In January, the Cybersecurity and Infrastructure Security Agency (CISA) released an Alert (AA22-011A) outlining the risk of Russian state-sponsored threats on the US. What's playing out now is a culmination of tested Russian cyber tactics developed through state-sponsored and cybercriminal organizations which operated within friendly territories for years with impunity.

Although the global community began to condemn the invasion, countering with sanctions and financial expulsion, it has only emboldened cybercriminals that pledge loyalty to Putin's actions to target these nations with cyberattacks. Their pedigree includes the ability to maintain an undetected persistent and long-term access to compromised environments across networks, devices, and cloud services.

The primary objective of these cyberattacks is to disrupt critical business operations by compromising third-party and supply chain infrastructure, deploying custom malware (including ransomware) and leveraging Distributed Denial of Service (DDoS) attacks.

These tactics and capabilities were leveraged against Ukrainian banks, government services and media outlets.

Based on an updated list of known vulnerabilities linked to Russian cybercriminal syndicates and lessons learned during counter offenses against Russian threat actors, eSentire's Threat Response Unit (TRU) and 24/7 Security Operations team have conducted over 67,000 threat hunts across 2,000 clients, discovered a handful of active malware attacks, and added over 2,000 indicators of compromise (IoCs).

In an ironic turn of events, one of the most prolific ransomware gangs, Conti, appears to be in a civil war of its own. Having initially pledged allegiance to Putin's invasion of Ukraine, 13 months of chat logs between affiliates of Conti were leaked and published with the message "Glory to Ukraine". The shared conversations expose the ransomware gang's operations and tactics used to develop defense-evading malware, including using fake companies to arrange meetings with prominent cybersecurity firms.

## Know thy enemy

When it comes to preparing for the potential aftershocks of geopolitical events and economic sanctions, the first step is to understand your adversary and their tactics. Russian-aligned cybercrime groups employ clever phishing campaigns and poisoned search results to harvest credentials and gain initial access to targeted organizations.

In fact, eSentire TRU discovered a prominent ransomware gang using SEO poisoning to spread the GootLoader malware through third-party websites that hosted infected downloadable resources like templates and contracts designed to attract executives from various business services.

These cybercriminal groups establish persistent access through remote access tools and leverage vulnerabilities in unpatched FortiGate, Cisco, Oracle, Pulse, Citrix, and Microsoft Exchange services to move in and out of the environment undetected.

Their ultimate goals vary. Once they have established persistent access to your environment, they can disable back-up systems and deploy ransomware to disrupt operations, use wipers to permanently destroy data as a scorched earth tactic, or use DDoS attacks to bombard websites with erroneous requests to overload servers and shut down public facing services.

## What you can do right now to enhance your cybersecurity posture

Long-term persistence gives your organization time to detect and stop unauthorized access before it becomes terminal. So, the reality is that many of the cyberattacks attributed to Russian agents could have been stopped before they crippled business operations. Here are a few recommendations:

- Familiarize yourself with the threats: Read the CISA advisory on Russian tactics, and eSentire's security advisories on Russian cyber threats and website poisoning campaigns. Your goal is to stay up to date with the latest security advisories, threat alerts, and news and, more importantly, encourage your employees to do the same. If you're not staying on top of the latest tactics, techniques, and procedures (TTPs), you can't strategize your cybersecurity program to defend your organization against the most impactful threats.
- Train your employees to identify cyber threats: Threat actors are increasingly taking advantage of fallible human nature and using phishing attacks to gain initial access into their targets' environment. Most recently, this was seen in the HeaderTip malware campaign launched by Russian-allied threat actors. Conduct ongoing phishing and security awareness training so your employees learn to identify phishing and other social engineering lures, help strengthen your cyber resilience, mitigate cyber risk, and develop practices and policies for employees to report suspicious activity.
- Patch systems and services: Threat actors commonly use unpatched vulnerabilities to access your IT assets and deploy malware or steal data. Ensure your critical systems and services (remote access, third-party software, email systems, etc.) are patched and up to date to reduce the risk of cybercriminals hijacking these systems to steal data, deploy malware or disrupt operations. Better yet, leverage a comprehensive vulnerability management program to help you identify vulnerabilities across your expanding IT assets, prioritize remediation against biggest vulnerabilities and minimize your vulnerability discovery to remediation timeframe.

- Be prepared for the worst case scenario: Review your business continuity and disaster recovery plans, ensure your back-up systems are properly segmented and working, and review your incident response (IR) plan and cyber insurance coverage. Most importantly, consider engaging an Incident Response partner for an IR retainer to ensure immediate support in the event of a cyberattack.

Even after weeks of the ongoing conflict between Russia and Ukraine, there is no sign of resolution. Ultimately, your goal is to put your business ahead of disruption. Increase your organization's vigilance to strengthen your cyber resilience.

To learn how eSentire's Managed Detection and Response (MDR) can help your team detect and respond to an attack before it disrupts your business, book a meeting with a cybersecurity specialist today.