Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2024, Number 2

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

EXECUTIVE SUMMARY

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats to help organizations protect their systems. Based on observations in January and February, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Ransomware threat survives individual takedowns
- Guide advises how to detect and defend against living off the land
- Ivanti vulnerabilities illustrate perimeter device risks

RANSOMWARE THREAT SURVIVES INDIVIDUAL TAKEDOWNS

The complex and multi-faceted takedown operation against LockBit attempted to sow uncertainty and distrust that could hamper the group's efforts to survive. But even if LockBit disappears, ransomware remains a major threat to organizations.

On February 19, 2024, the UK's National Crime Agency (NCA), the U.S. Federal Bureau of Investigation (FBI), and multiple international law enforcement partners conducted Operation Cronos to take down the LockBit ransomware group. The operation, which was well-organized and well-executed, involved multiple different elements, including seizure of LockBit infrastructure, arrests, indictments, sanctions, seizure of cryptocurrency and decryption keys, and staggered publication of threat intelligence about LockBit and the takedown. It also included messaging to discourage affiliates' future involvement in ransomware operations. Affiliate usernames were 'outed' on the seized leak site, and affiliates who logged in received personalized messages telling them to expect to hear from law enforcement "very soon."

There was one conspicuous similarity to the law enforcement takedown of ALPHV (also known as BlackCat) ransomware that took place in December 2023. LockBit remained active and rebuilt some of the group's infrastructure within a matter of days. At the end of February, both LockBit and ALPHV were still operational. Shortly afterwards, the ALPHV operators turned off their servers; time will tell if LockBit is able to return to its formerly high operating cadence. If it doesn't, its affiliates will likely pivot to other operational ransomware schemes.

In recent years, the U.S. Biden-Harris administration has placed significant emphasis on taking action against ransomware groups. Disruption to threat actors and the dismantlement of their operations formed the second pillar of the National Cybersecurity Strategy published by the White House in March 2023. However, multi-agency law enforcement operations of this nature are resource-intensive and expensive.

If the cybercriminals resume activity within a few days, either with the same ransomware or a different scheme, are these operations a good use of resources? Examining the output of the LockBit takedown reveals impactful results. The NCA obtained over 1,000 decryption keys for existing and previous victims, which gave victims the opportunity to recover their encrypted data. There were numerous arrests, and over 200 cryptocurrency accounts linked to threat actors were frozen.

Following the REvil ransomware takedown in 2021, threat actors' uncertainty about whether law enforcement had access to REvil servers may have helped to fatally hamper the group's attempts to return to business as usual. The NCA and other agencies likely hope that LockBit's attempts to survive will similarly fail to succeed for long. But whether they do or not, ransomware will remain the most significant cyber threat to most organizations for the foreseeable future.

What you should do next:
Implement and maintain defenses such as regular patching, a monitoring solution such as Taegis™ XDR, and multi-factor authentication to mitigate the ongoing ransomware threat.

GUIDE ADVISES HOW TO DETECT AND DEFEND AGAINST LIVING OFF THE LAND

Stealth techniques reduce opportunities for easy detection and help attacks succeed. Knowing how to identify them is essential.

In February, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and partner agencies published joint guidance entitled 'Identifying and Mitigating Living Off the Land Techniques'. It was released on the same day as a headline-grabbing advisory about how Chinese state-sponsored threat group BRONZE SILHOUETTE had compromised the IT environments of multiple U.S. critical infrastructure organizations and in some cases had remained undiscovered for five years. As a result, the guide arguably received less attention than it deserved.

Living off the land (LOTL) techniques, which involve abuse of native tools, are often associated with Chinese state-sponsored threat groups that use these techniques for stealth and speed. However, North Korean and Russian threat groups, as well as ransomware threat actors, also take advantage of these techniques, especially when trying to remain undetected on the victim's system for an extended period of time. According to the guide, CISA red team assessments revealed attackers could use these techniques to "achieve full domain compromise with little to no investment in tooling."

Not all industries are likely targets for state-sponsored attacks, but any organization can fall victim to ransomware. The average dwell time for ransomware attacks is decreasing, with many cybercriminals opting for speed rather than stealth in attacks that end in encryption. However, the slower, stealthier attacks often result in more widespread and damaging ransomware deployment. In these cases, using native or legitimate tools rather than malware reduces the chances of detection.

LOTL techniques can be used in multiple IT environments, including on-premises, cloud, hybrid, Windows, Linux, and macOS environments. Defense strategies that rely only on signature-based monitoring and detection, without the benefit of threat intelligence derived from real-world observations of threat actor behavior, can fail to identify the use of these techniques. Blanket 'allow' policies for common, legitimate IT administrative tools used in the environment expand the attack surface and make life easier for attackers. It is essential for critical infrastructure organizations to review and understand the prioritized detection best practices in the guide and is highly advisable for other organizations too.

What you should do next:
Share the guide with your network defenders to help them identify security gaps and detect LOTL activity.

IVANTI VULNERABILITIES ILLUSTRATE PERIMETER DEVICE RISKS

Threat actors are quick to exploit vulnerable devices on an organization's network perimeter. Ensuring that device procurement processes require evidence of security by design is an essential strategic measure.

Activity in January provided further evidence for the argument that the risk posed by vulnerabilities jumps as soon as they are publicly disclosed. On January 10, Ivanti and Volexity disclosed that zero-day vulnerabilities CVE-2023-46805 and CVE-2024-21887, which affected Ivanti's Connect Secure VPN and Policy Secure network access control (NAC) appliances, had been exploited in targeted attacks by Chinese state-sponsored threat actors since early December 2023. After this disclosure, the rate of exploitation by state-sponsored threat actors increased sharply until January 15.

On January 16, an exploit was included in the Metasploit Framework (a popular toolkit for penetration testers and threat actors), making it widely available. Mass exploitation by cybercriminals and other threat actors began on January 16. CTU researchers observed a surge in exploit attempts on January 23, suggesting that threat actors of all types had started scanning indiscriminately for vulnerable devices.

Ivanti appliances are examples of perimeter devices. A February 29 blog post by the UK's National Cyber Security Centre (NCSC) warned that improvements in monitoring and securing endpoints means threat actors are once again focusing on vulnerable perimeter devices in their attacks. In addition, the blog stated that many perimeter devices are not 'secure by design'. Security failings can include hard-coded credentials, inadequate logging, and a large attack surface. On February 15, Eclypsium claimed that Ivanti appliances operated on an 11-year-old version of Linux that reached end of life in 2020 and that they were built around outdated software packages.

Modern system development depends heavily on use of code libraries and packages, so vulnerabilities in one core software component often cause vulnerabilities in multiple other products. Guidance jointly published by CISA and other agencies in April 2023 encouraged developers to create a software bill of materials (SBOM) to maintain an inventory of components within a product to help develop software that is secure-by-design and secure-by-default. Without this type of inventory, it can be difficult to assess the risk associated with using a product. This point formed a core element of the National Cybersecurity Strategy published by the Biden-Harris Administration in March 2023.

The NCSC blog post advises readers to "Push vendors hard on whether their products are secure by design." Given how quickly threat actors can exploit publicly disclosed vulnerabilities in perimeter and other devices, CTU researchers urge organizations to follow this advice.

✓ **What you should do next:**
Protect and monitor your perimeter devices with as much care and focus as your endpoints.

CONCLUSION

Individual threat groups may rise and fall, but skilled threat actors are always alert to opportunities offered by insecure devices and native tools. Wide-ranging monitoring and detection solutions that can identify abnormal use of legitimate, native tools are essential to a layered defense. It is also important to choose perimeter devices containing features that allow them to be adequately and appropriately secured.

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 intelligence into the Secureworks Taegis XDR platform, managed solutions, and security consulting practices.

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of over 4,000 organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

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