HC3: Analyst Note

March 01, 2022 TLP: White Report: 202203011700

The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector

Executive Summary

Russia's unprovoked attack on Ukraine has, as expected, spilled over into cyberspace. The scope of conflict now includes allies on both sides, many of whom also bring cyber capabilities with them. As of March 1, 2022, the Department of Health and Human Services is not aware of any specific threat to the US Healthcare and Public Health (HPH) Sector. However, in the interest of being proactive and vigilant, we are briefly reviewing the cyber capabilities of Russia and its allies and specifically two malware variants most likely to be utilized in any collateral attacks which may impact HPH in this campaign.

Report

Adversaries

There are three potential threat groups to the HPH currently related to the Russia-Ukraine conflict: organizations that are part of the Russian government, cybercriminal groups based out of Russia and neighboring states, and organizations that are part of the Belarussian government. This is not to say that other threat actors can or will not get involved, but these three groups are the primary focus at this time

Russia has for several decades been one of the most capable cyber powers in the world. Going back to the Moonlight Maze attacks against the US Department of Defense in the 1990s, Russian state-sponsored actors have been believed to be behind some of the most sophisticated cyberattacks publicly disclosed. Specifically, they are known to target adversarial critical infrastructure in furtherance of their geopolitical goals. They are suspected to be behind cyberattacks on Estonian government, media and financial targets in 2007, Georgian government sites in 2008, Kirgizstan Internet Service Provider attacks in 2009, Ukrainian government, military and critical infrastructure attacks in 2014 and again on Ukraine as well as many other countries with NotPetya in 2017.

The most prominent cybercriminal group to publicly support Russia are the Conti ransomware operators. Historically, they have targeted US healthcare organizations aggressively. They are known to conduct Managed Service Provider (MSP) compromise, big game hunting (targeting of large organizations), multi-stage attacks (leveraging other malware variants as part of the attack) and double and triple extortion (data theft combined with the ransomware attack). More information on the Conti operators can be found here. It is very possible that other cybercriminal groups have or will join the conflict, and will bring with them their custom tools, tactics, techniques, and weapons.

The Belarus government, an ally of Russia, is known to have cyber capabilities. The group known as UNC1151 is suspected of being part of the Belarusian military. UNC1151 have been reportedly attempting to compromise the e-mail accounts of Ukrainian soldiers with a phishing campaign. More information on them can be found here.

Wipers

There are two malware variants – both wipers – that have been observed in significant use against Ukraine in the last two months: HermeticWiper and WhisperGate.

HermeticWiper – This is a new form of disk-wiping malware (at least one version is identified with the filename Trojan.Killdisk) that was used to attack organizations in Ukraine shortly before the launch of a Russian invasion on February 24, 2022. There are a number of variants in the wild and therefore all of the details included in this report may not apply to all variants. We have included a number of industry reports at the end of this section as well as in the references section at the end of this report to allow analysts to dig deeper and better understand individual variants.

HC3: Analyst Note

March 01, 2022 TLP: White Report: 202203011700

HermeticWiper comes in the form of an executable file, which is signed by a certificate issued to Hermetica Digital Ltd. It contains 32-bit and 64-bit driver files which are compressed by the Lempel-Ziv algorithm stored in their resource section. The driver files are signed by a certificate issued to EaseUS Partition Master. The malware will drop the corresponding file according to the operating system (OS) version of the infected system. Driver file names are generated using the Process ID of the wiper

Figure 1: HermeticWiper Digital Signature (Source: SentinelLabs)

Once run, the wiper will damage the Master Boot Record (MBR) of the infected computer, rendering it inoperable. The wiper does not appear to have any additional functionality beyond its destructive capabilities.

It leverages a signed driver which is used to deploy a wiper that targets Windows devices, manipulating the master boot record in such a way that causes boot failure. The digital certificate is issued under the Cyprus-based company named "Hermetica Digital Ltd". (Note: This company likely does not exist or is not operational if it does) The certificate is valid as of April 2021 but it does not appear to be used to sign any files.

HermeticWiper adjusts its process token privileges and enables SeBackupPrivilege which gives the malware read access control to any file, regardless of whatever is specified in access control list.

One malware sample is 114KBs in size and roughly 70% of that is composed of resources. It abuses a benign partition management driver, empntdrv.sys. HermeticWiper enumerates a range of physical drives multiple times, from 0-100. For each Physical Drive, the \\.\EPMNTDRV\ device is called for a device number. EPMNTDrv (EaseUS Partition Master NT Driver) is a process that is part of EaseUs Partition Manager software platform by EaseUS. It then focuses on corrupting the first 512 bytes, the Master Boot Record (MBR) for each physical drive and then enumerates the partitions for all possible drives.

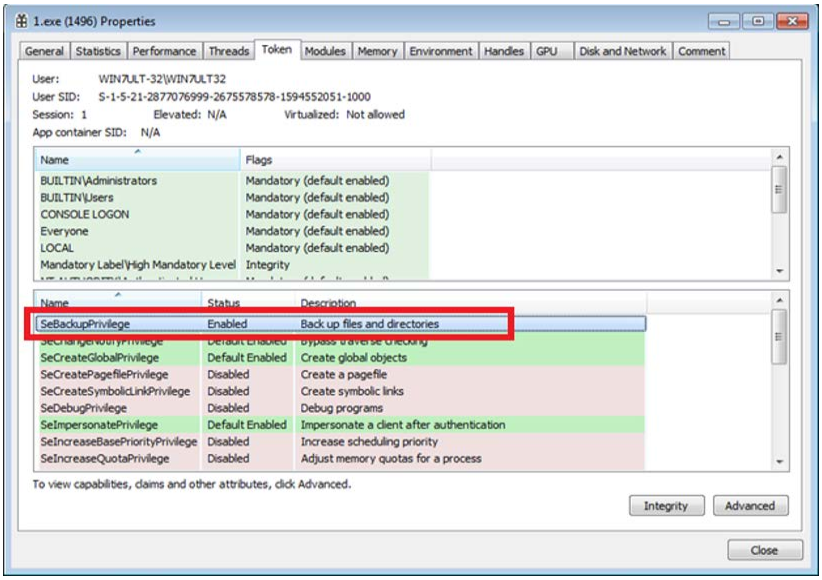

Figure 2: SeBackupPrivilege process token privilege modification (Source: IBM)

HermeticWiper differentiates between FAT (File Allocation Table) and NTFS (New Technology File System) partitions. In the case of a FAT partition, it calls to Windows APIs to acquire a cryptographic context provider and generate random bytes in order to corrupt the partition. For NTFS, it parses the Master File Table before calling the Windows APIs to acquire a cryptographic context provider and generate random bytes. Research also shows that it modifies several registry

keys, including setting the SYSTEM\CurrentControlSet\Control\CrashControl CrashDumpEnabled key to 0, which effectively disables crash dumps before the abused driver's execution starts. The system is then forced to shut down.

HermeticWiper has been observed targeting the financial, defense, aviation, and IT services sectors.

For more details on technical analysis of HermeticWiper, we recommend the following sources:

1. SentinelOne Labs report: HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine
2. ESET: HermeticWiper: New data-wiping malware hits Ukraine
3. Secureworks: Disruptive HermeticWiper Attacks Targeting Ukrainian Organizations
4. Symantec-Broadcom: Ukraine: Disk-wiping Attacks Precede Russian Invasion
5. CyberArc: HermeticWiper - What We Know About New Malware Targeting Ukrainian Infrastructure (Thus Far)
6. Security Alert HermeticWiper: Stormshield's product response
7. IBM Security X-Force Research Advisory: New Destructive Malware Used In Cyber Attacks on Ukraine
8. Cisco Talos Threat Advisory: HermeticWiper
9. ZScaler: HermeticWiper & resurgence of targeted attacks on Ukraine
10. CISA Alert (AA22-057A) Destructive Malware Targeting Organizations in Ukraine

WhisperGate – This is a new form of disk-wiping malware that is believed to operate in three stages/parts – a bootloader that corrupts detected local disks, a Discord-based downloader and a file wiper. The WhisperGate bootloader complements its file-wiper counterpart. Both irrevocably corrupt the victim's data and attempt to disguise themselves as ransomware operations. Whispergate has been observed attacking organizations in Ukraine shortly before the launch of a Russian invasion on February 24, 2022. There are a number of variants in the wild and therefore all of the details included in this report may not apply to all variants. We have included a number of industry reports at the end of this section as well as in the references section at the end of this report to allow analysts to dig deeper and better understand individual variants.

```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us  $10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23'
054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

Figure 3: Fake ransom note (Source: CrowdStrike)

The first step of the bootloader overwrites the master boot record in order to display the fake ransom note. The wiper itself will often be stored in one of several directories including C:\PerfLogs, C:\ProgramData, C:\, and C:\temp. It's often named stage1.exe. The wiper is known to execute via a collection of Python classes that work with network protocols called Impacket. The bootloader can access the target disk via the BIOS interrupt 13h, which provides sector-based disk read/write services using cylinder-head-sector addressing. It does this in logical block addressing mode and overwrites every 199th sector until end of the disk. It then moves onto the next disk on its list.

```
.3DM .3DS .7z .ACCDB .AI .ARC .ASC .ASM .ASP .ASPX .BACKUP .BAK .BAT .BMP .BRD .BZ .BZ2
.CGM .CLASS .CMD .CONFIG .CPP .CRT .CS .CSR .CSV .DB .DBF .DCH .DER .DIF .DIP .DJVU.SH
.DOC .DOCB .DOCM .DOCX .DOT .DOTM .DOTX .DWG .EDB .EML .FRM .GIF .GO .GZ .HDD .HTM
.HTML .HWP .IBD .INC .INI .ISO .JAR .JAVA .JPEG .JPG .JS .JSP .KDBX .KEY .LAY .LAY6
.LDF .LOG .MAX .MDB .MDF .MML .MSG .MYD .MYI .NEF .NVRAM .ODB .ODG .ODP .ODS .ODT .OGG
.ONETOC2 .OST .OTG .OTP .OTS .OTT .P12 .PAQ .PAS .PDF .PEM .PFX .PHP .PHP3 .PHP4 .PHP5
.PHP6 .PHP7 .PHPS .PHTML .PL .PNG .POT .POTM .POTX .PPAM .PPK .PPS .PPSM .PPSX .PPT
.PPTM .PPTX .PS1 .PSD .PST .PY .RAR .RAW .RB .RTF .SAV .SCH .SHTML .SLDM .SLDX .SLK
.SLN .SNT .SQ3 .SQL .SQLITE3 .SQLITEDB .STC .STD .STI .STW .SUO .SVG .SXC .SXD .SXI
.SXM .SXW .TAR .TBK .TGZ .TIF .TIFF .TXT .UOP .UOT .VB .VBS .VCD .VDI .VHD .VMDK .VMEM
.VMSD .VMSN .VMSS .VMTM .VMTX .VMX .VMXF .VSD .VSDX .VSWP .WAR .WB2 .WK1 .WKS .XHTML
.XLC .XLM .XLS .XLSB .XLSM .XLSX .XLT .XLTM .XLTX .XLW .YML .ZIP
```

Figure 4: List of file extensions used by the file corrupter (Source: Microsoft)

Stage2.exe is the downloader. Upon execution, stage2.exe downloads the file wiper malware hosted on a Discord channel, with the download link hardcoded in the downloader. Once executed in memory, the corrupter locates files in certain directories on the system with a set list of hardcoded file extensions that can be found in figure 4.

For more details on technical analysis of WhisperGate, we recommend the following sources:

1. Crowdstrike: Technical Analysis of the WhisperGate Malicious Bootloader
2. Microsoft: Destructive malware targeting Ukrainian organizations
3. CISA Alert (AA22-057A) Destructive Malware Targeting Organizations in Ukraine
4. Palo Alto Unit42: Threat Brief: Ongoing Russia and Ukraine Cyber Conflict
5. Avertium: How Whispergate Affects the U.S. and Ukraine
6. Netskope Threat Coverage: WhisperGate

The following timeline depicts some of the major cyber incidents over the last six weeks related to the Russia-Ukraine tension and conflict:

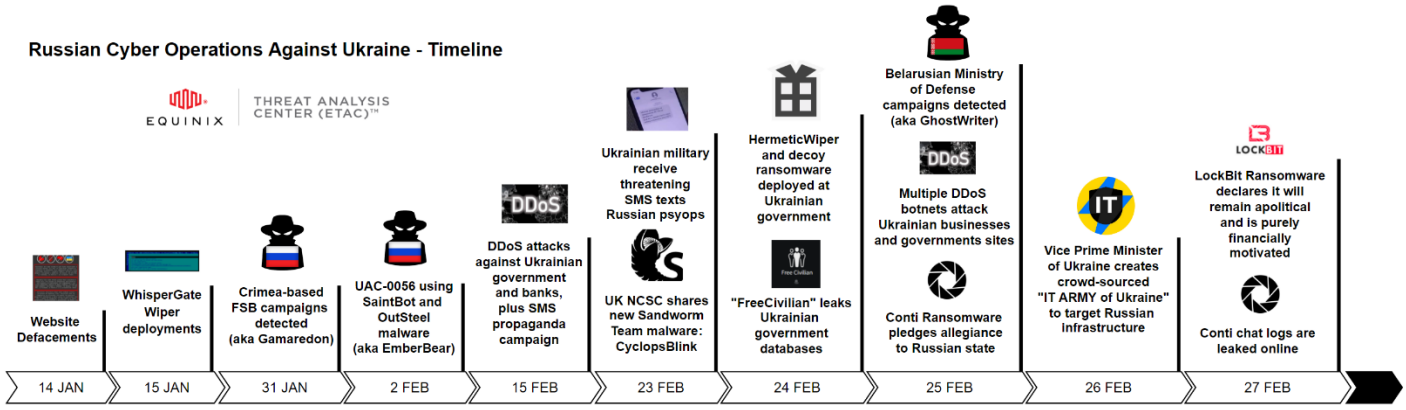

Figure 5: Timeline of significant cyber events (Source: CuratedIntel)

Finally, this report has only detailed two malware variants, however there are obviously many more cyber capabilities associated with the Russian government. Further information on Russian capabilities can be found here and information on their cyberspace capabilities can be found here.

Defense, Mitigations and Resilience

Each of the two malware sections above contain a list of resources at the end, many of which contain defense, mitigation and remediation recommendations. They also contain indicators of compromise. It's worth noting that indicators of compromise can become "burned" once they become public, which means as they become available to network defenders they are also available to the threat groups that they correspond to, who will often adjust their tactics, techniques, procedures, and weapons accordingly. We also recommend reviewing the references section at the end of this document. Finally, we recommend reviewing CISA's guidance on these malware variants which contains a number of useful defense and mitigation steps, along with indicators of compromise.

A Level-Set on Russia-Borne Cyber Threats
https://www.darkreading.com/omdia/a-level-set-on-russia-borne-cyber-threats

CONCERNS GROW OVER POTENTIAL NEW RUSSIAN CYBERATTACKS
https://duo.com/decipher/concerns-grow-over-potential-new-russian-cyberattacks

Ukrainian government calls out false flag operation in recent data wiping attack
https://therecord.media/ukrainian-government-calls-out-false-flag-operation-in-recent-data-wiping-attack/

Russian APT Steps Up Malicious Cyber Activity in Ukraine
https://www.darkreading.com/attacks-breaches/russian-apt-steps-up-malicious-activity-in-ukraine

Russia has been at war with Ukraine for years – in cyberspace
https://theconversation.com/russia-has-been-at-war-with-ukraine-for-years-in-cyberspace-176221

Ukraine says it's targeted by 'massive wave of hybrid warfare'
https://www.bleepingcomputer.com/news/security/ukraine-says-it-s-targeted-by-massive-wave-of-hybrid-warfare-/

How the Russia-Ukraine conflict is impacting cybercrime
https://intel471.com/blog/russia-ukraine-conflict-cybercrime-underground

Updates on the cyber phases of Russia's hybrid war against Ukraine. The British Foreign discloses a significant cyberattack (but not much else). ModifiedElephant seems to be engaged in digital frameups.
https://thecyberwire.com/newsletters/week-that-was/6/6

Ukrainian military agencies, banks hit by DDoS attacks, defacements
https://www.bleepingcomputer.com/news/security/ukrainian-military-agencies-banks-hit-by-ddos-attacks-defacements/

Russia says some troops withdrawing from Ukraine's border; NATO chief notes 'cautious optimism' but sees no de-escalation yet
https://www.washingtonpost.com/world/2022/02/15/ukraine-russia-nato-putin-germany/

The Ukraine Cyber Crisis: We Should Prepare, But Not Panic
https://www.mandiant.com/resources/ukraine-crisis-prepare-not-panic

Cyber, war and Ukraine: What does recent history teach us to expect?
https://news.sky.com/story/cyber-war-and-ukraine-what-does-recent-history-teach-us-to-expect-12542580

Ukraine Ministry of Defense confirms DDoS attack; state banks loses connectivity
https://www.zdnet.com/article/ukraine-ministry-of-defense-confirms-ddos-attack-state-banks-loses-connectivity/

Massive cyber-attack takes Ukraine military, big bank websites offline
https://www.theregister.com/2022/02/15/ukraine_ddos_attack/

Ukrainian government says websites for banks, defense ministry hit with DDoS attacks
https://www.cyberscoop.com/ukraine-banks-defense-ministry-ddos/

What CVE-2021-4034, Old-School Perl IRC Bots, Cryptominers and the Russia/Ukraine Situation Have in Common
https://www.countercraftsec.com/blog/post/cve-2021-4034-vulnerability-exploited-russia-vs-ukraine-situation/

DDoS attacks knock Ukrainian government, bank websites offline
https://www.helpnetsecurity.com/2022/02/16/ddos-ukrainian-government/

Cyber phases of a hybrid war.
https://thecyberwire.com/stories/b306f85093764164be77ba487edd67ad/cyber-phases-of-a-hybrid-war

Website disruptions were attempt to sow discord and cause panic, Ukraine officials say
https://www.cyberscoop.com/ukraine-websites-ddos-joint-briefing/

Ukrainian DDoS Attacks Should Put US on Notice–Researchers
https://threatpost.com/ukrainian-ddos-attacks-should-put-us-on-notice-researchers/178498/

White House pins Ukraine DDoS attacks on Russian GRU hackers
https://www.bleepingcomputer.com/news/security/white-house-pins-ukraine-ddos-attacks-on-russian-gru-hackers/

NCSC-NZ Releases Advisory on Cyber Threats Related to Russia-Ukraine Tensions
https://www.cisa.gov/uscert/ncas/current-activity/2022/02/18/ncsc-nz-releases-advisory-cyber-threats-related-russia-ukraine

White House attributes Ukraine DDoS incidents to Russia's GRU
https://www.cyberscoop.com/ukraine-ddos-russia-attribution-white-house-neuberger/

Technical Analysis of the DDoS Attacks against Ukrainian Websites
https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/

Russia denies accusations of false flag operation, cyber attacks on Ukraine
https://thehill.com/policy/international/russia/595026-russia-denies-accusations-of-false-flag-operation-blame-for-cyber

How a Russia-Ukraine conflict may affect cyberattacks
https://www.beckershospitalreview.com/cybersecurity/how-a-russia-ukraine-conflict-may-affect-cyberattacks.html

Officials: Russia likely cause of cyberattacks on Ukraine, but 'no specific credible threats to the US homeland'
https://www.scmagazine.com/analysis/cyberespionage/officials-russia-likely-cause-of-cyberattacks-on-ukraine-but-no-specific-credible-threats-to-the-us-homeland

EU to activate cyber response team to help Ukraine
https://www.kyivpost.com/world/eu-to-activate-cyber-response-team-to-help-ukraine.html

As Russian cybercriminals become emboldened, US banks prepare for potential attack
https://www.scmagazine.com/analysis/apt/as-russian-cybercriminals-become-emboldened-us-banks-prepare-for-potential-attack

Ukrainian government and banks once again hit by DDoS attacks
https://www.bleepingcomputer.com/news/security/ukrainian-government-and-banks-once-again-hit-by-ddos-attacks/

Russia-linked Sandworm reportedly has retooled with 'Cyclops Blink'
https://www.cyberscoop.com/sandworm-new-malware-cyclops-blink/

As Russia invades, Ukrainian government networks suffer high-profile DDoS disruption
https://www.cyberscoop.com/ukraine-government-networks-ddos-disruption-russia-invasion/

Important Detection and Remediation Actions for Cyclops Blink State-Sponsored Botnet
https://www.watchguard.com/wgrd-news/blog/important-detection-and-remediation-actions-cyclops-blink-state-sponsored-botnet

How to Prepare as Russia-Ukraine Situation Escalates
https://securityboulevard.com/2022/02/how-to-prepare-as-russia-ukraine-situation-escalates/

Russia's Sandworm Hackers Have Built a Botnet of Firewalls
https://www.wired.com/story/sandworm-cyclops-blink-hacking-tool/

Preparing for the Cyber Impact of the Escalating Russia-Ukraine Crisis
https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/

The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict
https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict

US ransomware attacks after Russian sanctions
https://www.cybertalk.org/2022/02/23/us-ransomware-attacks-after-russian-sanctions/

New data-wiping malware used in destructive attacks on Ukraine
https://www.bleepingcomputer.com/news/security/new-data-wiping-malware-used-in-destructive-attacks-on-ukraine/

Ukrainian gov't sites disrupted by DDoS, wiper malware discovered
https://www.zdnet.com/article/ukrainian-govt-sites-banks-disrupted-by-ddos-amid-invasion-fears/

Documenting and Debunking Dubious Footage from Ukraine's Frontlines
https://www.bellingcat.com/news/2022/02/23/documenting-and-debunking-dubious-footage-from-ukraines-frontlines/

Second data wiper attack hits Ukraine computer networks
https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/

Ransomware used as decoy in data-wiping attacks on Ukraine
https://www.bleepingcomputer.com/news/security/ransomware-used-as-decoy-in-data-wiping-attacks-on-ukraine/

EXCLUSIVE Ukraine calls on hacker underground to defend against Russia
https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/

Russia appears to deploy digital defenses after DDoS attacks
https://therecord.media/russia-appears-to-deploy-digital-defenses-after-ddos-attacks/

Anonymous Hackers Launch Cyber Ops Against Russia, Claim Government Site Takedowns
https://www.hstoday.us/subject-matter-areas/cybersecurity/anonymous-hackers-launch-cyber-ops-against-russia-claim-government-site-takedowns/

Hacker collective Anonymous declares 'cyber war' against Russia, disables state news website
https://www.abc.net.au/news/science/2022-02-25/hacker-collective-anonymous-declares-cyber-war-against-russia/100861160

AHA: Russia's Invasion of Ukraine Could Lead to Healthcare Cyberattacks
https://healthitsecurity.com/news/aha-russias-invasion-of-ukraine-could-lead-to-healthcare-cyberattacks

U.S. Declares Start of Russia's Invasion of Ukraine, Introduces Sanctions; "Cyber Shields Up," Says CISA
https://www.aha.org/advisory/2022-02-23-us-declares-start-russias-invasion-ukraine-introduces-sanctions-cyber-shields

Analysis shows new wiper malware in Ukraine cyberattack oddly thorough
https://www.scmagazine.com/analysis/cyberespionage/analysis-shows-new-wiper-malware-in-ukraine-cyberattack-oddly-thorough

Ukraine links phishing targeting armed forces to Belarus hackers
https://www.bleepingcomputer.com/news/security/ukraine-links-phishing-targeting-armed-forces-to-belarus-hackers/

HC3: Analyst Note

March 01, 2022 TLP: White Report: 202203011700

Ukraine: Disk-wiping Attacks Precede Russian Invasion
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

Ukraine Crisis: How the Rules of Cyber Warfare Are Changing
https://www.bankinfosecurity.asia/interviews/ukraine-crisis-how-rules-cyber-warfare-are-changing-i-5030

Threat Advisory: Cyclops Blink
https://blog.talosintelligence.com/2022/02/threat-advisory-cyclops-blink.html

HermeticWiper: New data-wiping malware hits Ukraine
https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

Ukraine links phishing targeting armed forces to Belarusian hackers
https://www.bleepingcomputer.com/news/security/ukraine-links-phishing-targeting-armed-forces-to-belarusian-hackers/

UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests
https://www.mandiant.com/resources/unc1151-linked-to-belarus-government

Current executive guidance for ongoing cyberattacks in Ukraine
https://blog.talosintelligence.com/2022/02/current-executive-guidance-for-ongoing.html