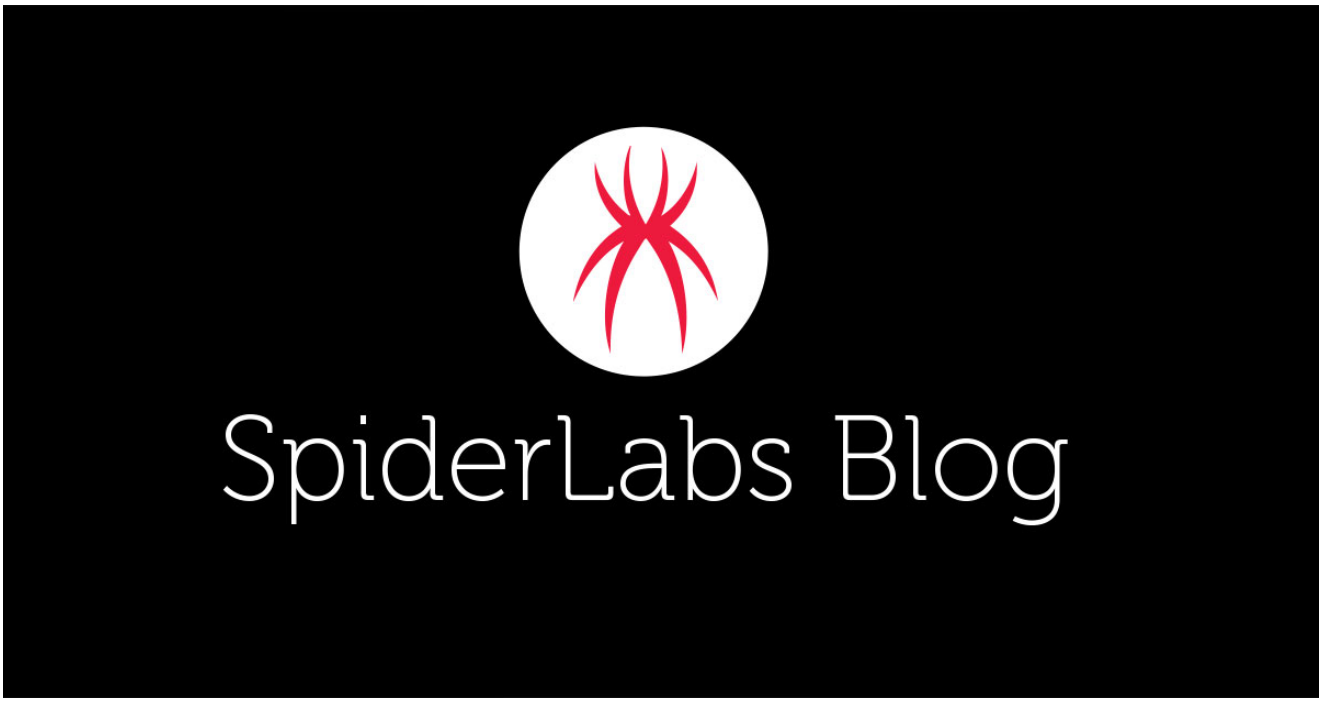
Overview of the Cyber Weapons Used in the Ukraine - Russia War



Blogs & Stories

SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

Observing the ongoing conflict between Russia and Ukraine, we can clearly see that cyberattacks leveraging malware are an important part of modern hybrid war strategy.

While conventional warfare is conducted on the battlefield and limited by several factors, cyber warfare continues in cyber space, offering the chance to infiltrate and damage targets far behind the frontlines.

Russia utilized cyberattacks during the initial phase of the invasion in February. Reports from Trustwave and other security researchers show that Russian cyberattackers have maintained pressure launching a series of attacks showing how malware has been used against organizations in Ukraine either to destroy or gain control over targeted systems.

In this article we will summarize some of the most prominent Russian threat actors involved and the malware tools used in cyberattacks against Ukraine.

Russian Threat Actors Behind the Attacks in Ukraine

Despite the high level and technical sophistication of the cyberattacks, and the Russian Special Services' ability to cover their tracks, several traces remain present after the attacks which leave no doubt of Russia's involvement in the current attacks against Ukraine.

As mentioned in a report released by the Estonian Foreign Intelligence Service and a UK government publication we can clearly draw some connections between the most notorious threat groups involved and Russian special services.

APT29, also known as Cozy Bear or The Dukes to the Russian Foreign Intelligence Service (SVR).

APT28, also known as Fancy Bear or Sofacy was traced to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Former GRU) Unit 26165.

SANDWORM, also known as Black Energy, was tied to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Former GRU) Unit 74455.

DRAGONFLY, also known as Energetic Bear or Crouching Yeti was identified as the Russian Federal Security Service (FSB) Unit 71330.

GAMAREDON, also known as Primitive Bear or Armageddon, traced to the Russian Federal Security Service (FSB) in November 2021. The Security Service of Ukraine (SSU) successfully identified individuals behind Gamaredon confirming their ties with FSB.

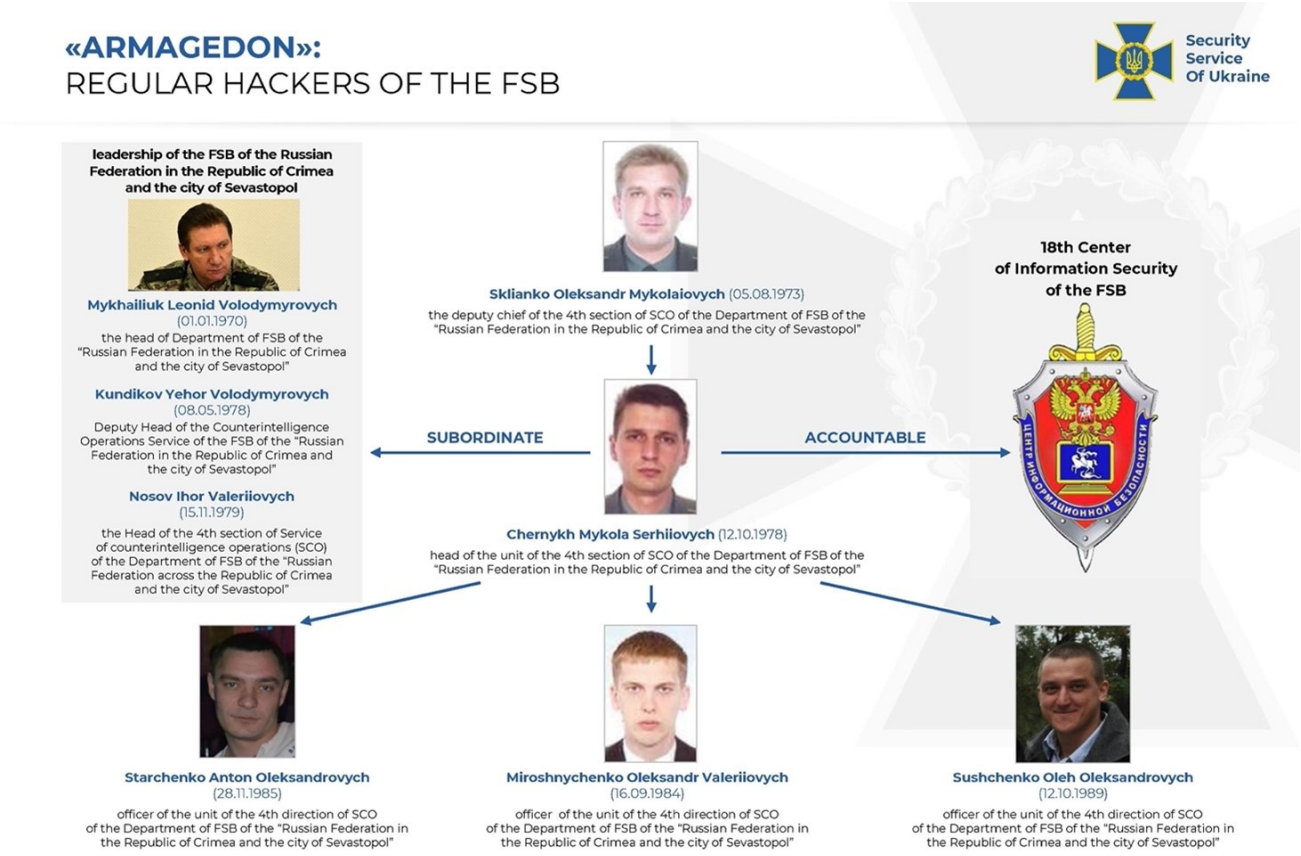


Figure 1 – Regular Hackers of the FSB
https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy

Other actively involved threat actors such as UNC2589, also known as Ember Bear or Lorec53, and InvisiMole do not present such clear ties with Russian special services. However, as published by ESET researchers, InvisiMole was found to be using server infrastructure operated by Gamaredon.

Figure 2 – Threat Actors and Russian Special Services Connections

Timeline of the Attacks & Malware Used

The flow timeline below illustrates the pressure placed on Ukrainian organizations and that government infrastructure is the attacker's primary target of the attackers. The variety of malware used, and involvement of Russian state-sponsored threat actors makes it evident that successful protection measures against attackers would require not only reactive but also a proactive approach.

Looking at the type of malware used, we can distinguish between 2 lines of attacks differentiated by the attacker's objectives:

- Destructive attacks are meant to destroy the data and render targeted systems inoperable.
- Espionage attacks are designed to establish a foothold and exfiltrate data from targeted systems. Malware used in the attacks usually provides attackers backdoor access with webcam and microphone captures, keylogging, and possibility to download and install additional components. Exfiltrated data includes operating system information, documents, pictures and stored passwords from web browsers and other software.

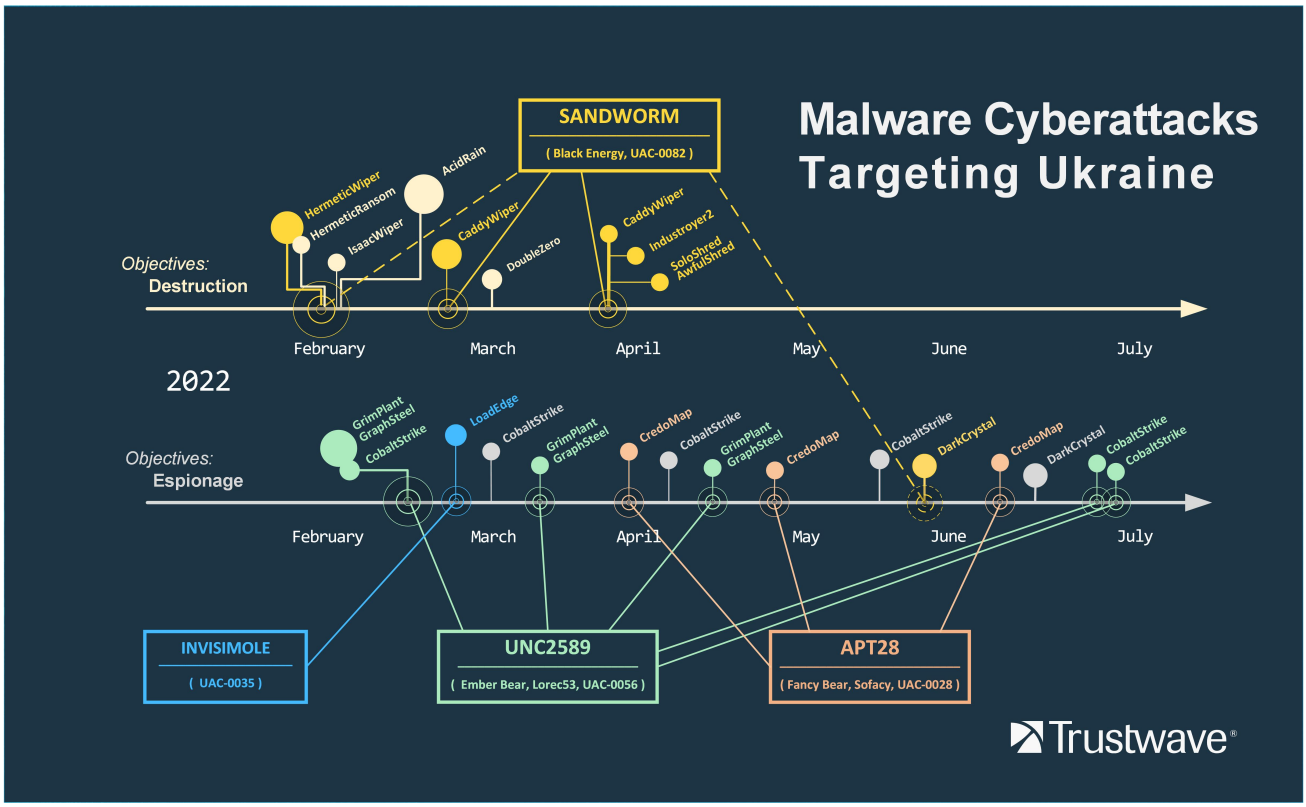


Figure 3 – Malware Cyberattacks Targeting Ukraine

Initial Vectors Used in the Attacks

The flow timeline below illustrates the initial attack vectors used to deploy malware. Spearphishing with malicious attachments or links are used to deliver CobaltStrike and GraphSteel backdoors or exploitation of vulnerabilities in public facing applications such as the VPN appliances compromised in the Viasat cyberattack are some of the most common intrusion methods used. While the initial attack vector of HermeticWiper, HermeticRansom and CaddyWiper are not entirely known, at least one security vendor reported that the attackers appear to have exploited a known vulnerability in Microsoft SQL Server (CVE-2021-1636).

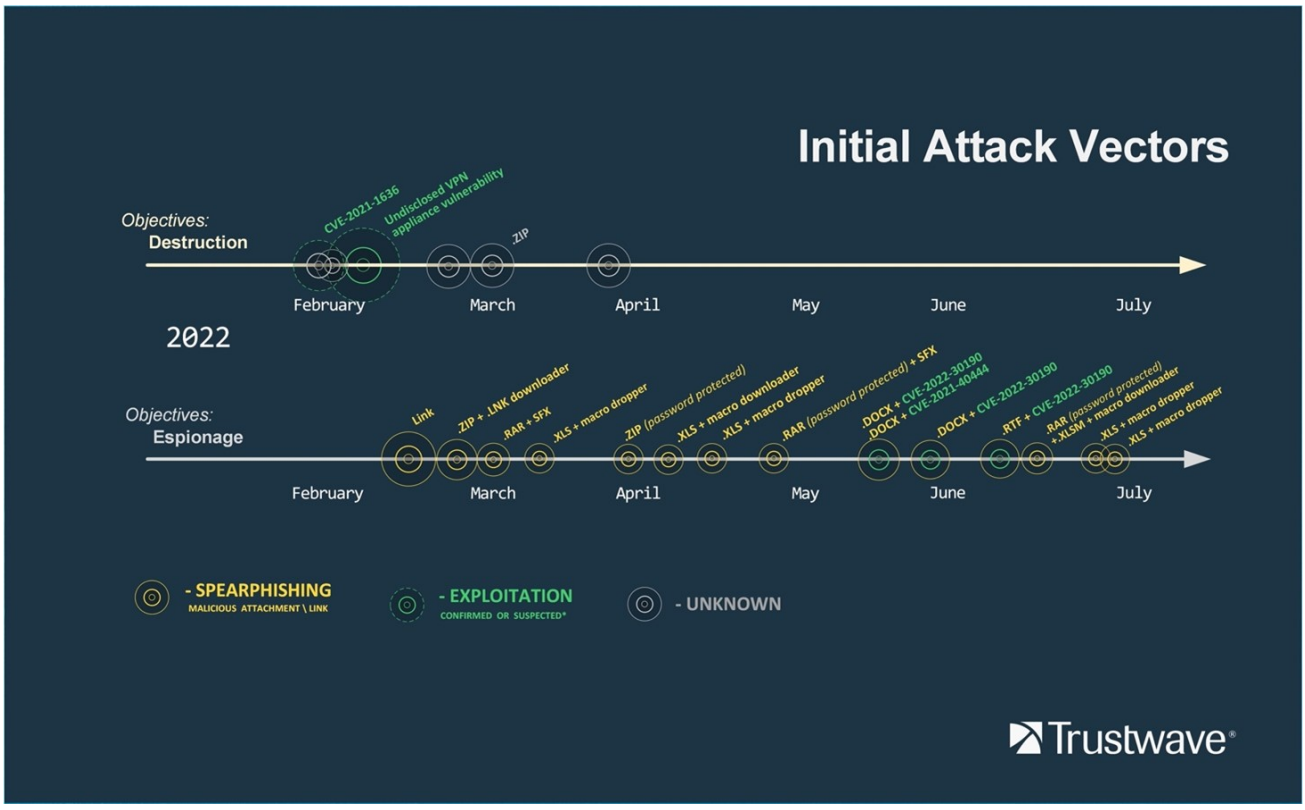


Figure 4 - Initial Attack Vectors

HermeticWiper

This wiper malware was given the name “HermeticWiper” based on a stolen digital certificate from a company called Hermetica Digital Ltd. HermeticWiper disables the Volume Shadow Copy Service (VSS) responsible for data backup and abuses legitimate drivers from the EaseUS Partition Master in order to corrupt data. As indicated by ESET and confirmed by the analysis of the Trustwave SpiderLabs Security Researchers, the wiper not only corrupts master boot record (MBR) and volume boot records, but also wipes files by defragmenting, rendering recovery impossible. It’s worth mentioning that HermeticWiper specifically targets Windows registry files ntuser.dat and Windows event logs to minimize the amount of usable forensic artifacts. Finally, the system restart is triggered rendering the targeted host inoperable.

It's interesting to note that the compilation timestamp of the HermeticWiper malware was December 28, 2021. This suggests that the February attacks were in preparation since at least that time.

APT responsible:

> *Sandworm (Black Energy,UAC-0082)*

Attacks reported:

February 23, 2022: HermeticWiper used in massive cyberattacks against high-profile Ukrainian organizations (Source: ESET)

IOCs for HermeticWiper:

SHA256:
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

HermeticRansom

HermeticRansom is written in Go language. As indicated by CrowdStrike's analysis, it enumerates available drives collecting a list of directories and files except for the Windows and Program Files folders. Selected file categories are renamed using the ransomware operator's email address and .encryptedJB extension, then file contents are encrypted using an AES algorithm. The ransomware also creates a read_me.html file in the Desktop folder which contains a ransom note with the attackers' contacts.

The encryption method is rather cumbersome and contains implementation errors making encrypted files recoverable. This flaw, together with political messaging found inside and deployment timing consistent with HermeticWiper, suggests that HermeticRansom was likely used as a distraction rather than a legitimate ransomware extortion attempt.

Attacks reported:

February 23, 2022: HermeticRansom used in cyberattacks against Ukrainian organizations (Source: ESET)

IOCs for HermeticRansom:

SHA256:
4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382

IsaacWiper

As indicated by ESET analysis, IsaacWiper is entirely different from HermeticWiper from a code perspective and is much less sophisticated. Upon execution it enumerates physical drives and volumes overwriting the existing content with random bytes. If a volume access is denied, the wiper creates a temporary directory and file within this directory. The name of the directory created will begin with the letters "Tmd" and file with the letters "Tmf;" the remaining part of the name will be randomly generated alphanumerical characters. It will then attempt to fill it with random data until the volume is out of space. The wiper also renames files it can't access to temporary names and then attempts to wipe the newly renamed file. IsaacWiper creates a log file *C:\ProgramData\log.txt.* where corrupting activity progress is saved.

APT responsible:

> Gamaredon (Primitive Bear, Armageddon)

Attacks reported:

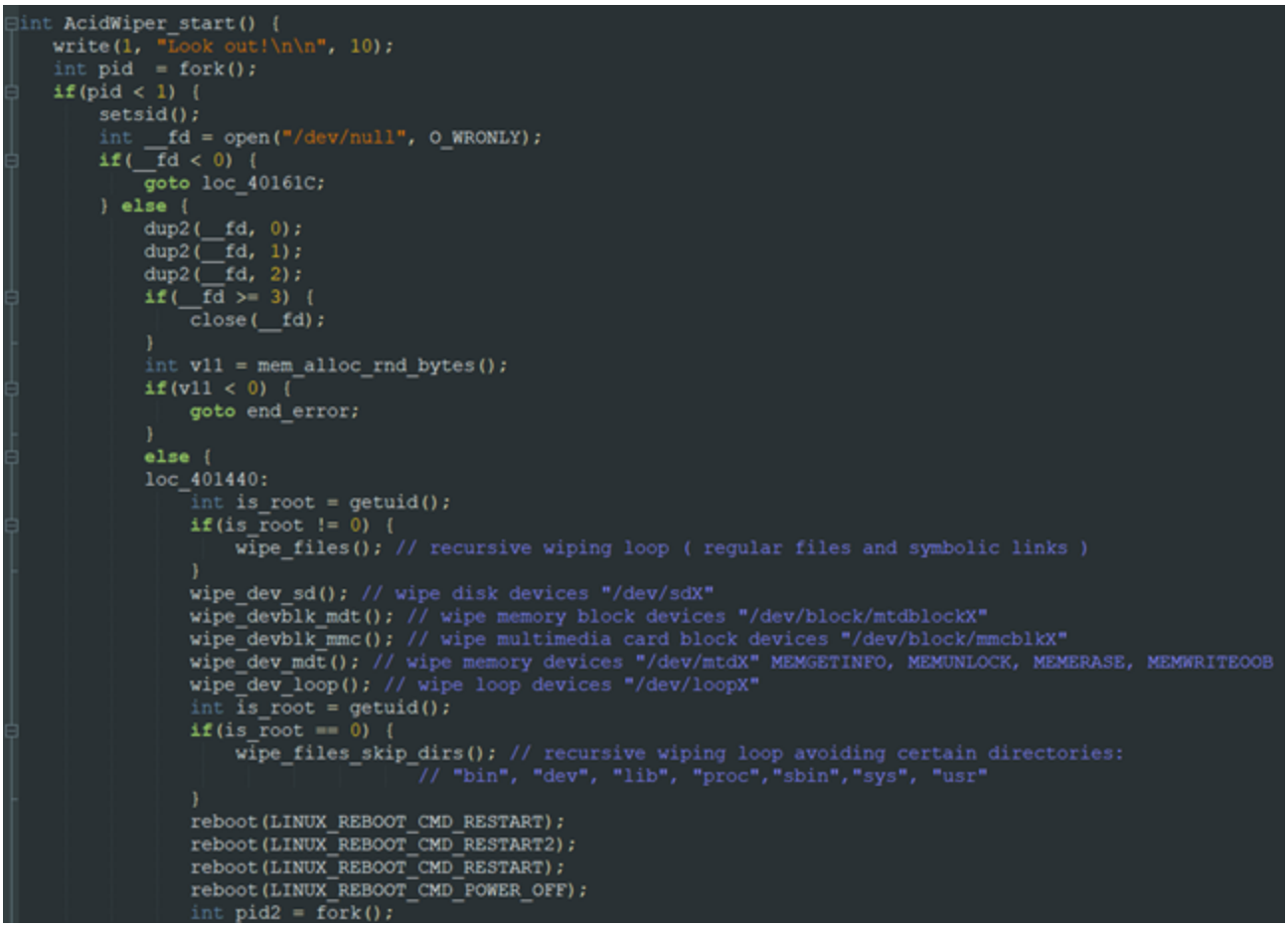
> February 24, 2022 - ESET: IsaacWiper used in cyberattacks against Ukrainian government organizations. (Source: ESET)

IOCs for IsaacWiper:

> SHA256: 13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033

AcidRain

As indicated by Trustwave SpiderLabs's analysis, AcidRain overwrites files and symbolic links with random data from the memory buffer in a recursive loop. If the wiper is executed with root permissions certain directories such as: 'bin,' 'dev,' 'lib,' 'proc,' 'sbin ' 'sys,' and 'usr' are avoided. The same random data buffer and write operation are used to wipe disk devices '/dev/sdX,' loop devices '/dev/loopX,' memory block devices '/dev/block/mtdblockX' and multimedia card block devices '/dev/block/mmcblkX.' Memory devices '/dev/mtdX' are wiped using MEMWRITEOOB ioctl instead. After the wiping is done a device reboot is triggered.



```
int AcidWiper_start() {
    write(1, "Look out!\n\n", 10);
    int pid  = fork();
    if(pid < 1) {
        setsid();
        int __fd = open("/dev/null", O_WRONLY);
        if(__fd < 0) {
            goto loc_40161C;
        } else {
            dup2(__fd, 0);
            dup2(__fd, 1);
            dup2(__fd, 2);
            if(__fd >= 3) {
                close(__fd);
            }
            int v11 = mem_alloc_rnd_bytes();
            if(v11 < 0) {
                goto end_error;
            }
            else {
            loc_401440:
                int is_root = getuid();
                if(is_root != 0) {
                    wipe_files(); // recursive wiping loop ( regular files and symbolic links )
                }
                wipe_dev_sd(); // wipe disk devices "/dev/sdX"
                wipe_devblk_mdt(); // wipe memory block devices "/dev/block/mtdblockX"
                wipe_devblk_mmc(); // wipe multimedia card block devices "/dev/block/mmcblkX"
                wipe_dev_mdt(); // wipe memory devices "/dev/mtdX" MEMGETINFO, MEMUNLOCK, MEMERASE, MEMWRITEOOB
                wipe_dev_loop(); // wipe loop devices "/dev/loopX"
                int is_root = getuid();
                if(is_root == 0) {
                    wipe_files_skip_dirs(); // recursive wiping loop avoiding certain directories:
                                            // "bin", "dev", "lib", "proc","sbin","sys", "usr"
                }
                reboot(LINUX_REBOOT_CMD_RESTART);
                reboot(LINUX_REBOOT_CMD_RESTART2);
                reboot(LINUX_REBOOT_CMD_RESTART);
                reboot(LINUX_REBOOT_CMD_POWER_OFF);
                int pid2 = fork();
```

Figure 5 – Reconstructed AcidRain's Main Routine

On February 24, 2022, the day the war started, a cyber-attack against Viasat's KA-SAT network impacted several thousand customers in Ukraine and tens of thousands across Europe. Spillover from this attack disabled the remote control of 5,800 Enercon wind turbines in Germany. As reported by Viasat, the attacker exploited Skylogic's VPN appliance gaining remote access to KA-SAT's network management segment. The attacker moved laterally to a specific segment part used to operate the network and executed legitimate, targeted management commands on a large number of residential modems, simultaneously. Specifically, these destructive commands overwrote key data in the flash memory on the SurfBeam modems.

AcidRain wiper being discovered shortly after, is a plausible fit for this attack pattern. Analysis of SurfBeam modems' firmware published in a Reversemode blog revealed the possibility to install arbitrary binaries without requiring either a signature verification or a complete firmware upgrade. Moreover, the first Virustotal submission for AcidRain's sample aligns with the incident investigation timeframe and Skylogic Mediterraneo infrastructure location.

Figure 6 – First AcidRain Sample Submitted to VirusTotal from Italy

IOCs for AcidRain:

SHA256: 9b4dfaca873961174ba935fddaf696145afe7bbf5734509f95feb54f3584fd9a

LoadEdge (InvisiMole)

As indicated by CERT-UA analysis, LoadEdge backdoor used in this campaign supports functionalities such as file execution, upload, download and deletion, obtaining system information, and interactive reverse shell over TCP port 1337.

Communication with the C&C server uses HTTP protocol and JSON formatted data, and persistence is provided by the HTA file creating an entry under the Run registry key. Drawing conclusions from the ESET research paper, LoadEdge resembles an upgraded version of InvisiMole's TCP downloader component used to download further backdoor modules called RC2FM and RC2CL, usually deployed as the first payload on a newly compromised computer. InvisiMole's RC2FM and RC2CL backdoors provide extended surveillance capabilities such as screen, webcam and microphone captures, documents exfiltration, collecting network information, and information about installed software.

APT responsible:

InvisiMole (UAC-0035)

Attacks reported:

March 18, 2022: LoadEdge used in email phishing attacks on Ukrainian government organizations (Source: CERT-UA)

IOCs for LoadEdge :

SHA256:
fd72080eca622fa3d9573b43c86a770f7467f3354225118ab2634383bd7b42eb

GraphSteel & GrimPlant

backdoors are both written in the Go language. As indicated by a BitDefender report, GrimPlant is a simple backdoor allowing for remote execution of PowerShell commands. Communication with the C2 server uses port 80 and is based on

gRPC – an open-source RPC framework. The communications are encrypted with TLS, and its certificate is hardcoded in the binary. GrimPlant sends a heartbeat containing a basic host information message every 10 seconds. Commands received from the C2 server are executed using PowerShell and the result is reported back.The GraphSteel backdoor is designed to exfiltrate data from infected machines. Communication with the C&C server uses port 443 and is encrypted using the AES cipher. GraphQL query language is used for communication. Files are exfiltrated from Documents, Downloads, Pictures, Desktop folders and all available drives from D:\ to Z:\. GraphSteel also exfiltrates basic system information, IP configuration, wifi profiles and steals credentials from the password vault using powershell.

APT responsible:

UNC2589 Ember Bear, Lorec53, UAC-0056)

Attacks reported:

- April 26, 2022: GraphSteel & GrimPlant used in email phishing attacks on Ukrainian government organizations (Source: CERT-UA)
- March 28, 2022: GraphSteel & GrimPlant used in email phishing attacks on Ukrainian government organizations (Source: CERT-UA)
- March 11, 2022: GraphSteel & GrimPlant used in email phishing attacks on Ukrainian government organizations (Source: CERT-UA)

IOCs for GraphSteel:

- SHA256: 47a734e624dac47b9043606c8833001dde8f341d71f77129da2eade4e02b3878
- SHA256: 8e77118d819681fdc49ce3362d8bfd8f51f8469353396be7113c5a8978a171f6

IOCs for GrimPlant:

SHA256: aca731d34c3e99d07af79847db369409e92e387520e44285608f18877b3a1d79

DoubleZero

DoubleZero is a .NET wiper malware. Our analysis indicated that execution stops immediately if the machine is a domain controller, otherwise it enumerates all the drives mounted to the machine and overwrites files with zero blocks, except for a specific hardcoded list of the system locations. Then the wiper moves on to the destruction of system files. In the end, the “lsass” process responsible for enforcing the security policy on the system is terminated and all the subkeys in the HKLM, HKCU, and HKU registry hives are destroyed. Once all the destructive activity has been completed, the wiper will shut down the system.

Attacks reported:

March 22, 2022: DoubleZero used in cyberattacks on Ukrainian enterprises (Source: CERT-UA)

IOCs for DoubleZero :

SHA256: d897f07ae6f42de8f35e2b05f5ef5733d7ec599d5e786d3225e66ca605a48f53

CaddyWiper

As indicated by a Cisco Talos advisory, CaddyWiper dynamically resolves most of the APIs used to make detection and analysis more challenging. CaddyWiper's execution stops immediately if the machine is a domain controller, otherwise the malware will attempt to destroy files on "C:\Users" followed by wiping all available drives from D:\ to Z:\. This means that any network mapped drives attached to the system may be wiped also. It wipes a maximum of a 10MB chunk from the beginning of the file, likely as part of performance optimization. Next the wiper attempts to zero out each physical drive corrupting master boot record (MBR) and extended information about a drive's partitions.

APT responsible:

Sandworm (Black Energy, UAC-0082)

Attacks reported:

- April 8, 2022: CaddyWiper used in a targeted cyberattack against a Ukrainian energy provider (Source: CERT-UA)
- March 14, 2022: CaddyWiper used in cyberattacks against Ukrainian organizations (Source: ESET)

IOCs for CaddyWiper:

SHA256: a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea

AwfulShred, SoloShred

AwfulShred and SoloShred are malicious shell scripts designed to corrupt Linux systems. Our analysis revealed that the destructive activity of both scripts relies on a shred command with one overwrite pass, chosen to increase the data damage. AwfulShred is also obfuscated, and its functionality is somewhat sophisticated. Prior to wiping the data, it disables and corrupts Apache, HTTP and SSH services, deactivates the swap file, and clears bash history. Finally, a system reboot is triggered, rendering the targeted host inoperable.

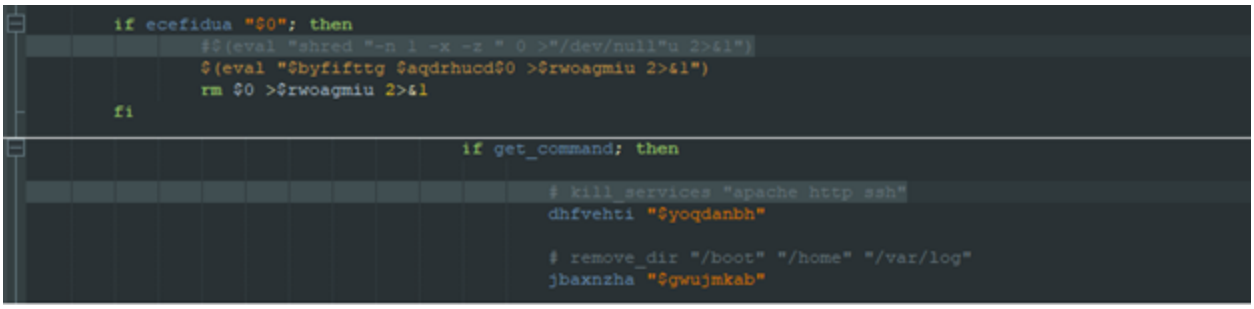


Figure 7 – Deobfuscated Commands Revealing AwfulShred Functionalities

APT responsible:

Sandworm (Black Energy, UAC-0082)

Attacks reported:

April 8, 2022: AwfulShred and SoloShred used in a targeted cyberattack against a Ukrainian energy provider (Source: CERT-UA)

IOCs for AwfulShred:

SHA256:
bcdf0bd8142a4828c61e775686c9892d89893ed0f5093bdc70bde3e48d04ab99

IOCs for SoloShred:

SHA256:
87ca2b130a8ec91d0c9c0366b419a0fce3cb6a935523d900918e634564b88028

Industroyer2

Industroyer2 is a sophisticated piece of malware targeting industrial control systems (ICS). As indicated by Nozomi Networks' analysis, it specifically abuses the IEC 60870-5-104 (IEC 104) protocol used in electric power control systems. Unlike its predecessor, Industroyer, Industroyer2 is a standalone executable consisting of a backdoor, loader, and several payload modules. Its only feature is to cause electric outages by disrupting operation of transmission substations.

Once executed, Industroyer2 attempts to terminate legitimate processes responsible for IEC 104 service communication: PServiceControl.exe and PService_PPD.exe, then renames the original executables by appending the ".MZ" file extension and begins IEC 104 interaction with transmission substations, interrupting the circuit breakers operation. Substations IP addresses and ports were found hard-coded, meaning that the attackers had at least limited knowledge of their target.

APT responsible:

Sandworm (Black Energy, UAC-0082)

Attacks reported:

April 8, 2022: Industroyer2 used in a targeted cyberattack against a Ukrainian energy provider (Source: CERT-UA)

IOCs for Industroyer2:

SHA256:d69665f56ddef7ad4e71971f06432e59f1510a7194386e5f0e8926aea7b88e00

CredoMap

CredoMap is a .NET credential stealer used by the threat actor APT28. CredoMap steals cookies and stored passwords from Chrome, Edge and Firefox browsers. Depending on the version, stolen data is then exfiltrated via email or HTTP POST requests to the web backend.

APT responsible:

APT28 (Fancy Bear, Sofacy, UAC-0028)

Attacks reported:

- April, 11, 2022: CredoMap malware targeting users in Ukraine discovered (Source: GOOGLE TAG)
- May 6, 2022: CredoMap used in email phishing attacks (Source: CERT-UA)
- June 20, 2022: CVE-2022-30190 (Follina) weaponized RTF downloading CredoMap malware discovered (Source: CERT-UA)

IOCs for CredoMap:

SHA256: 710faabf217a5cd3431670558603a45edb1e01970f2a8710514c2cc3dd8c2424

DarkCrystal RAT

DarkCrystal RAT or DCRat is a commercial Russian .NET backdoor that can be purchased in underground forums and is designed primarily to spy on victims and steal data from compromised hosts; DCRat supports surveillance using screen and webcam captures, keylogging as well as files and credentials theft. Other interesting features include persistence using registry, stealing clipboard contents, command execution and DOS attack function. DCRat communicates with the C2 server via HTTP using GET and POST requests.

Dark Crystal RAT (DCRat) appeared at the beginning of 2019. During its operation, the RAT got a lot of followers and clients. The malware became widely known for a variety of plugins including Stealer, Hidden Remote Desktop, file manager, and anonymous operation (via TOR proxy). The software was distributed on a subscription basis: two months for 600 RUB (~9.5 USD), one year for 2500 RUB (~39 USD), and a lifelong subscription would cost you 4500 RUB (~70 USD).

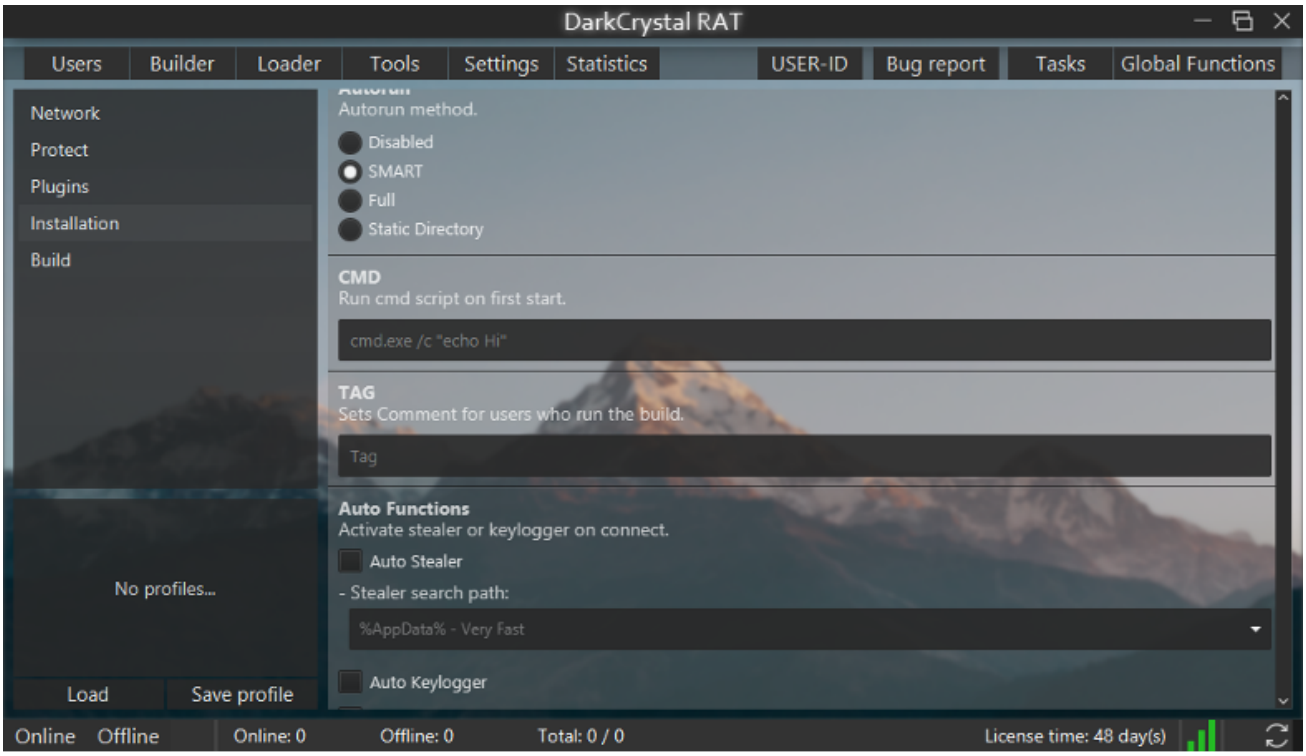


Figure 8 – DarkCrystal RAT

The DCRat code has been available on GitHub since at least March 2021. The versatility of the RAT, its abilities, and its low price make it so popular that even government-affiliated groups were choosing it for their operations.

Attacks reported:

- June 24, 2022: DCRat used in email phishing attacks on Ukrainian telecommunication operators (Source: CERT-UA)
- June 10, 2022: CrescentImp and DCRat used in a massive email phishing attack on Ukrainian media organizations (Source: CERT-UA)

IOCs for DarkCrystal RAT:

SHA256:
c84bbfce14fdc65c6e738ce1196d40066c87e58f443e23266d3b9e542b8a583e

Cobalt Strike

Cobalt Strike is a commercial penetration testing tool that allows an attacker to deploy a backdoor agent named 'Beacon' on the target machine. Although primarily designed for red teams, it is actively used by a wide range of threat actors from ransomware operators to APT groups for downloading and executing malicious payloads. The Beacon implant is file-less, in the sense that it consists of stage-less or multi-stage shellcode that is loaded either by exploiting a vulnerability or executing a shellcode loader. Communication with the C&C server is supported over several protocols including HTTP, HTTPS, DNS, SMB, named pipes as well as forward and reverse TCP with a wide range of modifications. Connections also can be established by chaining Beacons. Once an attacker gains access to a single system inside the compromised network, it can then be used to pivot internally into other systems.

APT responsible:

- UNC2589 (Ember Bear, Lorec53, UAC-0056)
- Other

Attacks reported:

- July, 7, 2022: Cobalt Strike Beacon used in email phishing attacks on Ukrainian government organizations. Attack attributed to UNC2589 APT (Source: CERT-UA)
- July, 5, 2022: Cobalt Strike Beacon used in email phishing attacks on Ukrainian government organizations. Attack attributed to UNC2589 APT (Source: CERT-UA)
- June 2, 2022: Cobalt Strike Beacon with CVE-2021-40444 and CVE-2022-30190 (Follina) exploits used in email phishing attacks on Ukrainian government organizations (Source: CERT-UA)
- April 18, 2022: Cobalt Strike Beacon used in email phishing attacks on Ukrainian government organizations (Source: CERT-UA)
- March 23, 2022: Cobalt Strike Beacon used in cyberattacks on Ukrainian government organizations (Source: CERT-UA)
- March 11, 2022: Cobalt Strike Beacon used in a massive phishing campaign targeting Ukrainian government organizations. Attack attributed to UNC2589 APT (Source: CERT-UA)

Conclusions

Without a doubt, sophisticated cyber weapons are key tools in the arsenal of a modern military, and the amount of global cyberwarfare will likely increase in the future.

First, with the constantly growing number of devices connected to the network, the attack surface is becoming massive, increasing the potential use cases for cyberwarfare.

Second, cyberwarfare is not bound by the territorial constraints of conventional warfare, offering the chance to infiltrate and damage targets far behind the frontlines.

Finally, compared to traditional warfare, cyberwarfare is invisible to the naked eye, does not risk lives on the side of the aggressor, and is cost effective.

With Ukraine being targeted by a variety of cyberattacks, we can see that even legitimate penetration testing tools can be hijacked and used as weapons. Cobalt Strike, originally created to train network defenders, is being actively abused by attackers in this conflict.

Protecting and Securing Your Network

Critical infrastructure is vital for the functioning of modern societies and will always be a lucrative target for attackers seeking monetary gain, political or military advantage. Understanding what digital technologies and tools are used in a conflict can help identify and mitigate future threats before the damage happens.

Unfortunately, people are usually the weakest link in the cybersecurity chain, as opening malicious attachments or links often leads to a compromise. Effective prevention strategy should include training programs, ensuring that personnel can identify and mitigate threats coupled with use of secure email gateways such as Trustwave MailMarshal, anti-malware and endpoint protection solutions.

Internet-facing systems should be always updated, protected by a firewall solution, regularly scanned for vulnerabilities, and audited for changes to the system integrity.

Trustwave’s researchers are continuously gathering more information on the latest cyberattacks, helping our customers to stay safe during these turbulent times.