Russian-Ukrainian Cyber Warfare - Rewterz Threat Intelligence Rollup - Rewterz

Published: 2022-03-22 · Archived: 2026-04-05 15:08:59 UTC

What’s Happening?

Tensions between the Ukrainian and Russian governments were running high at the beginning of 2022. And now, in a span of two months, Russia has launched devastating and catastrophic attacks on Ukraine. Cities are being bombed, people are losing their homes, and a mass exodus of refugees is expected. While the war on land continues, cyberspace is being used to weaken Ukraine’s defenses.

Right now, we can’t deny the fact that the Russian security services are very capable in the cyber arena. Global IT sectors all around the world have welcomed Russian companies as full partners. On top of the list is Kaspersky, Zer0Data, ANY.RUN, Site Secure, are the other known cybersecurity companies in Russia.

According to resources, Kaspersky is the fourth largest anti-malware provider for Windows computers in terms of market share. If Russia decided to strike Asia and the Middle-East, it already had a ready-made channel: anti-malware software built to defend against that threat.

We at Rewterz are committed to providing actionable Threat Intelligence (TI) for humanitarian support, to secure and protect our customers globally.

```
Note:
```

```
Russian developers have developed a large portion of the code that organizations integrate into thei
```

```
Russian intelligence agencies are capable of enlisting the help of domestic criminals to achieve the
```

Outsourcing: A Competitive Advantage?

According to a report, Russia’s IT outsourcing industry reached $6.75 billion in 2020.

This figure itself is quite alarming! It’s because outsourcing also assigns control of IT operations to the vendor organization. If Russia becomes a hostile player, the control granted by the organizations to Russian outsourcing operations could result in handing over all of their passwords and authentication credentials.

Business Risks from the Escalating Cyber Warfare

The Russian-Ukrainian war will perhaps have the acute cyber risks on the business and financial sector. Economic sanctions and measures taken against Russia will ultimately warrant an asymmetric response from the immensely

capable country.

Organizations and countries that are opposing Russian aggression and are taking actions to limit Russian involvement in their commerce, contests, and events, can face an elevated risk of retaliation in the future.

It may be improbable that Russian vendors will give up their market edge to support a conflict. But, No one knows what the future holds. The Russian-Ukrainian conflict will likely pour over from the European borders to Asian and Middle Eastern countries. Cyber Vigilance has become a necessity, and if organizations believe that they will not become a target, then they have already lost.

```
Note:
```

```
Second-order or third-order impacts are already seen in our cybersecurity environments as Chinese ad
```

Cyber Defense Assessment Recommended

While the Russian-Ukrainian cyber warfare creates an atmosphere of uncertainty in Europe and globally, a need for improved cybersecurity has arised. Some of the main cyberthreats that we believe will increase are DDoS attacks, APT attacks, Ransomware attacks, Phishing and Malware attacks, Zero-Day Vulnerabilities, Financial Frauds, and other emerging threats.

Rewterz has been actively monitoring the Russian-Ukrainian conflict and providing our customers with enriched information that will help improve your organization's cyber posture. Given the rapid pace of events surrounding the conflict, here is the chronological timeline of developments related to the ongoing cyberwar:

Attack Timeline

13th – 14th January, 2022

- In mid-January 2022, More than 70 websites of the Ukrainian Ministry of Foreign Affairs and a number of other government agencies were down temporarily and provocative messages were left on the websites.
- Microsoft also found a new and unique malware that was infecting the systems of Ukrainian politicians and government affiliates. Dubbed as "WhisperGate," this new malware was designed to render targeted devices inoperable and intended to be destructive.

4th February, 2022

- Fake social media accounts of Russian IOs were also dismantled by Ukrainian Security Services.

15th February, 2022

- On February 15th, 2022, Distributed Denial-of-Service (DDoS) targeted Ukraine's defense agencies and banks. Several Ukrainian websites were impacted by this attack, including the Ministry of Foreign Affairs,

bank, government, and Defense Council. The attacks were of a moderate magnitude. The main objective of this attack was to instill fear.

23rd February, 2022

- The 2nd wave of DDoS attacks hit Ukraine. Ukraine Ministry Of Foreign Affairs, Security service of Ukraine, Ministry of Defense, Ministry of Internal Affairs, and other Government institution websites were inaccessible for two hours.

25th February, 2022

- SALTY SPIDER, a russian-based threat group, made use of its Sality botnet to launch DDoS attacks on Ukrainian Web Forums. This HTTP request overflow attack was performed to get information from one of the forums that discusses real-time events taking place in the city of Kharkiv. The main motive was also to shut down any information sharing against the Russian militia.

27th February, 2022

- The Conti group opted to side with Russia, threatening to strike its rival's key infrastructure. They later clarified that they condemn the war and deny being the allies of any government. Shortly after, a security researcher released 13 months of sensitive data against the Russian nation-state actor. The data includes chat logs between the members of Conti and their victims with a bitcoin address, and it also contains manuals on the deployment of the Cobalt Strike.

28th February, 2022

- Ukraine called upon cyber security experts and specialists to launch attacks against Russia. Amid the Russian-Ukrainian cyber warfare, both entities have been on the offensive; Russia invasion on Ukraine is not only on the ground. As a response, Ukraine is recruiting white hat hacktivists to create an "IT Army" as said by Ukraine's Minister for Digital Transformation Mykhaylo Fedorov.
- Anonymous, a hacktivist and activist collective, has declared its support for Ukraine in this ongoing cyber war. In doing so, they have disabled Russian websites such as http://kremlin.ru/ and other government portals. In addition to this, the group also took down RT News and leaked 200GB of emails between Belarusian weapons maker Tetraedr and Russia. The collective also hacked Russian TV channels, played the Ukrainian national anthem on them, and also showed uncensored news of what was happening in Ukraine.

1st March, 2022

- Trojan.Killdisk – a new disk-wiping malware was discovered by security researchers. HermeticWiper (Trojan.Killdisk) is interestingly digitally signed by a certificate issued to Hermetica Digital Ltd (the origin of the name). The wiper attacks were targeted towards Ukraine in support of the Russian invasion, and these signatures can also be seen in attacks in Lithuania. Targeted sectors are aviation, defense, IT services, and the financial sector.

- UNC1151 – a Minsk-based threat group – has been targeting the Ukrainian government officials and military personnel with mass phishing emails. After the account is compromised, the attackers, by the IMAP protocol, get access to all the messages. Later, the attackers use contact details from the victim's address book to send the phishing emails.

2nd March, 2022

- Anonymous Collective performed DDoS attacks on many Russian websites, government entities, and television networks. The latest attack by the Anonymous-linked group Network Battalion 65 was on the Russian Nuclear Institute. The group released 40,000 files from the institute online.
- After HermeticWiper, another data-wiper to hit Ukraine was the IsaacWiper which is less sophisticated than HermeticWiper but may be related to it. The wiper enumerates the physical and logical drives and then recursively wipes the files off of each disk. This new version of the data-wiper also contains debug logs.

9th March, 2022

- APT28 – aka FancyBear, a Russian-linked threat actor, has carried out massive credential phishing attempts targeting ukr.net users. UkrNet is a Ukrainian media organization. The phishing emails were sent from a significant number of hacked accounts (other than Google/Gmail) and include links to attacker-controlled domains.
- UNC1151 – a Minsk-based threat group – targeted the Ukrainian government officials and military organizations with mass phishing emails. The attackers use contact details from the victim's address book to send phishing emails.
- Mustang Panda, a Chinese threat actor group, has taken advantage of the Russian-Ukrainian cyberwarfare by deploying the virus Ukraine.exe.

15th March, 2022

- CaddyWiper is another destructive data wiper suspected to be targeting Ukraine.

16th March, 2022

- Russian Nation-State threat actors have started exploiting default MFA protocols and PrintNightmare (CVE-2021-34527) vulnerability to run arbitrary codes with elevated privileges.

17th March, 2022

- Sidewinder Group has been actively targeting the Government of Pakistan via phishing emails, dropping malicious Word documents which enable macro when downloaded and executed. The malicious file suspected of being used as an attachment has the name "FOCUSED TALK ON RUSSIAN UKRAINE CONFLICT.docx".

How Can We Help?

- Rewterz is offering contextualized Threat Intelligence with Indicators, remediations, and recommendations, that will lead to a stronger security posture in this present cyberwar.
- Rewterz also provides customers with unparalleled insight to accelerate incident detection and response with our expert intelligence.
- Rewterz's Threat Intelligence Analysts deliver sector and region-specific reports, threat alerts, insights that will help shape your cybersecurity infrastructure.
- Rewterz also offers rapid threat analysis, triage, contextualization, and correlation for insight into your specific risk profile.

We are reaching out to let you know our entire organization is on high alert and that we are assisting our customers and the community in any way possible.

Therefore, through our Threat Intelligence, Threat Hunting, and SOC services, we are making numerous complementary tools accessible to aid the larger global community.

References

Gerden, E. (2022). Russian IT market growing steadily after the pandemic. Retrieved 27 October 2021, from https://www.computerweekly.com/news/252508694/Russian-IT-market-growing-steadily-after-pandemic

Gewirtz, D. (2022). How to avoid being unwillingly drafted as a cyber combatant in the Russia-Ukraine war | ZDNet. Retrieved 25 February 2022, from https://www.zdnet.com/article/how-to-avoid-being-unwillingly-drafted-as-a-cyber-combatant-in-the-russia-ukraine-war/

R. Kolbe, P., Zabierek, L., & Morrow, M. (2022). The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict. Retrieved 18 February 2022, from https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict

Rewterz Threat Alert – APT Mustang Panda – Active IOCs – Russian-Ukrainian Cyber Warfare | | Rewterz. (2022). Retrieved 1 March 2022, from https://rewterz.com/rewterz-news/rewterz-threat-alert-apt-mustang-panda-active-iocs-russian-ukrainian-cyber-warfare

SADOWSKI, J., & HALL, R. (2022). Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation | Mandiant. Retrieved 4 March 2022, from https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation

---