CSIS Cybersecurity Brief
Russia / Ukraine Crisis

Assessment of the evolving threat landscape and our guidance/ recommendations

TLP:WHITE

Version: 1.0
Last Updated: 2022-02-25 12:44UTC

This report has been created by:
CSIS Security Group A/S
Contact: support@csis.com

1 Contents

2 Threat landscape overview

2.1 General outlook

In recent months, the CSIS Security Group (hereinafter “CSIS”) has observed and closely monitored a significant mobilization of digital weapons which are likely to be used in attacks against Ukraine and other Western targets.

The mobilization has been taking place on several fronts and includes spear phishing and phishing campaigns, mass scans, destructive wiper and ransomware, malware/RATs, DDoS attacks, Cobalt Strike implants, Crime as a Service, and the revival of major botnets.

Media worldwide has given extensive coverage to the bilateral cyber-attack threats issued by Russia and the US, as well as the extensive sanctions being levied against Russia by the US and many European countries.

It should be noted that Russia, having spent decades building it, is one of the most modern and advanced countries in the world in terms of offensive cyber capabilities.

As the situation on the ground in Ukraine continues to escalate, it is highly likely that military activity will continue to be accompanied by cyber operations – a hybrid war scenario. Cyber operations are likely to serve multiple purposes, ranging from taking control of the information space to denying access to state services and critical infrastructure.

It can also be assumed that the criminal groups operating from Russia during this period could receive support from the Russian authorities and government. This is likely to increase the number of incidents and require an increased ability to defend and respond quickly.

2.2 Confirmed threats targeting Ukraine

2.2.1 Wiper malware

Hard-drive wiping malware dubbed HermeticWiper was used in targeted attacks against organizations connected to the Ukraine government. The binary is signed using a valid digital certificate and abuses legitimate drivers to corrupt data on the hard drives. As a final step the wiper will reboot the victim computer.[1]

Reports show the wiper is dropped via the default (domain policy) GPO meaning that attackers had likely taken control of the Active Directory several weeks or in some cases even months in advance.

[1] Sources: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia, https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/, https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

Attackers appear to have gained access to the victim networks as early as November 2021 by exploiting known vulnerabilities targeting Microsoft Exchange or Apache Tomcat servers. Initial access was usually followed by credential theft, lateral movement, and the deployment of web shells.

2.2.2 Scanning activity

CSIS has observed an increase in service scans performed from IP addresses in Russia over the past week. Mass scans are targeting VPN appliances, exposed web services, or similar. This reconnaissance appears to be related to further vulnerability exploitation in Fortinet VPN servers or applications relying on Apache Log4j.

2.2.3 Ransomware

At least one group (Conti) has officially announced full support of the Russian Government and has threatened to mobilize all its resources to strike back on critical infrastructure in countries that get involved in either cyber-attacks or warfare against Russia.

2.2.4 DDoS attacks

Websites for several banks and government organizations in Ukraine were hit with multiple DDoS attacks in the past weeks. The attacks were not sophisticated in nature and only caused moderate damage. The targeted websites successfully recovered and were available after just several hours.[2]

[2] Source: https://netblocks.org/reports/ukraine-banking-and-defence-platforms-knocked-out-russia-conflict-JBQX7mAo

3 Actions taken by CSIS to protect our customers

This chapter describes the additional initiatives that CSIS has taken to increase the company's own resilience and the effectiveness of our services due to the increased threats of cyber-attacks stemming from the evolving crisis.

3.1 CSIS (internally)

3.1.1 Extended monitoring and increased log level verbosity

CSIS has added extended monitoring and increased log level verbosity to heighten detection earlier in the kill chain.

3.1.2 Supply-chain risk evaluation

CSIS has evaluated all suppliers and has found no additional areas of concern related to the current situation. We will remain vigilant and continue to monitor any updates that could impact supply-chain risk.

3.2 CSIS' service portfolio

3.2.1 Managed Detection & Response

CSIS always ensures that all team members are continuously updated on new threats, but in the light of this new situation we are exercising extra vigilance, treating all alerts and potential incidents with a higher level of scrutiny.

3.2.2 Emergency Response retainers

CSIS has briefed and continues to update all team members as the threat landscape develops. Further, CSIS has recently expanded our Emergency Response capability with additional team members.

3.2.3 Cyber Defense feeds

CSIS is constantly adding new indicators-of-compromise and indicators-of-attack to this feed based on the attacks that we analyze and those that are reported by other security vendors.

3.2.4 Threat Insights

CSIS is monitoring the situation and will ensure all Threat Insight customers will be updated with the latest threats as close to real-time as possible.

4 Guidance and recommendations

4.1 Initiatives and actions

Based on the cyber-attacks we have seen from the past, current cyber-attacks, and what we expect to see in the future; the following points summarize our key recommendations for any company to increase its security posture and resilience:

Essential/ highly time-critical

- Increase focus on 24/7 monitoring of logs and Detection & Response capabilities (e.g. streamline “isolation” of devices).
- Secure and minimize attack surface of external services (e.g. IP restriction and extra authentication).
- Ensure Incident Response readiness.
- Increase vigilance on patch management (especially externally available services).
- Ensure backups are up to date.
- Issue internal communication to raise awareness and vigilance of all employees.

Important/ time-critical

- Provide EDR coverage to all endpoints.
- Implement backup measures and security in several layers: on-premise, cloud and offline.
- Harden Active Directory (e.g. protected users).
- Limit usage of administrator accounts.
- Follow guidelines for secure remote connections (remote support, EDR, patch, user rights).
- Use two-factor authentication (especially on externally available services).

Important

- Continue to run awareness campaigns for employees.
- Implement DDoS protection.
- Undertake assessment of supply chain cyber risk.

The above recommendations are based on the following attack methods:

- Malware (e.g. ransomware, RATs, data stealers).
- Spear phishing, phishing, smishing.
- Interception.
- Data leakage.
- Supply chain attack.
- DDoS.
- Defacements.
- Disinformation.
- Brute force.

4.2 Recommended services from CSIS

4.2.1 Threat Insights

The cyber threat landscape has changed and matured significantly in recent years. Threats and the modus operandi of criminal groups have reached an elevated level of sophistication and complexity that makes it ever more challenging for companies to defend themselves.

Access to information that is based on intelligence and continuous research into threat actor groups, their activity and infrastructure is an essential part of ensuring an organization can improve its security posture and resilience.

You can read more about this service here: https://csis.com/cti_threat-insights/

4.2.2 Active Directory Health Check

Active Directory is the lifeblood of modern networks, and without it, the whole organization can grind to a halt. Attackers target the system to access and obtain new credentials to help them move laterally through a network. Its progressive nature and complex security framework give an unfair advantage to attackers. Based on observations made during incident response assignments and penetration test assignments, we can confirm that the IT criminals put significant effort towards attacking Active Directory.

You can read more about this service here: https://csis.com/consulting_ad-health-check/

4.2.3 Threat Assessment

Our Threat Assessment service delivers a proactive and in-depth look at your full network, at an endpoint level, through which we answer one critical question: “Are there any indications of threats (malicious actors) present on my network?”

As some of the current disruptive attacks use “already” installed backdoors this service is something you should consider for your regional offices at the very least, though we recommend assessing your entire corporate network.

You can read more about this service here: https://csis.com/consulting_compromise-assessment/

4.2.4 Cyber Defense Feeds

Our Cyber Defense Feed protects organizations' infrastructure against harmful connections to malicious domains and IP addresses which are under the control of cyber criminals.
Risk indicators are accompanied with a confidence score ranging from 50 to 100. This allows you to customize the implementation of the feed in a way that is aligned to your risk profile.

You can read more about this service here: https://csis.com/cti_cyber-defence-feed/

4.2.5 Vulnerability Scanning

CSIS has already seen exploitation of external services being used as an attack vector. We recommend running a vulnerability scan.

4.2.6 Incident Response Retainers

The moment your organization is hit by an incident, you need the ability to take key decisions quickly and get the situation under control. The IR Retainer puts our expert team at your disposal and ensures you get priority support.

You can read more about this service here: https://csis.com/emergency-response-retainers/

4.2.7 24/7 Managed Detection & Response

This service makes sure CSIS detects, analyzes, and mitigates threats within your network, even those that are persistent, complex, and stealthy.

You can read more about this service here: https://csis.com/managed-detection-and-response/

5 External links

We have compiled some relevant sources of information, guidance and insight for any company wishing to improve its security posture and resilience. Please see below ...
https://www.cisa.gov/shields-up
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences
https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience/@@download/fullReport (PDF dokument)

These links provide some additional perspectives on threats stemming from the Russia/Ukraine crisis specifically:
https://www.sans.org/webcasts/russian-cyber-attack-escalation-in-ukraine/
https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/
https://www.rapid7.com/blog/post/2022/02/25/russia-ukraine-staying-secure-in-a-global-cyber-conflict/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/