Bulletin: 2022- 03

Date:2/25/2022

Name: Russian Cyber Activity Rise

Classification: Threat Intel Report

Summary

Due to source sensitivity please use TLP classifications for distribution.

TLP:Green

Menlo Labs is tracking the Russian-Ukraine situation. Palo Alto Networks reported over the past two weeks, the conflict between Russia and Ukraine has escalated substantially, including significant increases in cyber attacks. Beginning on Feb. 15, a series of distributed denial of service (DDoS) attacks commenced. These attacks have continued over the past week, impacting both the Ukrainian government and banking institutions. On Feb. 23, a new variant of wiper malware named HermeticWiper was discovered in Ukraine. Shortly after, a new round of website defacement attacks were also observed impacting Ukrainian government organizations.

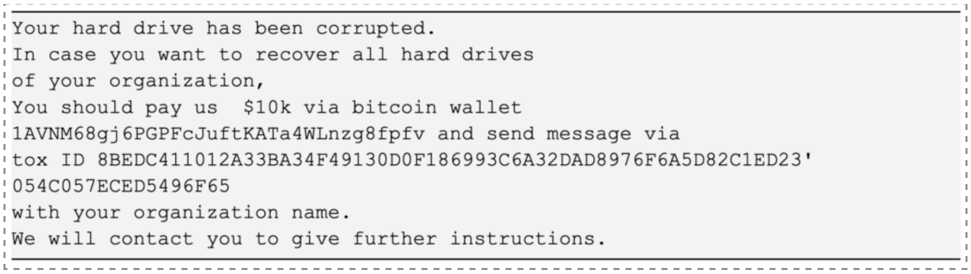
PaloAlto states that while these attacks are within Ukraine, their expectation is that similar attacks will be used against additional targets, should the situation continue to escalate.

Russian cyber activity in the past had no borders and we anticipate to keep seeing a rise in activity. We assess with moderate confidence that we may see an increase in scanning, phishing and other types of SWAG (stuff we all get) attacks.

BBC reported that several of Ukraine's bank and government department websites crashed on Wednesday. This corresponds to analyst reporting of increased APT and actor activity. It's not only cyber attacks that we are seeing.

SANS institution went on a live stream today (Feb, 25, 2022) and provided many resources for companies to scan their infracture and build up defenses against known TTPs and malware coming from Russian actors.

On Jan. 15, 2022, a set of malware dubbed WhisperGate was reported to have been deployed against Ukrainian targets. The incident is widely reported to contain three individual components deployed by the same adversary, including a malicious bootloader that corrupts detected local disks, a Discord-based downloader and a file wiper. The activity occurred at approximately the same time multiple websites belonging to the Ukrainian government were defaced.



```
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.
```

Sentinel labs reported that on February 23rd, the threat intelligence community began observing a new wiper malware sample circulating in Ukrainian organizations. The malware shows a signed driver by Hermetic Digital Ltd (now revoked) is being used to deploy a wiper that erases Windows devices, after deleting shadow copies and manipulating MBR after rebooting. The wiper has been named HermeticWiper.

Cybersecurity and Infrastructure Security Agency (CISA) put out an alert based on the United Kingdom's (UK) alert on Feb 23, 2022. The UK, National Cyber Security Centre (NCSC), the CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) in the U.S. have identified that the actor known as Sandworm or Voodoo Bear is using a new malware, referred to here as Cyclops Blink. The NCSC, CISA, and the FBI have previously attributed the Sandworm actor to the Russian General Staff Main Intelligence Directorate's Russian (GRU's) Main Centre for Special Technologies (GTsST).

TLP:Amber

Russian UNC2452 is also using the crisis to increase phishing activities. TTP's from a trusted source show two phishing emails using compromised legitimate email accounts to distribute a new downloader, BEATDROP, to European and North American diplomatic entities.

On social media Ukrainian citizens are going live and showing the world what is happening. During these streaming sessions the streamer is getting donations. Scammers have caught on to this and are recording the lives and broadcasting the recordings in order to get money. We anticipate these types of scam to increase and move to other platforms. The main platform being used for this type of scam is TikTok.

TLP:White

Menlo Protection

Menlo Labs continues to monitor the current cyber security landscape and will send notifications to inform customers of any increased cyber activity.

The Menlo platform is built with defense in depth in mind and has native integrations with AV, Sandbox detection technologies to provide additional defense.

The Menlo platform provides an additional layer of security against zero days and new malware campaigns by opening documents in a "safe" mode and letting the customer download a safe version of the document. The platform also completely eliminates browser exploits by safely rendering websites on our isolation platform.