SentinelOne blog

GET A DEMO

A CISO's Guide to the Security Impact of the Attacks on Ukraine

February 28, 2022
by SentinelOne

The situation in Ukraine presents many humanitarian and security challenges. We are obtaining a clearer view into a new form of hybrid warfare that we have previously only theorized about. SentinelOne is providing whatever technical resources we can to support Ukrainian organizations. We also have to recognize the larger threat posed by cyber threats leveraged against those that support sanctions, strategic Western sectors, or Ukrainian organizations. In this post, we offer a high-level overview of threats emerging as a result of the ongoing conflict in Ukraine.

To date, we have seen threat actors using three primary tactics: Distributed Denial of Service (DDoS) attacks, website defacements, and malicious wipers. While the techniques may be regarded as simple at a high-level, in conjunction they present a destabilizing force in limiting the availability of official information and services, either temporarily or permanently.

Denial of Service Attacks

In the early stages of the invasion, government websites belonging to Ukraine were taken offline by DDOS attacks. Specifically the Ukraine Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, and the Security Service of Ukraine websites all observed a disruption of service. Additionally, the financial sector in Ukraine also experienced a disruption of service. The UK government attributed the events to the Russian GRU.

HeremeticWiper | Crippling Systems in the Ukraine

On Wednesday, February 23rd, as the physical invasion of Ukraine was underway, researchers discovered that Ukrainian organizations were being targeted with a wiper dubbed HermeticWiper in reference to the digital certificate used to sign the sample.

HermeticWiper appears to be a custom written application with very few standard functions. It leverages the benign EaseUS driver to access physical drives directly as well as getting partition information.

The malware focuses on corrupting the first 512 bytes, the Master Boot Record (MBR), of every physical drive. While that should be enough for a device not to boot again, HermeticWiper proceeds to enumerate and corrupt the partitions for all possible drives. The malware is also able to differentiate between FAT and NTFS partitions and act accordingly to cause the most damage. HermeticWiper eventually initiates a system shutdown, finalizing the malware's devastating effect.

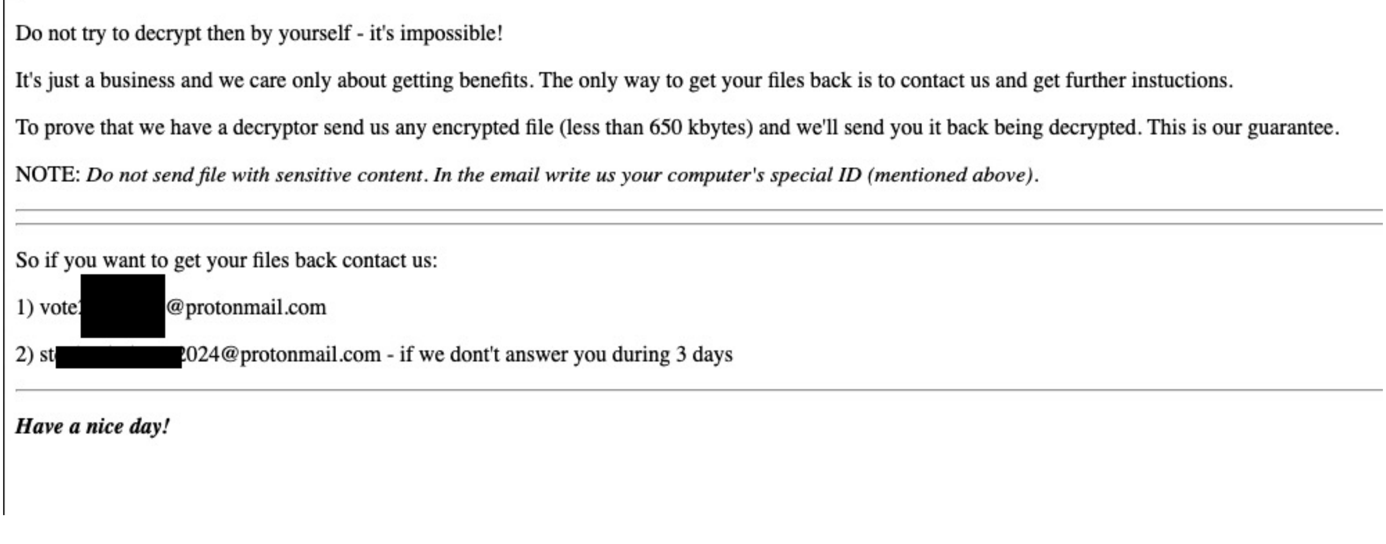
HermeticWiper is a 'fire-and-forget' tool. It has neither command-and-control nor self-spreading capabilities. The attackers need to establish access to deploy the wiper. In previous cases, they've done so via GPO, establishing a scheduled task to run the wiper as well as decoy ransomware.

HermeticWiper is far more thorough, better developed, and efficient than WhisperGate, a wiper deployed in Ukraine in January with a very limited distribution. Our assessment at this time treats the two as separate threats likely created by separate developers.

PartyTicket Ransomware

PartyTicket is the name SentinelLabs has given to the decoy ransomware component of the original HermeticWiper attacks. This malware was observed being delivered to targets alongside HermeticWiper and is believed to be used as a distraction while the devices are wiped.

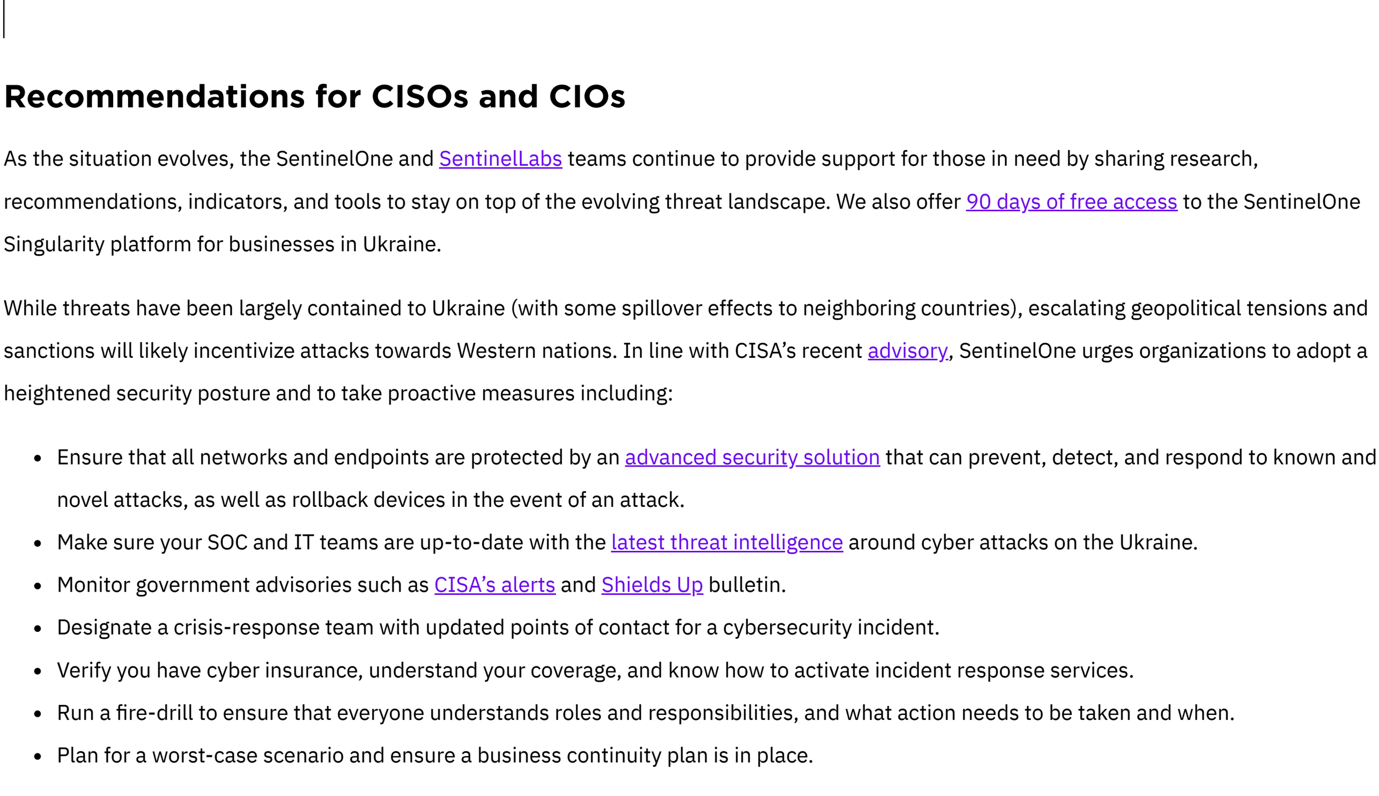
The ransomware is a custom Golang application that disrupts services and distracts defenders. PartyTicket is incredibly noisy, spawning hundreds of ancillary threads, likely resulting in an inadvertent local denial of service. The program's custom code is full of taunting references to the US government and the Biden administration.



```
_/C_/projects/403forBiden/wHiteHousE.baggageGatherings
_/C_/projects/403forBiden/wHiteHousE.lookUp
_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess
_/C_/projects/403forBiden/wHiteHousE.GoodOffice1
_/C_/projects/403forBiden/wHiteHousE.init
C:/projects/403forBiden/main.go
C:/projects/403forBiden/wHiteHousE/wHiteHousE.go
```

Project folders and function names referring to the Biden Administration

Similar taunts are present in the "ransom note" presented upon launch of the "ransomware".



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]d1e

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote[redacted]@protonmail.com

2) st[redacted]2024@protonmail.com - if we don't answer you during 3 days

Have a nice day!

Recommendations for CISOs and CIOs

As the situation evolves, the SentinelOne and SentinelLabs teams continue to provide support for those in need by sharing research, recommendations, indicators, and tools to stay on top of the evolving threat landscape. We also offer 90 days of free access to the SentinelOne Singularity platform for businesses in Ukraine.

While threats have been largely contained to Ukraine (with some spillover effects to neighboring countries), escalating geopolitical tensions and sanctions will likely incentivize attacks towards Western nations. In line with CISA's recent advisory, SentinelOne urges organizations to adopt a heightened security posture and to take proactive measures including:

- Ensure that all networks and endpoints are protected by an advanced security solution that can prevent, detect, and respond to known and novel attacks, as well as rollback devices in the event of an attack.
- Make sure your SOC and IT teams are up-to-date with the latest threat intelligence around cyber attacks on the Ukraine.
- Monitor government advisories such as CISA's alerts and Shields Up bulletin.
- Designate a crisis-response team with updated points of contact for a cybersecurity incident.
- Verify you have cyber insurance, understand your coverage, and know how to activate incident response services.
- Run a fire-drill to ensure that everyone understands roles and responsibilities, and what action needs to be taken and when.
- Plan for a worst-case scenario and ensure a business continuity plan is in place.

Conclusion

While cyberspace has become an integral part of our digital lives, it has also become a key aspect of geopolitical conflicts. As more offensive capabilities are available, they are used by governments for surveillance and disinformation. In the midst of a physical war, cyber has become an indispensable weapon to cripple defense systems, create chaos, and demoralize a population under duress.

SentinelOne's objective is to keep our customers safe while sharing our expertise with those who are in need. If you are a business in Ukraine or the surrounding area and your devices and networks might be impacted by the current crisis, we are here to help.

Read more about Cyber Security

- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- Bringing Identity to the Era of XDR
- Dealing with Cyberattacks | A Survival Guide for C-Levels & IT Owners
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- 6 Real-World Threats to Chromebooks and ChromeOS
- The 9 Biggest Cybersecurity Lies Told to CISOs