CYBER WORLD WAR

Alon Schwartz *reveals how the Russian invasion of Ukraine is fuelling a cyber war*

Russia's invasion of Ukraine has placed Europe in a precarious position. From a security standpoint, perhaps one of the most concerning implications of the invasion has been the aggravation of cybercriminal activity – a consequence that policymakers are already flagging with urgency.

On 20 April, 2022, the cybersecurity authorities of the United States, Australia, Canada, New Zealand and the United Kingdom released a joint Cybersecurity Advisory (CSA) warning that the invasion could expose organisations to increasingly malicious cyber activity from Russian state-sponsored cyber actors or Russian-aligned cybercriminal groups.

More specifically, the release highlights the threat posed to critical national infrastructure (CNI) in particular, stating that such groups are actively exploring options for attacks in this domain and urging critical infrastructure network defenders to prepare accordingly and bolster their defences.

The release hasn't come out of the blue. Cyberattacks played a prominent role in Russia's initial offensive in Ukraine, with a press release from the UK government published in May 2022 indicating that Russia was behind a cyberattack on commercial communications company Viasat in Ukraine that affected vast swathes of Europe just one hour prior to the 24 February invasion.

During the attack, threat actors gained access to the network of KA-SAT, a satellite owned by Viasat, by exploiting a misconfigured VPN appliance, then going on to damage tens of thousands of terminals in order to plunge many personal and commercial internet users into an internet blackout.

Albeit the first major cyber incident of the conflict, this is just one of many examples of the use of cyberware against CNI since Russia's invasion of Ukraine began. In a detailed report, Microsoft highlights 37 destructive Russian cyberattacks that were carried out within Ukraine between 23 February and 8 April.

"Starting just before the invasion, we have seen at least six separate Russia-aligned nation-state actors launch more than 237 operations against Ukraine – including destructive attacks that are ongoing and threaten civilian welfare," states Tom Burt, Corporate Vice President of Customer Security & Trust at Microsoft in a blog accompanying the report.

"The attacks have not only degraded the systems of institutions in Ukraine, but have also sought to disrupt people's access to reliable information and critical life services on which civilians depend and have attempted to shake confidence in the country's leadership."

While almost one third (32 percent) of these destructive attacks are said to have directly targeted Ukrainian governmental organisations, the largest proportion (40 percent) were aimed at organisations in critical infrastructure sectors, and in many instances were coordinated in tandem with ground offensives.

On 1 March, for example, Russian affiliated threat actors launched a cyberattack against one of Ukraine's major broadcasting companies – the same day that the Russian military expressed its intention to stem what is described as Ukrainian "disinformation" and launched a missile strike on a television tower in Kyiv. Equally, 13 March saw a Russian actor steal data from a nuclear safety organisation, just as the Russian military began to obtain control of a nuclear power plant, the Zaporizhzhia facility.

These efforts have extended beyond hacking efforts, however. In its report, Microsoft also details how Ukrainians began to receive fake emails from a Russian actor pretending to be a Mariupol resident, proclaiming that the Ukrainian government had abandoned its citizens as Russia proceeded to besiege the city.

In terms of CNI, there is evidence to suggest that second and third tier suppliers to such organisations may soon become the targets of Russia's threat actors. Indeed, a report from the US Cybersecurity & Infrastructure Security Agency (CISA) revised in March 2022 makes the point that Russian state-sponsored APT actors previously targeted third-party infrastructure and compromised third-party software, specifically targeting operational technology and industrial control systems with destructive malware.

The M.E.Doc accounting software attack involving Ukrainian firm Intellect Service and the infamous SolarWinds Orion attack stand as prime examples. They attest to how Russian state-sponsored attackers have been able to compromise trusted third-party software to spread malware to a range of victims.

Should second and third tier suppliers become key targets, it is likely that there will be dramatic international cyber spill over from the war in Ukraine as key software and solutions providers are affected globally, heightening potential that a cyber world war may develop.

Many cyberattack groups have already established specific target regions geographically. Looking at MITRE ATT&CK, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations, we can see that while several leading threat groups are either Russian state backed or aligned, Russia itself equally faces its own cyber threats.

RTM, for example, is described as a cybercriminal group that has been active since at least 2015 and is primarily interested in users of remote banking systems in Russia and neighbouring countries. Meanwhile, another threat group named Strider is said to have been active since at least 2011, targeting victims in Russia, China, Sweden, Belgium, Iran and Rwanda, while Anonymous has actively aligned itself against Russia.

Such a dynamic is concerning. For years experts have expected that the next war would be a cyber war, and with so many parties holding unique and varying interests – and with many often directly aligned with nation-states – there is a risk that the burgeoning cyber war over Ukraine might extend into new territories.

Russia's digital isolation may play into this. Facebook has been blocked entirely by Russian authorities who declared Meta (the firm's parent company) to be an "extremist organisation". Further, many other western firms including Apple, Microsoft, TikTok and Netflix have voluntarily withdrawn from the Russian market, while Twitter has been almost completely cut off.

Apple, Microsoft, TikTok and Netflix have withdrawn from the Russian market, while Twitter has been almost completely cut off

CYBERATTACKS PLAYED A PROMINENT ROLE IN RUSSIA'S INITIAL OFFENSIVE IN UKRAINE

Such moves have raised concerns over the possibility of a 'splinternet' – where the single global internet that we know today could be replaced by several national or regional networks. Should this happen, digital polarisation will only be exacerbated, paving the way for the further politicisation of cyber groups.

Within this context, it is highly likely that the cyber threat landscape is only set to continue to worsen moving forward. Between the pandemic creating new opportunities for attackers and the current geopolitical situation leading many threat actors to attack organisations and CNI in advanced ways, both the volume and sophistication of threats is expected to expand in the future.

At present, cybercriminals are using a variety of weapons in their endeavours. This has included traditional methods as well as adaptive techniques such as exploiting unpatched vulnerabilities and using modified malware to evade traditional detection-based defences.

Four of the core attack methods used in the Russia-Ukraine war include: phishing, wiper malware, DDoS and website defacement. Perhaps unsurprisingly, phishing campaigns remain one of the most popular attack methods. Indeed, according to the Verizon 2021 Data Breach Investigations Report, phishing attacks were connected to 36 percent of breaches in 2021. Russian-associated incidents include Minsk-based group UNC1151 (GhostWriter) deploying phishing attacks against Ukrainian soldiers on 25 February, as reported by CERT-UA. UNC1151's previous activities include promoting misinformation, website hijacking, spoofing and targeting media outlets in Belarus ahead of the country's 2020 election.

Wiper malware, intended to erase (wipe) the hard drive of endpoints that it infects, has also been used extensively against Ukraine. On 24 February, for example, a new data wiper named HermeticWiper was unleashed against several Ukrainian entities including a financial institution and two contractors in Latvia and Lithuania that provide services to the Ukrainian

Picture credit: Expect Best

Government. This wiper has proven to be particularly problematic owing to its ability to bypass Windows security features.

Distributed denial of service (DDoS) attacks have become common between Ukraine and Russia, the latter having launched several attacks earlier in February 2022, focusing on Ukrainian banking and defence websites. Equally, early March saw Russian groups using DanaBot, a malware-as-a-service platform, to again launch DDoS attacks against Ukrainian defence ministry websites.

RUSSIA WAS BEHIND A CYBERATTACK ON UKRAINE JUST AN HOUR BEFORE THE 24 FEBRUARY INVASION

Website defacements have also been used to spread misinformation and propaganda. The NCSC's assessment that Russian Military Intelligence was involved in the 13 January defacements of Ukrainian government websites is one such example. However, interestingly, since the infamous hacktivist group, Anonymous, declared Russia as its target, Russian military sites have also become targets of defacement.

Be it these four attack methods or others, the Ukraine-Russia invasion is adding complexity to the threat landscape. Given the heightened threats facing CNI, those organisations responsible for defending them must be prepared. Indeed, failing to do so can lead to catastrophic affects.

Such preparedness begins with monitoring for malicious activities and investigating post-compromise activity where attacks have taken place. To spot any accounts that have been compromised, organisations should be monitoring for password changes, unusual logins, emails, requests from any users and more.

Organisations should equally look out for suspicious files that have been downloaded using PowerShell, commands that have used generic evasion techniques like base64 encoding and unusual traffic that can be found between domains.

Known vulnerabilities, such as CVE-2021-1636, are often at the top of attacker agendas, so these too need to be monitored. Further, other possible red flags include suspicious parent processes, credential dumping attempts, the disabling of important features, logs being cleared, scheduled tasks being created, unusual remote access tools (RATs) making connections or security settings being changed unexpectedly. Unfortunately, monitoring for all these activities won't completely mitigate the risk of being compromised. That is why incident response is just as important.

With time being of the essence in the face of attacks, it is vital that operational procedures for planning and conducting cybersecurity incident and vulnerability response activities are detailed and easy to follow, with step-by-step instructions. Plenty of resources are available offering guidance on frameworks, the CISA, FBI and NIST standing as just a few examples of reputable bodies providing genuine advice.

Common best practices include using endpoint detection and response (EDR) tools with proper restrictive policies to avoid leakage of data and zero-trust protocols for confirming the authenticity of activities. It is also advisable that firms leverage tools such as security information and event management (SIEM) and security orchestration, automation and response (SOAR) to create active monitoring and incident response plans.

Firms should always aim to enable multifactor authentication (MFA) to mitigate potentially compromised credentials, ideally including the use of passwordless authenticator tools for an extra level of security. Further, ensuring that all systems are actively patched – and signatures are up to date for all endpoints, security and software products – is critical in avoiding exploitation.

Given the threat facing CNI as well as their secondary and tertiary suppliers, organisations of all shapes and sizes are at risk of becoming implicated. Therefore, security best practices have never been more imperative ●

Alon Schwartz is a Cyber Security Researcher at Logpoint in charge SOAR services and threat intel. His previous roles include SOC team leader, analyst and consultant and he holds qualifications in incident response and digital forensics.

Cybersecurity authorities are exploring options for attacks on CNI like banking and urging network defenders to bolster their defences