Secureworks®

Threat Intelligence Executive Report

Volume 2021, Number 5

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 July and August 2021, CTU™ researchers observed notable developments in threat behaviors, the global threat landscape, and security trends, and identified lessons to consider.

- Different name, same game
- Understanding the ransomware ecosystem
- Patching is not the only remediation

Different name, same game

Ransomware groups have not gone away. The threat from ransomware remains significant to all organizations regardless of size, and the scale of the threat is unlikely to diminish.

In the previous edition of the Threat Intelligence Executive Report, CTU researchers predicted that law enforcement action against ransomware operators after the May 2021 attack on Colonial Pipeline would not prevent the ransomware ecosystem from returning to full strength. Ransomware developments in July and August confirmed that prediction and illustrated how threat groups adapt in response to operational threats.

The threat groups operating the Darkside, Avaddon, and REvil ransomware appeared at the time to shutter their operations, and underground forums banned discussions regarding ransomware. However, at least seven ostensibly new name-and-shame ransomware groups emerged, and lightly disguised ransomware posts continued to appear on underground forums.

Some of the emerging ransomware families likely are genuinely new, such as AvosLocker, Hive, Hotarus, and Vice Society, but some are rebranded versions of previously known ransomware families. Some of the rebranding could be to avoid being linked to threat groups named on the U.S. Treasury Department Office of Foreign Asset Control (OFAC) sanctions list.

- GOLD HERON, which split from the GOLD DRAKE threat group, relaunched the DoppelPaymer ransomware as Grief.

- GOLD DRAKE named its newest ransomware Payload.Bin, which is the name of the leak site established by Babuk ransomware operators. This deception was likely to evade U.S. Treasury sanctions against GOLD DRAKE (also known as Evil Corp).

- GOLD WATERFALL shuttered its Darkside operation on May 13, but CTU research indicates that BlackMatter is a rebrand of Darkside ransomware. Third-party researchers have corroborated this finding by analyzing ransomware samples and cryptocurrency wallets.

- Although the Avaddon ransomware group closed its operation and issued decryption keys for victims, Haron subsequently emerged with some notable similarities to Avaddon.

In addition, affiliates that previously partnered with shuttered groups likely switched to working with other threat actors. This shift may be one reason behind the increase in activity associated with the LockBit ransomware operated by the GOLD MYSTIC threat group. LockBit activity increased rapidly after mid-July, with the total of just nine victims listed since the launch of its leak site in September 2020 surging to 144 by August 27. As leak sites only list victims that don't pay promptly, the actual number of victims is likely to be higher.

On underground forums, advertisements for 'pentesters' and other euphemisms replaced explicit requests for new affiliates. Despite the initial prohibitions issued in May on ransomware-related postings, little appears to have changed. This is partly because most of the important discussions regarding attacks already took place on private channels such as Telegram, and partly because enforcing the prohibitions would have negative financial consequences for forum owners who take a commission on forum transactions.

Law enforcement action against cybercriminals is to be welcomed, even if threat actors protect themselves from the consequences of this action by remaining in Russia and Commonwealth of Independent States countries. However, the ever-mutating nature of ransomware means that organizations must remain vigilant about ransomware developments to maintain an effective defensive posture.

✓ **If you do just one thing after reading this:**
Partner with an organization that has visibility into the evolving threat landscape.

Understanding the ransomware ecosystem

Ransomware groups may be selective about who they choose as victims based on initial discovery, but they do not ‘target’ them. Any organization with poor basic security hygiene is in danger of having threat actors sell access to its network on underground forums to ransomware groups and their affiliates.

The roles of ransomware operators and affiliates are well known. A less-known ransomware role is the initial access broker (IAB). IABs are specialists that obtain initial access into victims’ environments. IABs offer plenty of access brokering opportunities on underground forums. Ransomware-as-a-service (RaaS) groups, their affiliates, and private ransomware groups use IABs.

IABs specialize in finding poorly protected organizations. They often use publicly available scanning tools to identify vulnerabilities and then indiscriminately exploit those flaws. After gaining access, IABs perform basic discovery of the compromised network to determine if the victim is a lucrative prospect and whether it will be possible to expand access.

When a ransomware group decides to buy access to an organization from an IAB, the buyer will likely be told the victim’s sector and country, as well as the initial access vector (e.g., RDP, VPN). They might have an idea of the victim’s revenue. They often don’t know the organization’s name until after they agree to purchase the access. Increasingly, IABs are auctioning access rather than asking a fixed price.

The ransomware group or affiliate decides whether to buy access to the organization based on the victim’s revenue and sometimes sector. They decide whether to leverage the advertised access based on additional discovery activity. This decision occurs after they have purchased access. In other words, ransomware victims are not targeted. Any organization with a poorly defended perimeter is at risk of a breach and subsequent ransomware infection.

If you do just one thing after reading this:
Verify that your externally exposed systems are fully patched.

Patching is not the only remediation

To keep patching manageable, organizations can use risk-based vulnerability prioritization. To reduce risk, they should consider reducing the size of their attack surface.

On the second Tuesday of every month, Microsoft delivers one of the largest sets of security updates in the vendor community. During July and August, two sets of Microsoft vulnerabilities were notable: PrintNightmare, which affects Windows Print Spooler, and ProxyShell, which impacts on-premises Microsoft Exchange servers. Both sets of vulnerabilities were reportedly leveraged by ransomware groups soon after they were publicized.

When vulnerabilities receive publicity and are known to be under active exploitation, conflicting news can delay decisions about prioritizing. For example, the official PrintNightmare patch reportedly did not fully address the vulnerability, adding to the confusion. Patches released before corresponding exploits become public may be overlooked, as was the case for ProxyShell.

CTU researchers always advise patching where appropriate when alerting customers to vulnerabilities under active exploitation. In an ideal world, customers would apply patches as soon as they are released. Patching is one of the most effective ways that organizations can protect themselves against attacks. Organizations that delay get breached.

In reality, the world is not ideal. For example, Microsoft Exchange patches are usually specific to the most recent releases of Exchange Server software. If the software isn't up to date, then it must be updated before the patch can be applied.

Patch management can impose a considerable burden on organizations. Every month, the National Vulnerability Database receives as many as 2,000 reports of new vulnerabilities. Even though the average organization may only be affected by a few hundred patches per month, they must prioritize. Prioritization requires a risk-based approach. For example, active exploitation increases priority, but priority is lessened if the vulnerability exists on an asset that is inaccessible or extremely deep in the network. Organizations should perform a risk assessment, evaluating the likelihood and implications of exploitation.

Patching is not the only means of remediation. Organizations could deprioritize a high-profile vulnerability if compensating controls and mitigations exist. Reducing the attack surface and conducting operating system minimization and hardening are other proactive ways of reducing the patching burden.

The foundation of patch management, risk assessment, and compensating controls consists of essential tasks organizations must complete on a regular basis:

- Inventory hardware and software assets, as it can be challenging to patch an unknown device.
- Scan for hardware and software vulnerabilities and monitor for security updates or remediations.
- Patch high-priority vulnerabilities as soon as possible.
- Monitor endpoints for unusual behaviors. If an attacker takes advantage of an unpatched vulnerability, detection early in the attack chain could prevent ransomware deployment.

✓ **If you do just one thing after reading this:**
Check when you last conducted a software and hardware inventory.

Conclusion

Threat actors are highly resilient and often adapt quickly to operational threats. Monitoring helps organizations keep up. This includes staying abreast of changes in the threat landscape and monitoring internal systems for vulnerabilities and unusual behaviors on endpoints.

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
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp