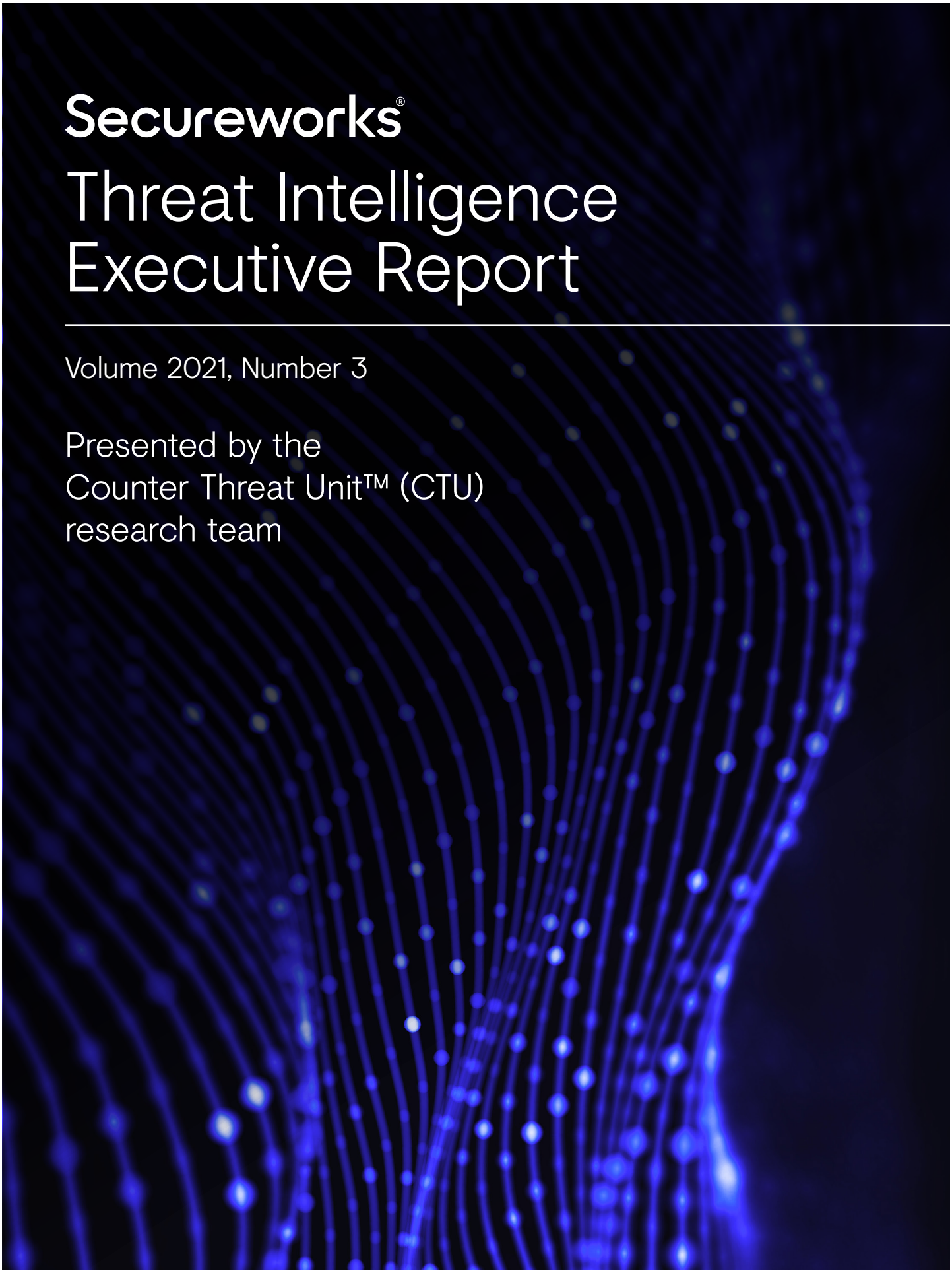
Secureworks®

Threat Intelligence Executive Report

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

- Fighting ransomware: Deter, disrupt, prepare, respond
- Defending against supply chain attacks
- The risk calculation is clear - patch or be punished

Fighting ransomware: Deter, disrupt, prepare, respond

Most importantly, prevent. Recent industry and government anti-ransomware initiatives underline just how big a menace ransomware has become. Ransomware operators continually evolve their tactics to maximize returns and minimize effort. Good fundamental security practices such as patching, monitoring, and implementing multi-factor authentication (MFA) can stop threat actors from gaining access in the first place.

The Institute for Science and Technology's (IST) multi-sector Ransomware Task Force released its ransomware framework in April 2021, advocating nearly 50 interlocking government and private sector strategies to tackle the ransomware plague. Also in April, a United States Department of Justice (DOJ) internal memo outlined the formation of another ransomware task force made up of DOJ prosecutors and U.S. Federal Bureau of Investigation (FBI) agents.

The IST initiative framework's goals are to "**deter** ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; **disrupt** the ransomware business model; help organizations **prepare** for ransomware attacks; and **respond** to ransomware attacks more effectively." The DOJ/FBI initiative appears to be aimed at improving the U.S. government's ability to disrupt attacks and prosecute the criminals behind them.

Both groups face a sizeable challenge. During March and April, criminal operators of the Avaddon, Astro Team, REvil, Darkside, Babuk, DoppelPaymer, Maze, Clop, and Conti ransomware remained highly active.

Of the ransomware families monitored by CTU researchers, the Avaddon ransomware-as-a-service (RaaS) operation added the most victims to its leak site during this period: a total of 44. LV, which is a custom-configured version of REvil, has accumulated 15 victims since appearing on the scene in April. The Clop and Babuk operators appear to be moving toward extortion without encryption, stealing and holding data for ransom without locking victims out of their systems.

To date, CTU researchers have counted at least 1,800 organizations publicly 'named and shamed' on ransomware leak sites. These are largely just the victims that are slow to pay or don't pay. Organizations that immediately pay ransoms generally don't appear on leak sites. Furthermore, just like any financially motivated entity, ransomware operators are constantly evolving their tools and techniques to improve success rates.

Motivation can be difficult to discern. An April 15 statement from the U.S. Treasury regarding sanctions against Russia explicitly linked the financially motivated GOLD DRAKE threat group that operates the Dridex botnet (also known as Evil Corp) with Russia's Federal Security Service (FSB). The U.S. Treasury stated that the FSB enabled GOLD DRAKE to engage in disruptive ransomware attacks and phishing campaigns. Many ransomware operators are based in Russia or other former Soviet states. They operate with the implicit understanding that if they avoid targeting potential victims in those regions, they will remain untroubled by those countries' law enforcement operations. It is likely that Russia perceives criminal ransomware groups as a useful destabilizing influence and is happy to tolerate them, so long as none of their activities negatively impact on Russian interests.

While overall losses for ransomware have not yet equaled those associated with business email compromise, it remains one of the fastest growing and fastest evolving threats. The impact of an individual attack can be huge for the victim. It's not just a question of the ransom cost; there is the potentially near-catastrophic business disruption, the trauma of experiencing and having to recover from an incident, and the consequential costs that may dwarf the initial ransom.

In addition, the move toward extortion without encryption seen during this period exemplifies the macro trend of criminal threat groups focusing on maximum reward for minimal effort. Ransomware carries the overhead of tool development and supporting victims with decrypting their data. Extortion without encryption only requires data theft, eliminating the need to stage detectable malware throughout the compromised environment.

This move means that organizations must focus on detecting these threat groups and their activities earlier in the attack lifecycle. Detecting and preventing unauthorized access, persistence mechanisms, and lateral movement together form a much more effective strategy than attempting to detect and prevent the execution of ransomware. The various task force activities will undoubtedly be helpful, but by avoiding basic security mistakes like failing to patch or not protecting systems with MFA, organizations can already take big steps toward preventing attackers from gaining access.

If you do just one thing after reading this:
Protect access to internet-facing systems by implementing MFA.

Defending against supply chain attacks

You can't secure what you can't control. That means perfect supply chain security is not possible. But to guard against supply chain attacks, organizations can do three things:

- **Identify: Know which systems and assets the supply chain can access**
- **Assess: Decide what's essential and reduce access accordingly**
- **Mitigate: Secure those touch points to minimize impact**

In April, Codecov, a code review and auditing company that helps 29,000 other organizations test their own code for mistakes and vulnerabilities, announced that its software had been compromised. Many of Codecov's customers sell software to their own clients. The altered version of Codecov's Bash Uploader script could steal data from code development environments. That data could include tokens or keys that provide access to source-code repositories and other sensitive information assets. By breaching Codecov, the attacker could potentially unleash numerous other supply chain breaches.

Ransomware attacks also have supply chain implications: an April ransomware attack on Dutch logistics firm Bakker Logistiek led to a nationwide cheese shortage in Dutch supermarkets. Supply chain attacks that target systems or software distributed among hundreds or thousands of organizations are less common. Examples include the attack on Codecov software, the Russian compromise of SolarWinds Orion platform updates in 2020, and the attacks targeting Accellion File Transfer Appliances (FTA) in late 2020 and early 2021. But these incidents amply demonstrate just how hard some risks are to control.

Also in April, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute for Standards and Technology (NIST) published Defending Against Software Supply Chain Attacks to help organizations identify, assess, and mitigate software supply chain risks. The publication reviews risks, describes common attack techniques, and makes recommendations to help both software vendors and their customers protect against these attacks.

Supply chain assurance can be like compliance. It's easy to check boxes, but reducing access and potential impact is what make it effective.

If you do just one thing after reading this:
Apply the advice in the CISA/NIST report.

The risk calculation is clear – patch or be punished

If you don't patch, your chances of experiencing a breach increase exponentially. So do the potential impact and complexity of any breach. Patching is one of the most important ways to protect against threat actors, whether they want to drop ransomware, steal credentials, or exfiltrate sensitive data.

During March and April 2021, CTU researchers published 23 threat intelligence reports and 67 vulnerability assessments that included advice about patching. More than half of the threat intelligence reports and a considerable amount of media coverage concerned Microsoft Exchange Server vulnerabilities: four linked in March to exploitation by government-sponsored threat actors, and four additional remote code execution vulnerabilities addressed in April.

The Exchange Server vulnerabilities may have grabbed the headlines, but they weren't the only ones catching threat actors' attention. Other vulnerabilities prompting the advice to patch as soon as possible included ones affecting Fortinet FortiOS, macOS, Chrome, and SAP NetWeaver. The SAP NetWeaver vulnerability was disclosed in 2020 and received the highest possible Common Vulnerability Scoring System (CVSS) severity score of 10.

The U.S. National Security Agency (NSA), FBI, and CISA also issued a joint advisory warning that the Russian foreign intelligence service (SVR) was actively exploiting five well-known vulnerabilities in popular authentication and virtualization software used in enterprises around the world. Several of these vulnerabilities were previously leveraged

by multiple threat groups. The NSA states that mitigation against these vulnerabilities is "critically important as U.S. and allied networks are constantly scanned, targeted, and exploited by Russian state-sponsored cyber actors." This advisory followed a similar publication in November 2020 about vulnerabilities targeted by Chinese threat actors.

Along with 'implement MFA', and 'use comprehensive endpoint and network monitoring', 'patch in a timely fashion' is one of the most frequent recommendations by Secureworks incident responders. There are reasons, some of them risk related, why organizations won't or can't patch in a timely fashion. But threat actors of all types, from government-sponsored threat groups to financially motivated criminals, are actively looking for unpatched vulnerabilities they can exploit. Organizations may protect the front door to systems with MFA and keep the back door locked through phishing education, but those security measures won't prevent breaches if the windows are all left open.

Patching is an essential element of a security strategy. Knowing what systems are in the network, assessing risk with the help of threat intelligence, and designing a prioritized patch management system are key steps in implementing that strategy. If patching a specific system isn't possible, then building in compensating controls to prevent, detect and contain successful exploitation is essential. But that should be the exception and not the rule. Whether you are concerned about supply chain attacks, ransomware, or other types of attack, patching is one of the most effective ways to reduce your risk.

If you do just one thing after reading this:
Update your asset inventory. You can't patch it if you don't know you use it.

Conclusion

The threat landscape continues to evolve. Individual threat groups rise and fall. Attack types fluctuate in frequency of use. However, the importance of implementing basic good security practices remains constant. Why make life easy for threat actors? Implement comprehensive network and endpoint monitoring and detection solutions, use MFA, and patch in a regular and timely fashion to stop them from gaining initial access.

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 global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions. www.secureworks.com

Corporate Headquarters
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

