Secureworks®

Threat Intelligence Executive Report

Volume 2022, Number 3

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 March and April 2022, CTU™ researchers observed notable developments in threat behaviors, the global threat landscape, and security trends, and identified lessons to consider.

- Ransomware and hack-and-leak attacks continue
- Russia and Ukraine: a focused threat
- Spring4Shell was less impactful than feared

Ransomware and hack-and-leak attacks continue

Despite leaks, law enforcement action, and occasional poor tradecraft, cybercriminals persevere and thrive. Organizations must remain vigilant.

The Conti leaks continued through March and provided revelations about the professionalism of the GOLD ULRICK threat group and how it operates the Conti ransomware. There was speculation that the negative impact from the disclosures could cause the group to cease operations, but that had not happened by the end of April. CTU analysis indicates that Conti activity as of April 30 matched peak-2021 levels.

Overall, ransomware activity continued to flourish. After a lull in January around the Russian Orthodox Christmas, activity across many of the ransomware leak sites tracked by CTU researchers steadily increased. Additionally, the GOLD SOUTHFIELD threat group resumed REvil ransomware operations in April following October 2021 U.S. law enforcement takedown activity and January 2022 arrests in Russia.

Even less accomplished groups such as Lapsus$, which conducts extortion-only attacks (also known as hack-and-leak attacks), have been successful. Seemingly comprised of relatively unsophisticated teenage operatives, Lapsus$ compromised global corporations such as Microsoft using social engineering.

Despite law enforcement action against individuals, threat groups, money laundering services, and underground forums, the risk from ransomware attacks remains high. Regardless of whether an attack is technically complex or not, organizations are at risk if they have unpatched systems and if they lack identity controls like multi-factor authentication, security oversight in their supply chain, and layered security controls. To protect against ransomware or hack-and-leak attacks, organizations must meticulously implement basic security practices.

If you do just one thing after reading this:
When assessing risk, prioritize ransomware as the most significant threat.

Russia and Ukraine: a focused threat

Network defenders protecting organizations without Ukrainian ties must not allow fears about the conflict to distract from longer-term security priorities. Ransomware remains a far greater concern for most organizations than attacks related to the war in Ukraine.

Russian government-sponsored threat activity connected to Russia's invasion of Ukraine remained focused on Ukrainian targets during March and April. An unsuccessful April 8 attack on a Ukrainian energy provider used industrial control system malware that had code similarities to malware implicated in a December 2016 Ukrainian power grid outage. The U.S. government attributed the December attack to Unit 74455 of Russia's military intelligence directorate (GRU). A February attack on Viasat civilian satellite equipment was attributed to Russian threat actors. It was intended to disrupt Ukrainian communications during the invasion but caused wider collateral damage. The impact included a partial service interruption for tens of thousands of residential broadband customers across Europe and the loss of remote access and monitoring capabilities for electricity-generating wind turbines in Germany. As of this publication, this is the only publicly disclosed conflict-related attack by Russian government-sponsored threat actors that impacted systems outside Ukraine.

In addition to collateral damage, risks to non-Ukrainian organizations could originate from pro-Ukraine threat actors targeting organizations linked to Russia, or pro-Russia hacktivists targeting organizations that have connections to Ukraine. A significant increase in distributed denial of service (DDoS) attacks, which are often used by hacktivists, has been attributed to this conflict. Organizations that consider themselves at risk should implement DDoS protection services.

While talented hacktivists can cause limited chaos, analysis of the threat landscape confirms that cybercrime poses a far greater threat to organizations than hacktivism. Ransomware attacks are increasing globally, and organizations outside Ukraine should prioritize defenses against those attacks.

If you do just one thing after reading this:
Simulate a ransomware attack in a tabletop exercise scenario. Ransomware groups use many of the same techniques as government-sponsored threat groups and hacktivists, so this exercise is excellent preparation for a broad range of attacks.

Spring4Shell exploit was less impactful than feared

Not all high-profile vulnerabilities are as damaging as first thought. Staying current with threat intelligence and maintaining good asset management help organizations determine whether a vulnerability is being actively exploited or only poses a theoretical risk.

On March 29, rumors began circulating about a zero-day remote code execution (RCE) vulnerability in the Spring Framework Core component. Spring is a popular Java application framework that has a global userbase. Early on March 30, a Twitter persona shared a link to a proof-of-concept exploit but quickly deleted their account. The vulnerability (CVE-2022-22965) received a CVSSv3 severity rating of 9.8 out of 10 and was dubbed Spring4Shell as a nod to the widely exploited Log4Shell vulnerability (CVE-2021-44228) that impacted the Log4j Java logging library.

Like Log4Shell, Spring4Shell had the potential to affect a large number of organizations. However, the impact appears to have been much less widespread than anticipated. Just as Log4Shell was more difficult to exploit than originally thought, successful exploitation of Spring4Shell requires specific conditions and default implementations are not vulnerable. CTU researchers and Secureworks incident responders encountered only a few examples of successful Spring4Shell exploitation.

These vulnerabilities highlight how important it is to pay attention to the details. Network defenders must continually evaluate how a vulnerability can be exploited and specifically how it impacts their environment. Secureworks incident responders consistently advise organizations to patch high-profile vulnerabilities because it is one of the most important ways to ward off ransomware and other cyberattacks. Combining up-to-date threat intelligence with good asset management helps organizations prioritize and apply recommendations as appropriate in their environment.

If you do just one thing after reading this:
Check that your resources are current, reliable, relevant, and comprehensive, as threat intelligence continually evolves.

Conclusion

Risks from high-profile vulnerabilities or hostile governments may not be as critical as they first appear. Threats like ransomware are serious, remarkably resilient, and enduring. Making decisions based on up-to-date threat intelligence rather than panicking in response to published speculation enables you to successfully and appropriately defend your organization.

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

