripts, and downloaded a malicious payload from a compromised Ukrainian website hosted on confluence[.]novus[.]ua.

An unrelated attack discovered by **Bellingcat** we briefly discussed below includes a trojan horse to be used against Ukrainian citizens showing support to their institutions. This trojan contacted and tried to download a probable malicious second stage from "stun[.]site/pet1.exe", then write it to C:\Users\Public\svchosts.exe, and finally execute it. Unfortunately, this site is currently inaccessible, thus the final payload remains unknown to us. Some researchers call the threat actor behind this campaign as **TA471**.

In yet other news, British and American cybersecurity agencies have issued a joint security advisory on another new piece of malware, dubbed **Cyclops Blink,** which they formally attributed to

the Russian-backed SandWorm APT group. This malware has been active since at least June 2019 and, among other things, allows for the creation of a botnet. To date, the malicious actors behind this malware have targeted WatchGuard Firebox and other Small Office/Home Office (SOHO) network devices. However, it is likely that this malware can also be compiled on other architectures and firmware.

There is no evidence so far that this malware and the associated botnet is used in current cyber operations against Ukraine today, but it's yet another weapon in the arsenal of Russian authorities.

We advise you to follow our recommendations from the geopolitical advisory related to this conflict, that echoes recommendations from CISA and the other Western countries cybersecurity agencies.

Update 6, 2022-02-24, 10:00 CET

A new DDoS attack affected yesterday multiple websites tied to the Ukrainian government. This new disruption campaign successfully impacted the local Ministry of Foreign Affairs, Ministry of Defense or the Parliament websites. Networks from Privatbank and Oschadbank, also targeted a week ago in the previous similar attack, again struggled to serve some of their clients. The attack started around 14h GMT and echoed those of last week.

Indeed, on February 20, Cado Security released a technical analysis of the low-scale DDoS attack which has targeted Ukrainian websites some days ago. According to these researchers, the botnet behind this attack was composed of Linux-based vulnerable devices (such as routers or IoT) using a malware known since some time as Katana, a publicly available variant of Mirai with improved DDoS capabilities. The attack was combined with a rarer BGP hijack, attempting to disrupt traffic routing, in particular towards PrivatBank's autonomous system.

Those attacks were attributed to GRU, Russia's intelligence service, both by the US, UK or Australian authorities for example, on top of the Ukrainian ones previously. Bellingcat, a well-known group of online investigators which shared some details on the forged videos used as propaganda here, provided some evidence related to the attacks. But they also identified another attack in preparation. This one involved fake websites mimicking the official Ukrainian government ones, but embedding some malicious payload disguised as a PDF that would be dropped on the computer of those opening it. We ave not analyzed in details this trojan yet, and the forged websites have been taken down by the hosting provider. This specific attack could nevertheless be relaunched from another hosting location easily.

Furthermore, ESET identified a new wiper campaign distributed to hundreds of computers in Ukraine since 15h GMT yesterday. This malware strain is now called HermeticWiper, and was reversed by Sentinel Labs. They confirmed the malware is well coded for sabotage purposes, and ESET mentioned it was dropped in one case to machines joined in one Active Directory through GPO, which means the hackers had previously gained access to one Administration account in this network.

The IoCs of these two malware campaigns have been added to our Datalake CTI repository and can be seen in Appendices. Considering these new evolutions, we raised the threat level to 4 out of 5, even if no propagation of this malware is expected as of now.

Update 5, 2022-02-16 10:00 CET

DDoS attack hits Ukrainian government and two major banks

On February 15, several Ukrainian websites including those of the defense ministry, the publicly-funded state radio and the two biggest national banks (Privatbank and Oschadbank), have been hit by a Distributed Denial of Service (DDoS) attack. Privatbank and Oschadbank were down for two hours, starting around 3pm local time, leaving the banks' mobile applications and any online payment inaccessible. Privatbank alone claims to serve nearly 20 million Ukrainian customers. Ukraine's public radio also suffered an attack, but it didn't bring its services down, announced its general producer. A few hours later, all targeted websites were once again accessible.

According to the Ukrainian Cyber Police, this attack was part of a bigger disinformation campaign targeting the Ukrainian people, as some of them received unsolicited SMS signaling that ATMs in the country were also offline, which was not true. It is quite clear that this attack didn't aim at causing heavy damages to the impacted systems, but rather to create panic among the local population. DDoS attacks are relatively cheap and easy to carry out. While they can be disruptive, they do not necessarily require sophistication from the attackers.

The attack came amid growing concerns about a possible Russian military invasion of Ukraine. For now, as the investigation is still ongoing, Ukrainian authorities have not formally attributed this cyberattack to a specific country. Indeed, DDoS attacks can be difficult to trace to their source, as hackers can spoof the source addresses of the packets sent to make it seem those are coming from a country, they are not located in. They also usually leverage networks of compromised machines, botnets, that can be located in multiple countries.

For now, the conflict does not impact organizations except Ukrainian ones, but as some private organizations start being targeted, and more disinformation campaigns keep happening, we increased the threat level of this advisory to 3 out of 5.

Update 4, 2022-02-15 10:00 CET

Tension between Russia and Ukraine at its peak, disinformation flourishing

While rumors about an imminent Russian military invasion of Ukraine keep being announced by Western authorities for this week, including US and French ones, Ukrainian intelligence forces says the country is targeted by "massive wave of hybrid warfare".
According to the Security Service of Ukraine (SSU), this campaign aims at systemically sowing panic, by spreading fake information and distorting the real state of affairs. The SSU said it conducted several operations to counter these malicious activities. One of them happened last week as the intelligence service said it dismantled two bot farms linked to Russian intelligence services and controlling 18,000 social network accounts. These botnets were used to distribute fake news to further spread panic and send fake bomb threats to disrupt normal operations across the country.

Consequences of a full-fledge war between the two foes could have a big impact in the whole world. The European Central Bank has for instance asked banks to increase their cyberdefenses amid the growing tensions between Ukraine and Russia. A similar warning was issued earlier by CISA to urge US organizations to strengthen their security stance because of potential Russian cyberattacks. According to the US cybersecurity agency, the Russian government may consider "escalating its

destabilizing actions" to impact entities outside of Ukraine. CISA recommended in particular to those working with Ukrainian organizations to monitor, inspect, and isolate traffic from those organizations.

There is currently a huge difference between the official communication of the US and the UK governments, which foresee an imminent invasion, and on the contrary, statements from Ukraine and Russia dismissing probability any conflict would happen in the coming days. Yet the US government is temporarily moving its embassy in Ukraine from Kyiv to Lviv (in the West of the country), due to the "dramatic acceleration in the buildup of Russian forces". On the other side, Russian-backed news agency Interfax reported on February 15 that some of the military units recently positioned near the Ukrainian border are returning to their bases in the Western and Southern military districts.

It is thus obvious that an informational warfare is ongoing in this crisis, so every statement released by the involved parties should be taken with a grain of salt.

We did not change our threat level (i.e. our "severity") rating for this advisory so far, as no new cyber incidents impacting our customers were yet reported.

Update 3, 2022-02-07 10:00 CET

Cyberespionage against Ukraine by Gamaredon group

On February 4th, Microsoft Threat Intelligence Center (MSTIC) and the Microsoft Digital Security Unit (DSU) **said that Gamaredon's** cyberespionage campaign is being coordinated out of Crimea, by officers of the Crimean FSB who sided with Russian authorities since the 2014 occupation. This threat actor they now name "**ACTINIUM**" (and previously DEV-0157) has targeted Ukrainian government including judiciary, law enforcement and military, as well as local non-government organizations (NGO). Its primary intent remains acquiring and maintaining access into victim organizations in order to exfiltrate sensitive information.
Gamaredon, also called Armageddon, Primitive Bear or Shuckworm (as mentioned below), is not linked as of now to last month's attacks that targeted multiple Ukraine entities with destructive data-wiping malware disguised as ransomware. A list of IOCs tied to this threat actor was disclosed by Microsoft, including for its **Pterodo** (also called Pteranodon below) and **QuietSieve** malware strains.

Palo Alto Networks' Unit42 also issued a report regarding this group's recent activity and said it has detected three "large clusters" of Gamaredon infrastructure that are used to support phishing and malware delivery. The IOCs are associated to downloaders, file stealers and a custom remote access tool called "**Pteranodon**," which has been exclusively attributed to Gamaredon for years.
An attempt on January 19 to compromise a Western government entity in Ukraine via a spear-phishing attack dropping a malware downloader was mentioned by the security company. In this particular attack, rather than emailing the downloader directly to their target, the actors applied to an open job posting within the targeted entity, embedding a malware-laced resume in their application, Unit42 said.

Update 2, 2022-02-01 12:00 CET

Cyberespionage against Ukraine by Gamaredon group

On January 31, 2022, researchers from Symantec's Threat Hunter team published a report in which it states that the Russian-linked Shuckworm group (aka Gamaredon, Armageddon), deploys custom malware in cyber-espionage operations against **Ukrainian entities**.

According to researchers, the first ones started in July with the dissemination of spear phishing emails containing Word documents with macros. These attacks continue with **seven different payloads.** These different malicious files are self-extracting 7-zip binaries that minimize user interaction requirements.

Furthermore, since 2014, the Shuckworm group has been responsible for more than 5,000 attacks against more than 1,500 Ukrainian government systems according to the November 2018 SSU report.

Finally, we recall that the Shuckworm group is reportedly directly operated by the FSB, so this new report might once again increase tensions between Ukraine and Russia.

The indicators of compromise (IOC) present in the Symantec report are available on our OCD Datalake platform.

Update 1, 2022-01-27 10:30 CET

Destructive malware targeting Ukrainian organizations detected by Microsoft

On January 26, the Ukrainian government qualified the latest data-wiping attack as a false-flag operation. Indeed, they have found evidence that the WhisperGate malware contained more than 80% of code that was similar to a ransomware strain named WhiteBlackCrypt. This malware was part of a campaign which has targeted several Russian companies in the past. Ukrainian authorities believe that the use of this particular malware strain was meant to conduct a "false-flag" operation in order to distract investigators from the real culprits behind the attack (formally attributed to the Russian government).

The same day, CERT Ukraine has released a report about the recent cyberattacks the country suffered and explained that the most likely vector was a supply-chain attack, but the exploitation of vulnerabilities against OctoberCMS or Log4j were not ruled out. A few days after the attacks, a likely supply-chain compromise involving the product from local company KitSoft, used to manage the targeted websites, was already mentioned.

Moreover, several cybersecurity blogs including Stairwell and Talon SW2 have detailed the 3rd stage of the wiper code. This "Stage 3" is relatively more complex than the two previous ones and once loaded by the stage 2, it will overwrite files on a system with specific extensions:

- Stage 1: MBR payload
- Stage 2 (or 2+3 at Elastic): Discord downloader / injector
- Stage 3 (or 4 at Elastic): File corruptor

Even if no new cyberattacks were recorded recently, tensions between Ukraine and Russia remain very high. Considering the attempt to misdirect attribution in order to probably reinforce a propaganda narrative, we increased the threat level of this alert to 2 out of 5.

Initial alert on: 2022-01-17 10:00 CET

1.1 Executive summary

On January 15th, Microsoft announced in a blogpost that it has detected a **data-wiping malware** disguised as a ransomware being used in **attacks against multiple organizations in Ukraine**. These attacks combine a destructive "MBRLocker" (a kind of disruptive tool as described in this previous case) with a data-corrupting malware used to destroy the victim's data intentionally. The MBR is the part of a hard drive that tells the computer how to load its operating system.

This new malware family is called "**WhisperGate**" by Microsoft and was initially detected on January 13th. The threat actor behind this malicious campaign is not previously known and now tracked by the Redmond giant as **DEV-0586**.

1.2 What you will hear

A new threat actor targets Ukraine with a data-wiping malware called WhisperGate.

1.3 What it means

According to Microsoft, the WhisperGate malware family has two main components:

- stage1.exe, launched from the C:\PerfLogs, C:\ProgramData, C:\, or C:\temp folders, that overwrites the Master Boot Record (MBR) to display a ransom note
- stage2.exe, is executed simultaneously to download a data-destroying malware named "Tbopbh.jpg" hosted on Discord, that overwrites targeted files with static data.

Despite the presence of a ransom note, Microsoft researchers said that the malware is not attempting to deploy a ransomware payload. This behavior is fake and an easy-to-spot smokescreen. Indeed, the MBRLocker's ransom note uses the same bitcoin address for all victims and does not provide a method to input a decryption key. Thus, the goal of these attacks is to render targeted devices inoperable and not to obtain a ransom. For now, victims include multiple government, non-profit, and information technology organizations, but all based in Ukraine. Microsoft believes it is highly likely that there are more victims.

Microsoft said that no vulnerability impacting its products was used to launch these attacks, and it for now remains unknown publicly how this malware was deployed initially.

This report released by Microsoft comes amid several cyberattacks targeting Ukraine these last days. At least fifteen websites of Ukrainian public institutions and government agencies were hacked, defaced, or taken offline through DDoS attacks last week. The Ukrainian government believes a threat actor linked to the Belarusian intelligence service is behind this massive campaign which used a malware similar to that used by a group tied to Russian intelligence.

Security researchers believe hackers have exploited a vulnerability in a CMS editor called OctoberCMS, which was patched by the vendor back in March 2021. We can assume that Ukrainian affected agencies didn't keep their systems updated and ended up being vulnerable t external attackers.

Relations between Russia and Ukraine are very tense amid concerns over an imminent invasion of Ukrainian territory by Russian forces. Cyberattacks are considered as a mean to further escalate these tensions and create panic in the population.

We have attributed a risk-level of 1 as the threat actor targets victims only in Ukraine. However this threat actor seems sophisticated and the cybersecurity community has begun to track it seriously. Some researchers have already written detection rules (i.e. Yara) to hunt for WhisperGate.

2 APPENDICES

2.1 External references

Update 10, 28/02/2022

https://cyberknow.medium.com/2022-russia-ukraine-war-cyber-group-tracker-6e08ef31c533

Update 6 and 7, 24/02/2022

https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/

https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf

Update 2, 01/02/2022

https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine

Update 1, 01/02/2022

https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine

2.2 Orange Cyberdefense resources

All IoCs that can be quickly operationalized (i.e. network, host-based IoCs) are available in CERT Orange CyberDefense Datalake platform:

https://datalake.cert.orangecyberdefense.com/gui/?query_hash=e4d0e4bbb0fddc1b308e0eedff9cbaa6

Yara rule by Orange Cyberdefense CERT:

```
rule HermeticWiper : malware {
   meta:
      description = "Hermetic Wiper loading epmntdrv.sys by resources"
```

```
        source = "OCD"
        date = "24/02/22"
        researcher = "Alexandre MATOUSEK"
        category = "apt"
    strings:
        $s1 = "\\\\.\\EPMNTDRV\\%u" wide fullword
        $s2 = "\\\\.\\PhysicalDrive%u" wide fullword
        $s3 = "%s%.2s" wide fullword
        $s4 = "\\\\?\\C:\\Windows\\System32\\winevt\\Logs" wide fullword
        $os1 = "DRV_XP_X86" wide fullword
        $os2 = "DRV_XP_X64" wide fullword
        $os3 = "DRV_X86" wide fullword
        $os4 = "DRV_X64" wide fullword
        $cert = /Hermetica Digital Ltd[0-1]/
    condition:
        uint16(0) == 0x5A4D and
        all of ($s*) and
        2 of ($os*) and
        $cert
}
```

Yara rule by Sentinel Labs:

```
rule MAL_HERMETIC_WIPER {
    meta:
      desc = "HermeticWiper - broad hunting rule"
      author = "Friends @ SentinelLabs"
      version = "1.0"
      last_modified = "02.23.2022"
      hash = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591"
    strings:
        $string1 = "DRV_XP_X64" wide ascii nocase
        $string2 = "EPMNTDRV\\%u" wide ascii nocase
        $string3 = "PhysicalDrive%u" wide ascii nocase
        $cert1 = "Hermetica Digital Ltd" wide ascii nocase
    condition:
      uint16(0) == 0x5A4D and
      all of them
}
```