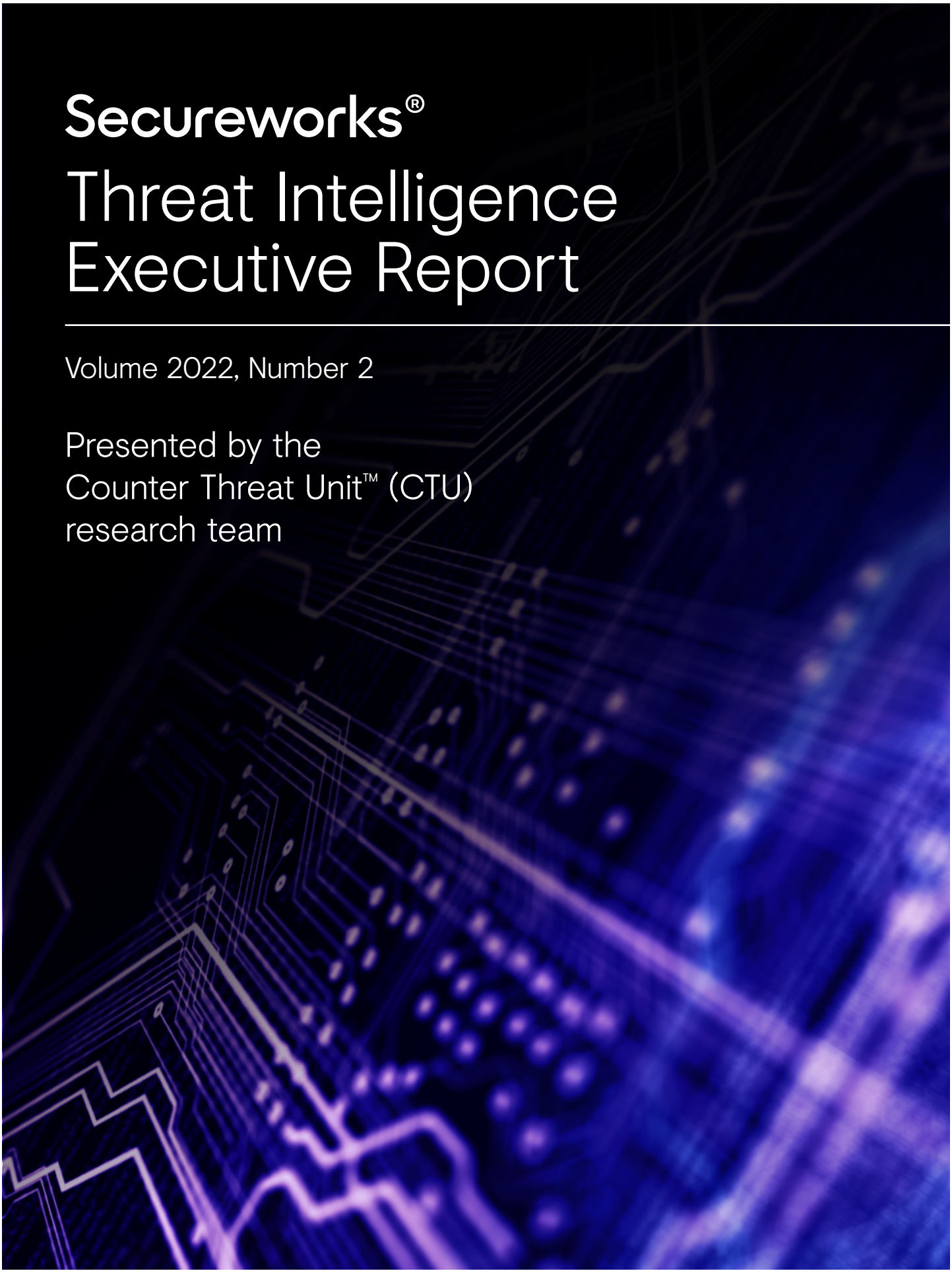
Secureworks®

Threat Intelligence Executive Report

Volume 2022, Number 2

Presented by the Counter Threat Unit™ (CTU) research team



Executive Summary

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats and helps organizations protect their systems. During January and February 2022, CTU™ researchers observed notable developments in threat behaviors, the global threat landscape, and security trends, and identified lessons to consider.

- Russian cyberattacks were highly focused in the first week of the Ukraine invasion
- GOLD ULRICK and Conti details leaked
- Downloaded legal documents concealed malware loader

Russian cyberattacks were highly focused in the first week of the Ukraine invasion

Russia's use of cyber capabilities prior to and into the first week of its invasion of Ukraine focused solely on Ukrainian targets. Most organizations outside Ukraine experienced little threat from Russian government-sponsored activities, as ransomware remained the primary threat. Security controls that mitigate ransomware-style attacks are the best preparation for any escalation of Russian cyber activity.

Since the January build-up to Russia's invasion of Ukraine, there has been concern that Russia would unleash wiper malware that could spread autonomously, as NotPetya did with significant damaging effect in 2017. In the initial phases of the invasion, those concerns have not materialized. The cyberattacks appear to specifically target Ukrainian organizations. Threat actors launched distributed denial of service (DDoS) and wiper attacks against Ukrainian government entities and financial institutions on February 23 and 24, immediately prior to the Russian military invasion of Ukraine. Wiper malware was deployed after prolonged access to the target networks rather than the rapid deployment of NotPetya. The attacks followed similar DDoS and defacement attacks against Ukraine in mid-January and early February. Financially motivated ransomware remains the greater threat to organizations outside Ukraine.

Russia has a history of using its cyber capability as an additional dimension to physical attacks, punishing countries it considers hostile. Russia used DDoS attacks, website defacements, and massive spam campaigns against the country of Georgia in 2008, immediately prior to the Russian invasion of the Georgian province of South Ossetia. Russian threat groups also launched DDoS attacks against Estonia in 2007

and Kyrgyzstan in 2009. These attacks aspire to create panic, undermine trust in the government, disrupt the operation of critical infrastructure, and weaken the resolve of the civilian population. Russia has also previously targeted Ukraine, notably with the December 2015 and December 2016 destructive attacks conducted by the IRON VIKING threat group against the Ukrainian power grid.

The potential for Russia to indiscriminately use its cyber capabilities may increase as the country becomes more isolated due to Western sanctions. The possibility of additional reprisal attacks by Russian criminal or activist threat actors in response to disruptive attacks against Russian critical infrastructure by pro-Ukraine threat actors is also a cause for concern. Focusing on security controls that mitigate ransomware and DDoS attacks is the best form of defense against whatever may come next from the evolving Ukrainian crisis. These controls include patching, multi-factor authentication, network segmentation, engaging DDoS mitigation services, and monitoring endpoint detection and response solutions.

If you do just one thing after reading this:
Bookmark the Secureworks microsite on the Russia-Ukraine crisis to stay current on rapidly evolving developments.

GOLD ULRICK and Conti details leaked

The February Conti ransomware leaks provide insight into the inner workings of the GOLD ULRICK cybercriminal group that operates it. However, the leaked data is unlikely to reduce the overall threat posed by ransomware. Organizations should not let their guard slip.

On February 25, the GOLD ULRICK cybercriminal group that operates the Conti ransomware-as-a-service (RaaS) offering publicly sided with Russia and claimed it would retaliate in response to cyberattacks targeting Russia. On February 26, the group modified its statement to support the Russian people rather than the government. That moderated statement did not appease everyone.

Starting February 27, a newly created Twitter @ContiLeaks persona dumped information about the threat group. The data included internal chat logs, organizational hierarchy, ransomware source code, details of ransomware attacks, and victim negotiations. CTU analysis suggests that the individual responsible for leaking the data is a Ukrainian security researcher rather than a GOLD ULRICK member or affiliate unhappy with the threat group's stance on the war. The information was likely leaked to fuel paranoia and conflicts within the group, and some affiliates may switch to other RaaS schemes as a result.

Conti first emerged in November 2019 and is one of the most prolific ransomware families. Its leak site lists 729 victims as of late February, and there may be many more unlisted victims who paid the ransom. The average Conti ransom payment is reportedly over $650K USD. Since late 2021, GOLD ULRICK has changed some of its tactics, techniques, and procedures (TTPs). The group discontinued using the currently dormant TrickBot malware as an initial access vector (IAV), favoring the Emotet malware to deliver malicious payloads. GOLD ULRICK is also reportedly responsible for persuading GOLD CRESTWOOD to resurrect Emotet. The leaks show how closely enmeshed GOLD ULRICK is with other cybercriminal groups. They reveal a sizeable and organized criminal group with recruitment, staff performance issues, and salary considerations familiar to legitimate businesses.

GOLD ULRICK has survived previous leaks. The group's playbook leaked in August 2021 listed numerous tools used in Conti attacks. It also survived a September 2021 takedown operation carried out by the Irish national police force, Europol, and Interpol that was in response to the May 2021 GOLD ULRICK attack on the Irish Health Service.

GOLD ULRICK is not the only Russian-aligned ransomware group declaring support for Russia. But other groups like LockBit operator GOLD MYSTIC proclaimed themselves apolitical, noting that they run a multinational operation composed of individuals with diverse political views. While it is generally true that many cybercriminal groups have a Russian nexus, many are motivated by money first and politics second.

It's too early to judge how the leaks will impact Conti's operations specifically. The group is still adding new victims to its public leak site as of early March. It is unlikely that the overall threat posed by ransomware will decline. When this is added to the uncertainty created by Russia's attack on Ukraine, it is clear that organizations cannot afford to let their security guard down.

If you do just one thing after reading this:
Organizations should review their business continuity plans and restoration processes to address ransomware-style or wiper malware attacks.

Downloaded legal documents concealed malware loader

Not all websites are what they seem to be. In addition to being wary of unsolicited emails with attachments or links, users should also exercise caution regarding what they download from websites, even if it appears to be legitimate business content.

In February, CTU researchers analyzed the GOLD ZODIAC cybercriminal group's attempts to deploy malware via legitimate-looking websites that delivered legal and financial documents. The group crafted blog articles and built a complex network of compromised WordPress sites to deliver the Gootloader JavaScript-based loader. Gootloader infections have led to the deployment of multiple malware families, including the LockBit ransomware.

The threat actors leveraged search engine optimization (SEO) poisoning to increase the ranking of the compromised sites in search results. They posted content seeded with highly ranked legal and financial search terms onto these compromised sites to convince site visitors to download Gootloader disguised as legal or financial documents.

This is an ingenious technique, as victims feel like they found the download through a legitimate internet search rather than being directed to it by an unsolicited phishing email. As such, the technique bypasses much of the traditional training on how to detect social engineering. Organizations should educate employees that phishing and malware distribution attacks don't always start with emails. Downloading files from marginal or non-authoritative websites can be just as dangerous. Organizations can mitigate this threat by controlling access to websites based on how new the website is, or by using third-party threat intelligence feeds. However, none of these approaches provide comprehensive protection.

Organizations using content management systems (CMS) such as WordPress must patch the CMS software in a timely fashion. They should also patch third-party plugins, as threat actors can exploit vulnerabilities in them as well.

If you do just one thing after reading this:
Ensure your user awareness training is comprehensive and addresses emerging threats.

Conclusion

As of this publication, cyber activity related to the Russia-Ukraine crisis has been highly targeted. That may change as the conflict progresses. Ransomware and other cybercriminal activity are a greater threat to organizations outside Ukraine. Staying up to date with developments in the threat landscape remains essential.

A glance at the CTU research team

CTU researchers frequently serve as expert resources for the media, publish technical analyses for the security community, and speak about emerging threats at security conferences. Leveraging Secureworks' advanced security technologies and a network of industry contacts, the CTU research team tracks threat actors and analyzes anomalous activity, uncovering new attack techniques and threats. This process enables CTU researchers to identify threats as they emerge and develop countermeasures that protect customers before damage can occur.

Research

Understanding the nature of threats customers face, and creating countermeasures to address and protect.

Intelligence

Providing information that extends the visibility of threats beyond the edges of a network.

Integration

Infusing CTU research and intelligence into Secureworks managed security services and security consulting practices.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086

Japan
Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

If you need immediate assistance, call our 24x7 **Global Incident Response Hotline:**

+1-770-870-6343

