What is HermeticWiper – An Analysis of the Malware and Larger Threat Landscape in the Russian Ukrainian War

deepinstinct.com/blog/hermeticwiper-malware-the-russian-ukrainian-cyber-war

March 1, 2022

Learn more

March 1, 2022 | Ido Kringel

On February 24, the Russian-Ukrainian conflict escalated into an invasion of Ukraine by Russian armed forces. However, these hostilities were not limited to the physical domain. Cyber warfare is happening in parallel to the armed conflict, becoming an inseperable part of the hostile exchanges between these nations.

Our Threat Research team noted various cyberattacks deployed by Russia in the weeks preceding the invasion aimed at sowing chaos and disrupting communications within Ukraine's government and military institutions. While the most publicized of these cyberattacks were the DDoS attacks, official government website take-downs, and website defacements, the most disruptive attack was a disk-wiping malware called WhisperGate which we covered in a previous post.

On February 23, one day before the larger Russian land invasion began, Ukrainian organizations were targeted by another destructive disk-wiping malware dubbed HermeticWiper designed to wipe a computer's hard disk data and destroy the Master Boot Record and partitions, making any impacted machines inoperable.

What is HermeticWiper

HermeticWiper makes use of a driver belonging to an outdated version of EaseUS Partition Master application, developed by CHENGDU YIWO Tech Development. The attackers used a benign, digitally signed kernel driver to evade detection while utilizing the driver's ability to interact with storage devices and acquire low-level disk access for retrieving partition information, corrupting the device's disks.

While the driver is digitally signed by 'Hermetica Digital Ltd' (hence the wiper name), the certificate is now revoked.

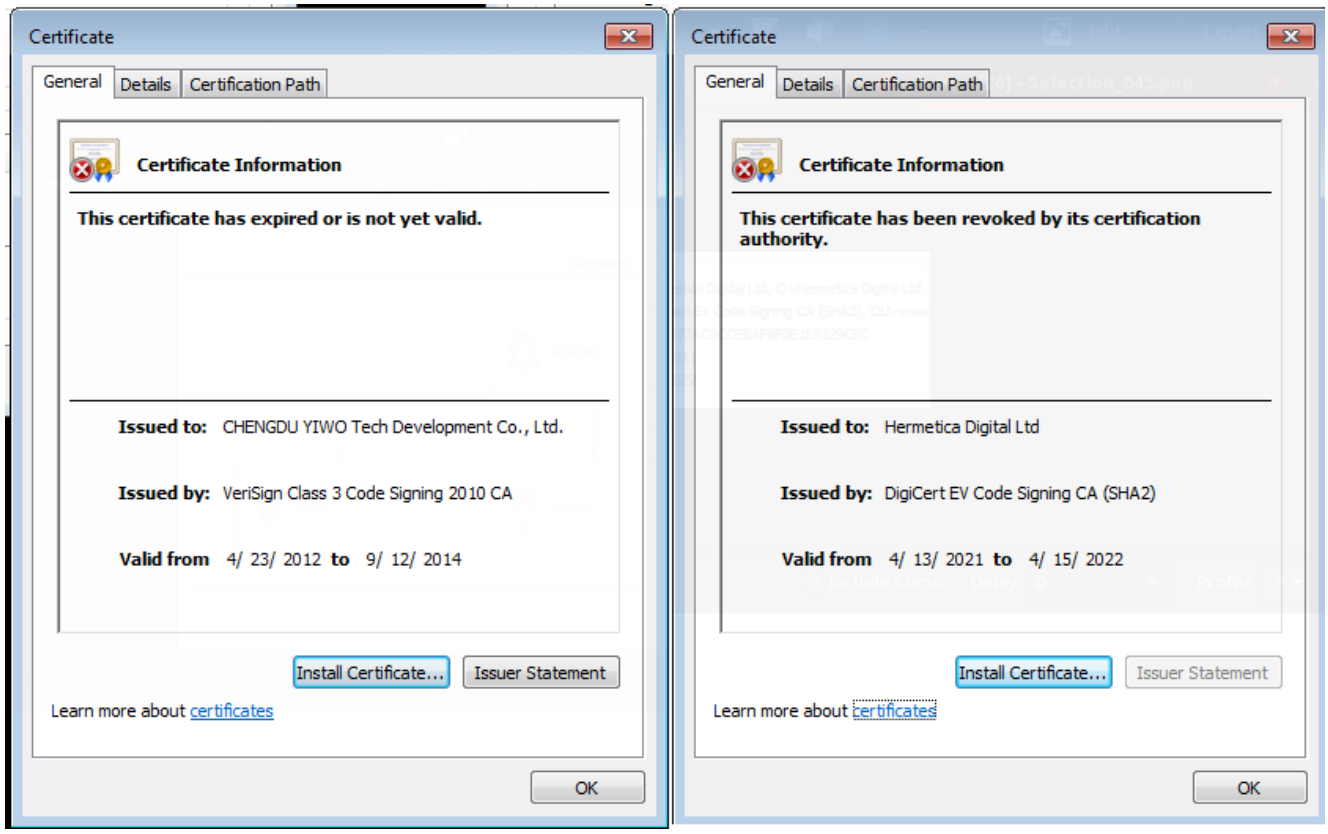


Figure1 – left – EaseUS invalid signed driver; right – HermeticWiper signed certificate

The malware stores 32-bit and 64-bit versions of the driver in MS-compressed copies within its resource section, deploying it according to the operating system version. Forensic analysis reveals that the malware has several variants, one with a timestamp dating to December 2021,

indicating the attack has been 'in progress' for quite some time.

We've observed several attacks which precede the execution of the wiper. In one case, the attackers exploited a known vulnerability in Microsoft SQL Server (CVE-2021-1636) to gain a foothold in one of the Ukrainian organizations. In a separate case, the attackers gained access to the network via malicious SMB activity against a Microsoft Exchange Server, which led to credential theft, and later to the deployment of the wiper. Several other methods were also employed, including the Apache Tomcat vulnerability, which allowed the attackers to run PowerShell commands, dump credentials, and execute the malware.

When executed, HermeticWiper will first gain higher privileges by utilizing Access Token Manipulation [T1134] and then obtain "SeBackupPrivilege" (which allows it to retrieve any file content) and "SeLoadDriverPrivilege" (which allows it to load/unload any driver). As we previously mentioned, HermeticWiper uses EaseUS signed driver in order to manipulate the disk.

Next, HermeticWiper will disable Volume Shadow Service (vss) and disable crash dumps by modifying specific registry keys, ensuring that no backups will be available and covering its tracks.

It will then enumerate the system's physical drives. For each, it will then corrupt the first 512 bytes and destroy the Master Boot Record (MBR).

While this should be enough to make any computer inoperable, HermeticWiper doesn't stop there. It next checks for NTFS or FAT file systems and corrupts them, ensuring that systems with both MBR and GPT drives are compromised. The Wiper will then force system shutdown to complete the wiping operation.

Similar to the previous WhisperGate attack, where the wiper was disguised as ransomware, the attackers appear to be using PartyTicket ransomware as a decoy in addition to the HermeticWiper malware to distract from the wiper attacks.

Russia-Ukraine Cyber Warfare

As we mention above, Russia started its cyberattack campaign long before the armed forces invasion. However, after the HermeticWiper attack began on February 23 we've seen a surge in cyber warfare between the two countries.

Here is the timeline of the major events:

- Feb 23
    - Ukraine's ministry of foreign affairs and the Security Service of Ukraine (SBU) websites were taken down while Ukrainian troops received threatening SMS messages with the aim of demoralizing them by urging them to flee or be killed.
    - Sandworm/VoodooBear group, both of which have previously been attributed to the Russian military intelligence service (GRU), use Cyclops Blink, a Linux malware which can extract device information and download additional payload.
- Feb 24

- The portal of the “Ministry of Agrarian Policy and Food” of Ukraine is defaced by a group named Free Civilian. The group offers databases containing sensitive government and citizens information for sale.
- The Anonymous hacking collective announced their support for Ukraine with the following message:

Figure2 – Anonymous group declaration

- Feb 25
  - A massive phishing email campaign targets Ukrainian troops’ private “i.ua” and “meta.ua” accounts, delivered by UNC1151 (aka GhostWriter) which relates to officers of the “Ministry of Defence of the Republic of Belarus.”
  - The infamous Conti group announces their full support the Russian government in the following blog post:

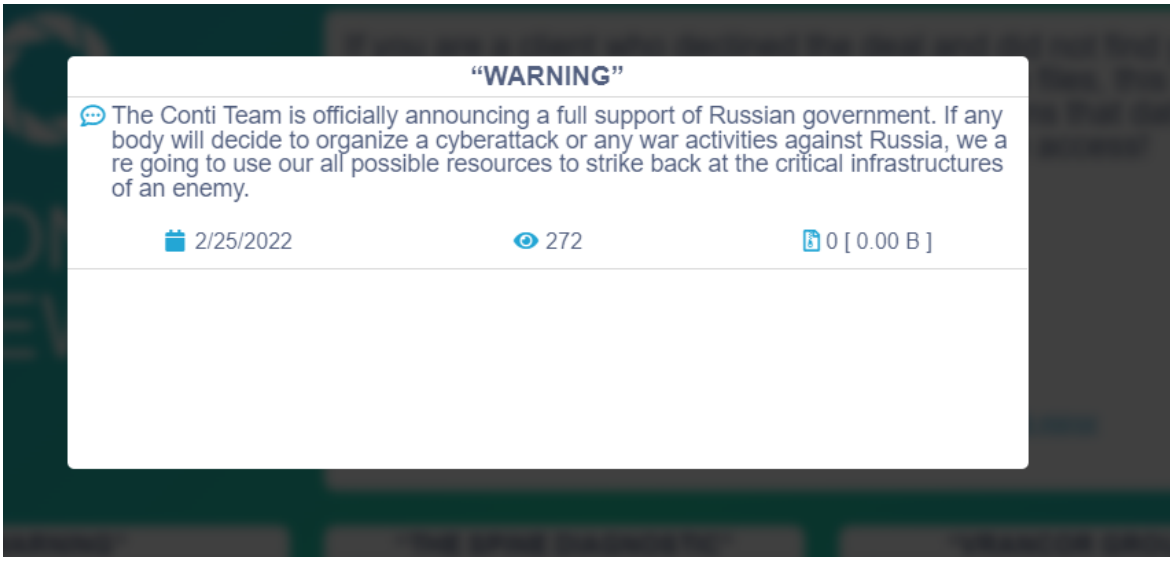


Figure 4 – Conti group declaration

- Feb 26 - The Vice Prime Minister of Ukraine Mykhailo Fedorov announces the creation of the “IT Army,” crowdsourced offensive operations against Russian infrastructure, aimed at recruiting cyber specialists willing to help.
- Feb 27 - The LockBit ransomware group declares they will leak all victims’ data.

- Feb 28 – One of Conti group members begins leaking data from the group's chat after their previous announcement supporting the Russian government.

```
Greetings,

Here is a friendly heads-up that the Conti gang has just lost all their
shit. Please know this is true.
https://twitter.com/ContiLeaks/status/1498030708736073734

The link will take you to download an 1.tgz file that can be unpacked
running tar -xzvf 1.tgz command in your terminal . The contents of the first
dump contain the chat communications  (current, as of today and going to
the past) of the Conti Ransomware gang.  We promise it is very interesting.

There are more dumps coming , stay tuned.
You can help the world by writing this as your top story.

It is not malware or a joke.
This is being sent to many journalists and researchers.

Thank you for your support

Glory to Ukraine!
```

IOCs

Context	sha256
EaseUS driver	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
EaseUS driver	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
EaseUS driver	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
EaseUS driver	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
EaseUS driver	96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
EaseUS driver	8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
EaseUS driver	23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
EaseUS driver	2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d
HermeticWiper	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591

HermeticWiper	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
HermeticWiper	ca3c4cd3c2edc816c1130e6cac9bdd08f83aef0b8e6f3d09c2172c854fab125f
HermeticWiper	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
HermeticWiper	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
PartyTicket	4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382

Predictions and guidance

The ongoing Russian-Ukrainian conflict is already causing a significant escalation in the quantity and scope of attacks from many, disparate parties. Elevated activity is being seen from state-sponsored groups, non-state-sponsored actors, and by independent hacktivists like the Anonymous group.

The unprecedented raft of sanctions enacted against Russia may invoke further retaliation and response in the form of cyberattacks by Russian-based organized cybercrime groups and state-sponsored or contracted actors. We have already seen several cyber gangs supporting Russia threaten to use their resources to strike back against nations and organizations that may coordinate cyberattacks against Russia.

We estimate the ongoing physical conflict escalation combined with the new sanctions will lead to a higher risk profile; this will be heightened for sectors associated with sanctions and have high economic or national security value. These may include financial services, aviation and aerospace, energy, and critical infrastructure.

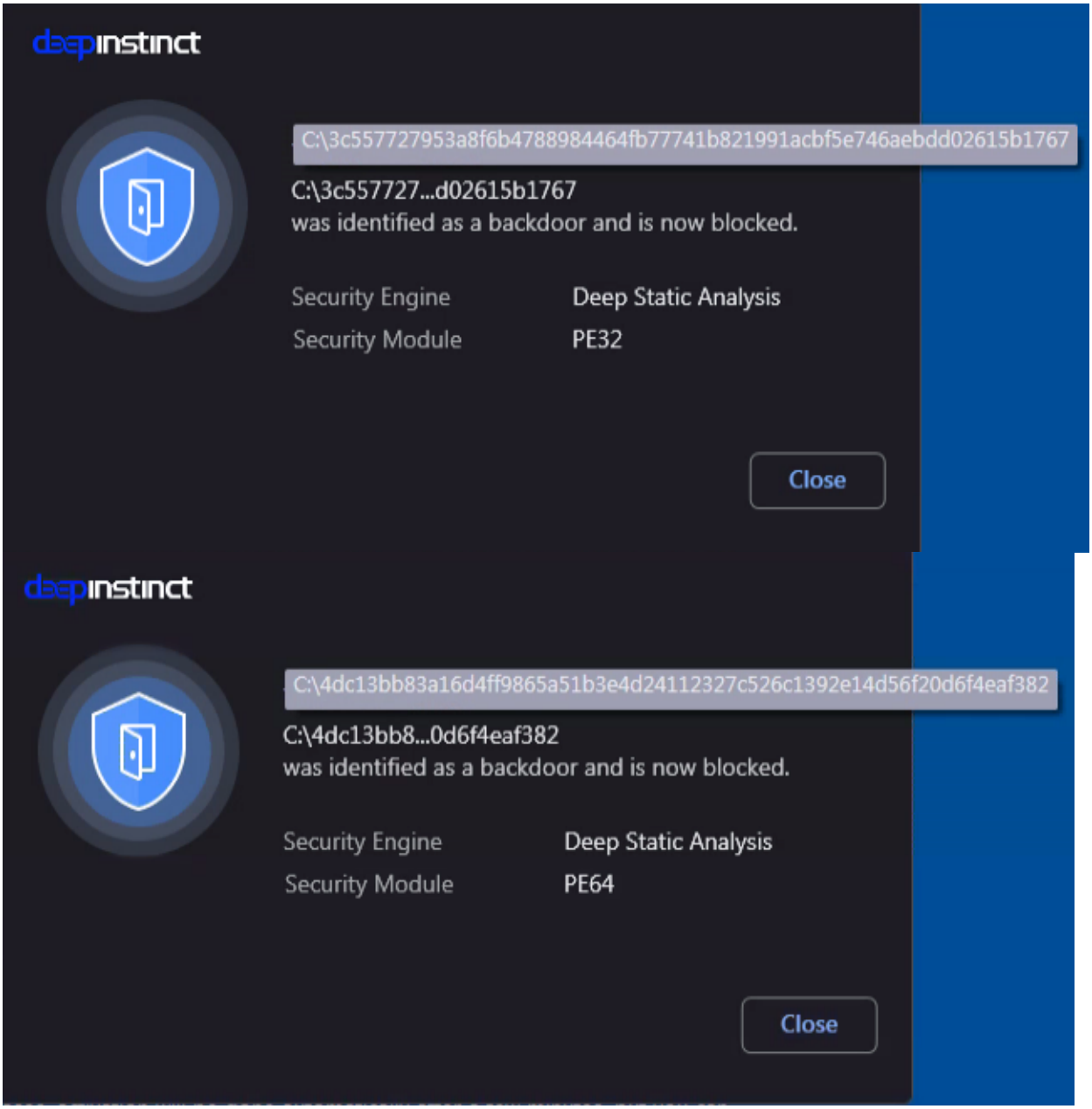
Following are some key points to consider or act upon given the changes in the risk profile:

- Threat actors are targeting organizations with phishing attempts related to the conflict. Security staff should remind or re-educate employees to minimize successful social engineering attempts.
- Every application in the organization can be a potential backdoor to the organization. These applications need to be updated frequently with the latest security patches. Organizations should apply a strict application control policy while limiting applications which are not critical to their business.
- Scripts are a powerful execution mechanism. There are entire industries (healthcare, for example) where most users in the organization have no need to execute scripts. Security staff should restrict scripts execution based on a user’s roles and devices.
- To ensure increased visibility, it is recommended to configure or enable additional layers of logging when and where available.

- Incident response requires considerable time and resources. The initial response of the security staff to a possible threat can make a huge difference in the overall impact of the attack impact. Trained security staff with a dedicated playbook for incident response scenarios should prevent additional infection and lateral movement inside the organization.
- In order to be as evasive as possible threat actors have learned to live-off-the-land. With the use of PowerShell and other libraries in the operating system, bad actors can stay under the radar. SOC operators should be extremely attentive to potential LOLbins attacks.

Protection from HermeticWiper with Deep Instinct

Deep Instinct prevents HermeticWiper and PartyTicket statically prior to execution, stopping it before it can deploy.



If you'd like to learn more, please request a demo.