

Cyber Threat Intel (CTI) Alert

TLP: GREEN

Date: February 25, 2022

Subject: Cyber Watch: Ukrainian/Russian Geopolitical Conflict

Key Takeaways

- On Thursday, February 24, 2022, Russian armed forces invaded Ukraine, culminating in military strikes against multiple Ukrainian cities.
- Multiple cyber events targeting Ukrainian critical infrastructure have preceded this physical conflict, and analysts assess that additional cyberattacks aimed at Ukraine and countries perceived as Ukrainian allies are highly likely to occur.
- As of this reporting, cyber incidents related to this activity include **distributed denial of service (DDoS) attacks, misinformation campaigns**, and the use of several different **malware variants**, many with the ability to destroy data (e.g., **WhisperGate, Cyclops Blink, and Hermetic Wiper**).
- On February 14, 2022, the United States Cybersecurity & Infrastructure Security Agency (CISA) advised all organizations to adopt a “Shields Up” approach in anticipation of cyberattacks.
- At this time, managed detection and response services at Kroll are not observing an uptick in activity related to this situation.
- Kroll recommends that all organizations take a proactive approach to cybersecurity during this period; Kroll will continue to monitor this rapidly developing situation and update clients accordingly.

Overview

Since March 2021, the number of Russian armed forces stationed along the Ukrainian border has steadily increased, with the number reaching an estimated 100,000 soldiers by December 2021. In January 2022, efforts to de-escalate border tensions went unresolved, culminating in a full-scale physical attack by Russian forces on February 24, 2022¹. Multiple cyberattacks have preceded this physical conflict, including destructive malware and distributed denial of service (DDoS) attacks against Ukrainian infrastructure. In parallel, actors reportedly affiliated with Russia are believed to be behind multiple misinformation campaigns attempting to highlight “Ukrainian aggression” and control the narrative around the ongoing tensions.

¹ <https://www.reuters.com/world/europe/putin-orders-military-operations-ukraine-demands-kyiv-forces-surrender-2022-02-24/>

Observed Malware Variants

Over the past few weeks, multiple new malware variants have been observed in cyberattacks on Eastern Europe targets. Specific targets included the Ukrainian financial institutions PrivatBank and Oschadbank, and Ukrainian state-operated entities. Organizations doing business with Ukrainian organizations or those who conduct business in countries likely to be perceived as Ukrainian allies may be impacted by these variants or others like them.

WhisperGate

WhisperGate History

On January 15, 2022, Microsoft's Threat Intelligence Center ("MSTIC") reported on a new destructive malware operation that was specifically targeting organizations and enterprises in Ukraine. According to MSTIC research, their analysts assessed that the WhisperGate malware first emerged on victim systems within Ukraine on January 13, 2022. Although it presented itself like ransomware, the malware was "destructive and designed to render targeted devices inoperable rather than to obtain a ransom".

Technical Analysis

Initial analysis of this malware indicated that it was a data wiper; however, further analysis identified two additional malicious stages to the malware. As of this writing, open-sourced reporting indicates a high degree of confidence in the security community in Microsoft's analysis of the initial WhisperGate samples.

Stage 1.exe Analysis

The initial **stage1.exe** file used in the WhisperGate malware was observed being created in directories typically used by actors in ransomware attacks, i.e., locations that are not commonly used for data storage. The first stage consists of overwriting the Master Boot Record ("MBR") on a victim system with a ransom note. Without the MBR, a computer cannot properly load its operating system. It should be noted that in Kroll's experience investigating ransomware matters and open-source reporting, overwriting the MBR is not standard practice for ransomware actors as it renders the device inoperable by the victim, making payment less likely².

Stage 2.exe Analysis

The **stage 2.exe** file, which comes into play during the second stage of the attack, is a malicious file corrupter downloaded from a web communication application known as Discord³. This malware variant

² <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>

³ <https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3>

locates various file extensions most commonly used in everyday user activity and overwrites the contents of the file⁴.

Cyclops Blink

History of Sandworm Group

The UK National Cyber Security Centre (NCSC) and US Cybersecurity & Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) have identified that the actor known as Sandworm Team, or Voodoo Bear, is using a new malware called **Cyclops Blink**. The NCSC, CISA, and FBI have previously linked the Sandworm Group to the Russian General Staff Main Intelligence Directorate's ("GRU") Main Center for Special Technologies (GTsST)⁵. Additionally, in 2020, six GRU United 74455 officers were indicted by the United States as being associated with the Sandworm group⁶. Previous operations of this group have been attributed to attacks in both 2015 and 2016 against Ukrainian electrical companies and other Ukrainian government organizations⁷.

Cyclops Blink Historical Analysis

Open- and closed-source reporting indicates that Cyclops Blink has been deployed since at least June 2019, primarily to WatchGuard devices, but it is likely that Sandworm Group would be capable of compiling the malware for other architectures and firmware.

The February 23, 2022, CISA alert indicated that Cyclops Blink is likely replacing VPNFilter malware that emerged in 2018. VPNFilter mainly targeted internet of things (IOT) devices, including routers, and network attached storage (NAS) devices.

Watchguard Vulnerability

According to US CISA, "only WatchGuard devices that were reconfigured from the manufacturer's default setting to open its remote management interfaces" are susceptible to attack⁸.

Cyclops Blink enters a network via a firmware update to the WatchGuard devices, which provides a mechanism to establish rootkit capabilities on the kernel, and consequently, makes it more difficult to remediate. Cyclops Blink then establishes a hierarchy among the infected devices by putting infected devices into clusters in order to provide anonymity to the command-and-control (C2) channel. Moreover, these communications are done via TLS and generated keys and certificates, rendering it much more difficult for victims to assess the malicious traffic on their network without proper Deep Packet Inspection ("DPI") or SSL stripping techniques.

⁴ <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>

⁵ <https://www.cisa.gov/uscert/ncas/current-activity/2022/02/23/new-sandworm-malware-cyclops-blink-replaces-vpnfilter>

⁶ <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>

⁷ <https://attack.mitre.org/groups/G0034/>

⁸ <https://www.cisa.gov/uscert/ncas/current-activity/2022/02/23/new-sandworm-malware-cyclops-blink-replaces-vpnfilter>

WatchGuard currently provides a method for detecting a Cyclops Blink compromise and will also work with a victim to provide mitigation steps due to the sophisticated nature of the infection at the firmware level⁹.

Cyclops Blink 2022 Analysis

As of February 23, 2022, the NCSC believes it is likely that Sandworm Group would be able to manipulate the old Cyclops Blink code, which was used for vulnerable WatchGuard devices in 2019, to work on other architectures and firmware. Given Sandworm Group's ongoing persistence in attacking Ukrainian government agencies and industrial control systems ("ICS") within the country's borders, security experts anticipate that new code will be developed to specifically exploit vulnerable systems in Ukraine.

Hermetic Wiper

According to ESET, on February 23, 2022, a new wiping malware, subsequently dubbed **Hermetic Wiper**, reportedly hit organizations in Ukraine. While widely believed only Ukraine was a victim of the new data wiping malware, other reports have surfaced indicating the attack has since spread outside of Ukraine's borders¹⁰. According to Sentinel One, ESET has not publicly disclosed at least one variant of this wiper. Based on outside reporting, this malware appears to have a valid digital certificate from April 2021 to April 2022¹¹. It primarily targets Windows-based computers, registering itself as **epmntdrv**, which subsequently opens the system up to the wiper to destroy data by attacking the Master Boot Record ("MBR").

Targeting

Current reporting by Zscaler indicates that one initial infection vector for the malware is via email that contains a malicious document (maldoc). Once the maldoc is opened, a compressed file is downloaded to the victim's system¹². This in turn leads to an assortment of malicious stager components until the subsequent C2 channel is open and Hermetic Wiper is dropped as the eventual payload .

Technical Analysis

Per multiple open-source reports, Hermetic Wiper targets the physical hard drive's MBR in the Windows operating system, along with any subsequent partitions mounted to that system. For both NTFS and FAT file systems, a direct call to a "bit fiddler" is utilized to initiate the corruption. Per Sentinel One's updated report, where NTFS file systems are concerned, this malware "walks" the Master File Table (MFT) in order to enumerate the NTFS artifacts along with the location of Windows logs. At the time of this writing, it is not yet known what this enumeration is intended to do; however, it is done prior to the "bit fiddler" being initiated and rendering the MBR useless.

DDoS Incidents

⁹ <https://detection.watchguard.com/>

¹⁰ <https://www.reuters.com/world/europe/ukrainian-government-foreign-ministry-parliament-websites-down-2022-02-23/>

¹¹ <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>

¹² <https://www.zscaler.com/blogs/security-research/hermetic-wiper-resurgence-targeted-attacks-ukraine>

On February 14, 2022, the Security Service of Ukraine (SSU) published an advisory stating that the country was experiencing a “wave of hybrid warfare”. The statement indicated that objectives of the attacks were to “sow anxiety in Ukrainian society”, pointing to reportedly fake and misleading information being posted online about the current tensions in the region¹³.

This advisory came after a report stating that the SSU disrupted 121 attacks against state information systems in January 2022. Most prevalent tactics observed in those attacks were malware, connection to C2 servers, brute force, and web application attacks¹⁴.

Subsequently, on February 15, 2022, several websites, including one belonging to the National Defense ministry, became unavailable due to a large-scale distributed denial of service (DDoS) attack according to the Ukrainian Information Security Centre¹⁵. Online banking services were also reportedly impacted by this attack, disrupting customer access to online payments and mobile banking applications.

Misinformation Campaigns

Misinformation Historical Background and Analysis

Misinformation campaigns have been increasingly popular among nation-states seeking to change public opinion or influence perspectives on a particular matter. Many misinformation campaigns are typically carried out through social media campaigns that leverage an intended target’s most prominent social media application¹⁶.

Misinformation – Current Events

In November 2021, Ukrainian websites belonging to government institutions were cloned and modified by alleged nation-state actors.¹⁷ The websites were targeted specifically due to their visibility to the Ukrainian population. These websites contained login pages that could be exploited to harvest credentials from victims. The stealing of these credentials could be used to help further disinformation campaigns on social media platforms.¹⁸ One of the cloned websites mimicked the official website of Ukraine’s president and featured a large button surrounded by text inviting visitors to “Support Mr. President.”¹⁹ When visitors click on the button, trojan-like malware is downloaded to the user’s device. The deployment of a trojan to a significant number of systems belonging to Ukrainian citizens could have a significant impact on the country’s internet infrastructure, if for example they are used in a DDoS attack.²⁰

¹³ <https://ssu.gov.ua/en/novyiny/zaiava-sbu-shchodo-proiaviv-hibrydnoi-viiny-v-informatsiinomu-prostori>

¹⁴ <https://ssu.gov.ua/en/novyiny/u-sichni-2022-roku-sbu-zablokuvala-ponad-120-kiberatak-na-ukrainski-orhany-vlady>

¹⁵ <https://www.reuters.com/world/europe/ukraine-reports-cyber-attack-defence-ministry-website-banks-tass-2022-02-15/>

¹⁶ <https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation>

¹⁷ <https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/>

¹⁸ *Ibid.*

¹⁹ *Ibid.*

²⁰ *Ibid.*

Best Practices and Recommendations

In light of the ongoing threat to information systems related to this conflict, organizations should closely review their cybersecurity posture and controls to minimize the risk of system disruption. The following guidance is based on Kroll expertise along with recent reporting from CISA and NCSC:

- Validate multifactor authentication is in place, particularly for remote access.
- Review software applications to ensure systems are running the most recent, patched versions, with a particular focus on applications which fall into CISA's Known Exploited Vulnerabilities²¹ catalog.
- Disable internet-facing ports or protocols that are not essential to business.
- Designate a crisis management team which can operationalize in the wake of a suspected incident to maintain business continuity.
- Test back-up procedures.
- Verify anti-virus deployment with full current definitions and recent scans.
- If running services such as industrial control systems or operations technology, confirm that manual controls are working in the event of network disruption.

Such recommendations are in line with previous reporting by Kroll highlighting 10 priority areas for cyber resiliency:

1. Multifactor Authentication
2. Virtual Private Network
3. Remote Desktop
4. Endpoint Detection and Response
5. Incident Response Planning
6. Infrastructure and Segmentation
7. Backups
8. Access Control
9. Security Control Training
10. Email Hygiene

These [10 essential cyber security controls](#) have been validated by our seasoned cyber experts and can greatly improve your security posture and resilience against a cyberattack when fully implemented.

Kroll is standing by to answer any questions you may have or assist with investigations related to these concerns if the need arises. You can reach us directly, 24x7, via our [global hotlines](#) or by contacting the practitioners below.

²¹ [hxxps://www.cisa.gov/known-exploited-vulnerabilities-catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)



Marc Brawner
Managing Director, Cyber
Risk
+1 615 585 2419
marc.brawner@kroll.com






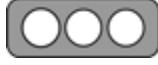
Keith Wojcieszek
Managing Director, Cyber
Risk
+1 443 295 5082
keith.wojcieszek@kroll.com



Laurie Iacono
Associate Managing
Director, Cyber Risk
+1 412 588 4337
laurie.iacono.com

Appendix

Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>