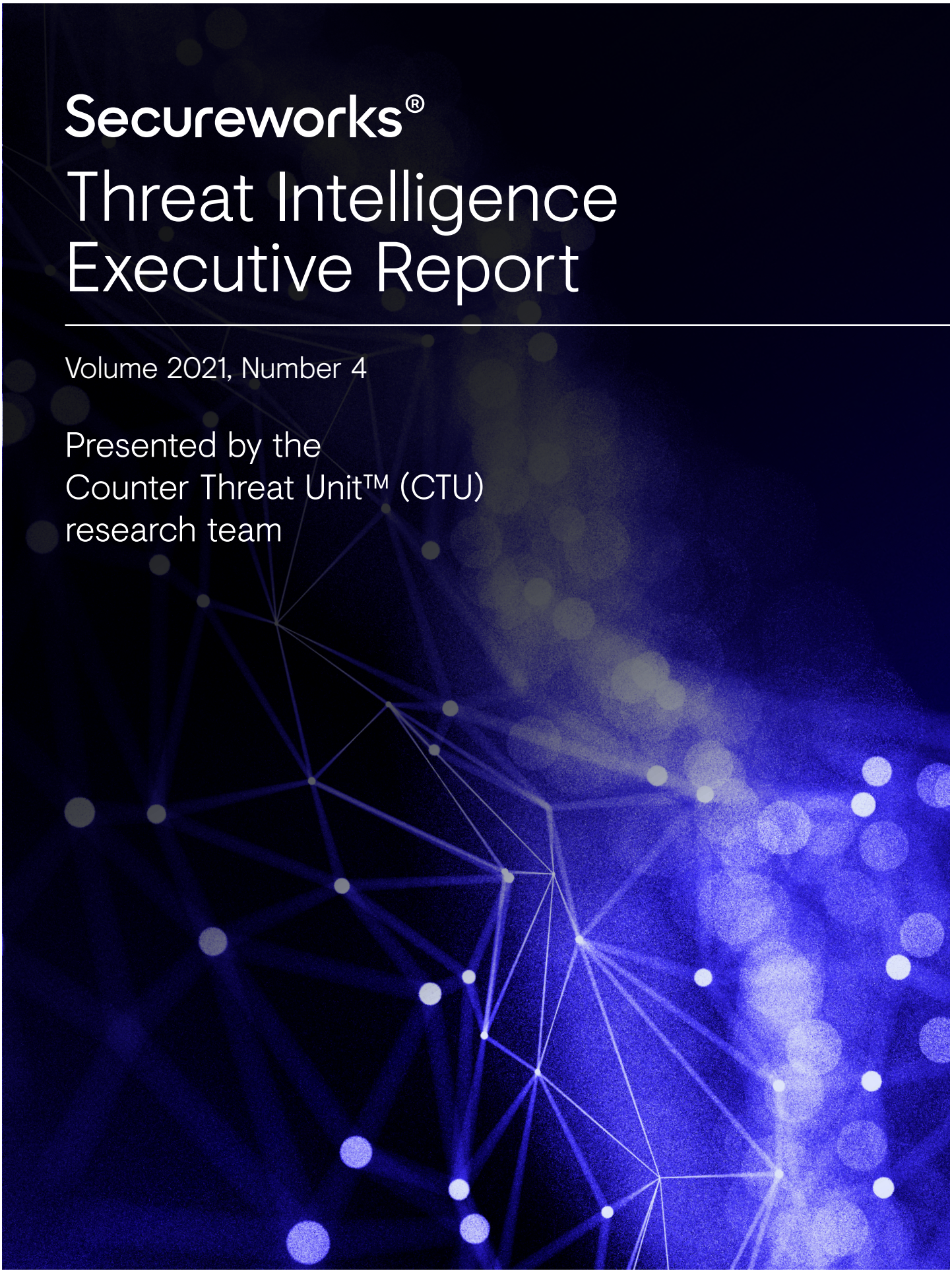
Secureworks®

Threat Intelligence Executive Report

Volume 2021, Number 4

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

- Did the Colonial Pipeline attack really change the ransomware landscape?
- Tactics may change, but commodity tools remain popular
- Threat actors love a lack of security controls

Did the Colonial Pipeline attack really change the ransomware landscape?

Despite law enforcement victories against ransomware operators, network defenders should not let down their guard. Without constant attention to good security practice, fighting ransomware is like playing whack-a-mole.

The May 7, 2021 attack by a Darkside ransomware affiliate on Colonial Pipeline impacted oil and gas distribution throughout the U.S. East Coast, causing sharp price increases and angering U.S. government and law enforcement agencies, not to mention voters.

In the days following this incident, the GOLD WATERFALL threat group that operated Darkside claimed it had lost access to its public-facing infrastructure, presumably as a result of law enforcement efforts. The group announced that it was closing down its ransomware-as-a-service (RaaS) program effective May 13. It also promised to issue decryptors to all victims, although there is little evidence it followed through. On June 7, the U.S. Department of Justice (DOJ) announced that it had seized 63.7 bitcoin (approximately $2.3 million USD), allegedly representing the affiliate portion of the ransom paid by Colonial Pipeline as a result of the Darkside ransomware attack.

Other ransomware groups reacted too. The Avaddon ransomware operators announced that affiliates were no longer permitted to attack organizations in the public sector and had to receive approval before infecting systems. Shortly afterwards, in June, they closed their operation entirely. The GOLD SOUTHFIELD threat group that operates REvil ransomware discontinued its RaaS offering. Underground forums like XSS and RaidForums banned ransomware-related posts.

In an unrelated move on June 16, law enforcement registered an additional victory in the fight against ransomware. Ukrainian police arrested six members of GOLD TAHOE, the group that operates Clop ransomware.

Do these events indicate that the security community is nearing a turning point with the ransomware menace? The numbers suggest not. Days before the Colonial Pipeline attack, the April total of new name-and-shame victims listed on the active leak sites monitored by CTU researchers was 229. The number of new victims increased to 235 in May, the third-highest monthly total since CTU researchers started tracking in 2019.

In addition, the leak sites likely list only a fraction of the victims. For example, Avaddon's leak site listed 182 victims during its entire period of activity. But when the group closed its operation, it released 2,934 individual decryption keys corresponding to different victims.

Furthermore, within days of the GOLD TAHOE arrests, the group added more Clop victims to its leak site. The Babuk ransomware operators, who claimed to have abandoned ransomware in favor of data theft and extortion in late April 2021, started adding victims to a new leak site and boasted they had developed of a new version of their ransomware. They also publicly released the old Babuk ransomware builder for other threat groups to use.

Ransomware group activity levels may fluctuate and individual groups may disappear, but new ransomware families or variants derived from other ransomware appear continuously. Network defenders cannot allow their defenses to drop.

If you do just one thing after reading this:
Monitor endpoints as well as network traffic to pinpoint early signs of ransomware intrusions.

Tactics may change, but commodity tools remain popular

Skilled government-sponsored threat actors adapt their tactics, techniques, and procedures (TTPs) to their targets, but they regularly include popular commodity payloads to achieve their goals. Monitoring for commonly abused offensive security tools like Cobalt Strike helps provide protection from cybercriminals and government-sponsored actors alike.

In May and June 2021, Microsoft exposed additional campaigns by Russian government-sponsored IRON RITUAL (also known as NOBELIUM), the advanced persistent threat (APT) group that carried out the SolarWinds supply chain compromise. IRON RITUAL is linked to Russia's foreign intelligence service (SVR).

In the first campaign, spearphishing emails were sent to more than 350 government organizations, intergovernmental organizations (IGOs), and non-governmental organizations (NGOs). Victims included organizations responsible for anti-corruption activism and conflict mediation in Ukraine, disinformation awareness in the European Union, and distribution of U.S. government foreign aid. The second campaign targeted IT companies, government bodies, NGOs, think tanks, and financial services in the U.S., UK, Germany, Canada, and 32 other countries.

The TTPs in these campaigns provide a contrast to those used in the SolarWinds campaign, where IRON RITUAL conducted a sophisticated supply chain compromise to stealthily access a small number of high-value targets, even though the nature of the targets are similar. The spearphishing activity reported in May was high volume, noisy, and required a victim to perform a series of actions before the malware was installed that provided persistent access to the compromised system. The second campaign involved the threat group sending large numbers of passwords to guess login credentials. This technique is straightforward to detect and relatively easily to prevent.

The first campaign also used Cobalt Strike. This commercial software tool is widely used by authorized security testers, but APT groups and cybercriminals often use unlicensed versions. IRON RITUAL similarly used Cobalt Strike in the SolarWinds attack. Using common offensive security tools for initial access allows threat actors to gain a foothold without exposing valuable components in their arsenal. It can also make attribution more difficult because network defenders cannot tell the difference between a cybercriminal and a government-sponsored threat actor based solely on the use of this type of tool by the attacker.

More information about the TTPs used by IRON RITUAL and other APT groups is available in an advisory released in early May by the U.S. Cybersecurity Infrastructure Security Agency (CISA), the UK National Cyber Security Centre (NCSC), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). CISA and the FBI published an additional alert in late May.

If you do just one thing after reading this:
Search for indicators from common offensive tools like Cobalt Strike when monitoring endpoints and network traffic for early signs of intrusion.

Threat actors love a lack of controls

No one claims that network defense is easy, but most attacks are not sophisticated. Common attack vectors are well known, and their use can be prevented. Organizations that make life hard for threat actors are more likely to avoid attacks.

CTU researchers track a wide range of threat groups that possess many different motivations. Some are focused on financial gain, while others are interested in monitoring NGOs, tracking dissidents, or disrupting elections. One attribute they all have in common is that they love easy ways to access a targeted network, such as weak or compromised credentials, unpatched vulnerabilities, unprotected remote services, single-factor authentication, and a lack of monitoring.

Threat intelligence reports published by CTU researchers in May and June provided evidence of some of these easy wins for adversaries.

- The GOLD ULRICK threat group conducted a Ryuk ransomware attack in early 2021 using well-established tools for which detections already existed.
- Another attacker abused Office 365 email account credentials, likely by trying commonly used passwords, to compromise an organization's network. Because the organization had not implemented MFA for the compromised Office 365 account, the threat actor was able to access the email inbox.
- A Secureworks incident response engagement investigated a network intrusion that started when a user downloaded a malware-infected Zoom installer file from a third-party website.

- Yet another incident started with an individual downloading a messaging app from a malicious website.
- Multiple reports covered attacks that started with the attacker taking advantage of known vulnerabilities, for which patches were available, in unpatched systems.

It's no coincidence that the financial services vertical, which has multiple overlapping cybersecurity compliance requirements and a history of understanding that security and appropriate controls are worthwhile, is not often impacted by ransomware. Every day, organizations prevent attacks from taking place or detect and stop compromises in the early stages. These organizations have implemented MFA, hardened internet-facing devices, mandated strong password and internet download policies, applied patches in a timely fashion, and implemented comprehensive monitoring solutions that look for known indicators. These 'non-events' do not always make for good threat intelligence case studies. However, they reinforce the message that it is the simple oversights that let the adversaries win.

If you do just one thing after reading this:
Implement basic security controls and avoid becoming a target.

Conclusion

Many attacks can be prevented or thwarted in their early stages by employing proven security measures. Organizations should employ comprehensive monitoring and detection across endpoints and network traffic to alert on known threat indicators, including activity from commodity tools. Combining threat intelligence with good security practices makes life much more difficult for threat actors, denying them the easy wins.

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

