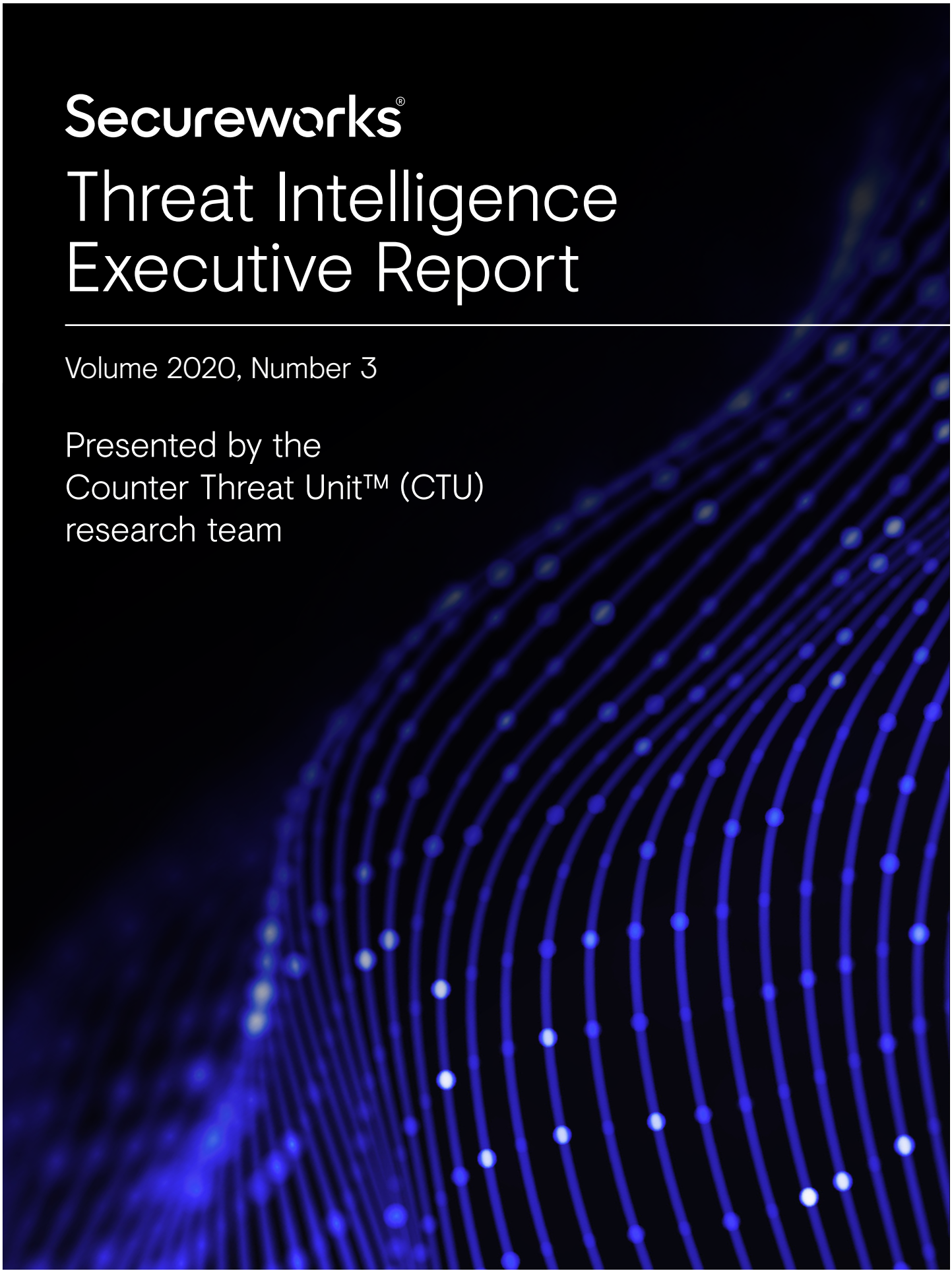
Secureworks®

Threat Intelligence Executive Report

Volume 2020, 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 2020, CTU™ researchers observed notable developments in threat behaviors, the global threat landscape, and security trends, and identified lessons to consider.

- Multiple threat actors leverage COVID-19
- Remote access security is essential in the current working environment
- Big breaches begin with small intrusions

Multiple threat actors leverage COVID-19

Observed threat volume has not increased, but threat actors are exploiting coronavirus concerns.

CTU researchers have been tracking cyber threat activity associated with the COVID-19 (also known as coronavirus) pandemic since March 2020. Many threat actors are leveraging interest in the pandemic to attract victims. However, while a slight increase in scanning and other activity levels began in mid-April, there has been very little change in the overall threat faced by most organizations as of this publication.

Due to the global interest in the pandemic, government-sponsored threat groups have tailored their lures to exploit this worldwide event. For example, COPPER FIELDSTONE targeted Indian citizens with a malicious Excel file that delivered malware capable of stealing files and system data; BRONZE PRESIDENT targeted Taiwanese citizens with a phishing lure that delivered a fully-featured attacker toolkit; and a likely China-based threat group targeted Mongolian citizens with a malicious file that dropped previously unobserved malware. Organizations working in direct response to the pandemic, such as healthcare or pharmaceutical organizations that are developing a vaccine, generating research, or formulating policy advice, could be at greater risk of targeting from government-sponsored actors.

Low-sophistication phishing, smishing (phishing via SMS), and other scam activity continues. Cybercriminal phishing campaigns with coronavirus-themed lures include a coronavirus “antivirus” website delivering a previously unknown remote access tool for the BlackNET botnet, a compressed file that drops information-stealing malware (also known as an infostealer), and an email that combines World Health Organization (WHO) and Centers for Disease Control and Prevention (CDC) branding to deliver an infostealer.

Threat actors also continue to register fraudulent domains. In fact, over 90,000 coronavirus-themed domains using terms such as covid, corona, chineseflu, and wuhan were created between January 1 and April 1. However, a large proportion

of them are not directly associated with malicious activity, so it is important that organizations rely on verified threat indicators to avoid burdening security teams.

CTU researchers observed ransomware attacks targeting organizations in healthcare-related industries, although there is no indication that this is a broad change in targeting. The threat groups operating the ransomware likely continue to opportunistically identify targets across all industries. Threat actors recognize that healthcare organizations are under particular pressure due to the pandemic and therefore could be more susceptible to extortion.

Threat actors are also exploiting the increased use of teleconferencing solutions as employees work from home during the pandemic. Attackers are spoofing teleconference provider applications to deliver malware and are creating malicious domains imitating providers such as Zoom, Microsoft Teams, and Google Hangouts.

Key Takeaway

CTU researchers have not observed an overall increase in threats due to COVID-19. Threat actors have shifted to using coronavirus as a theme and have increased their scanning activity as organizations transitioned to remote working. Employees should be aware that unexpected coronavirus-themed emails could be malicious.

Remote access security is essential in the current working environment

Securing remote access protects organizations during the pandemic and beyond.

CTU researchers observed a sharp increase in the use of remote access services such as virtual private networks (VPNs) or Remote Desktop Protocol (RDP) as businesses transitioned to employees working from home. In many cases, this change created a large increase in the organizations' external attack surface. Because the transition took place quickly to meet new legal requirements, some organizations did not properly plan full-scale deployment of technologies that may previously have been used by a small fraction of its workforce.

Secureworks telemetry shows that there has not been an overall upturn in intrusion activity or in confirmed security incidents. What has increased is scanning activity for remote access service vulnerabilities. Criminal and government-sponsored threat groups rapidly began exploiting misconfigured remote access technology for financial gain and espionage, respectively.

CTU researchers had observed an increase in disclosed network security device flaws prior to COVID-19, and the additional reliance on these devices during the pandemic makes organizations more vulnerable. The rapid expansion in the use of remote access solutions could cause organizations to prioritize infrastructure scalability and reliability over patching. CTU researchers recommend that organizations continue to assign appropriate resources to ensure timely security updates for all elements of network infrastructure.

Key Takeaway

Organizations must not overlook remote access security, especially given that some level of remote working may continue after the COVID-19 crisis. Organizations should apply security updates in a timely manner and use multi-factor authentication for external access into the corporate environment.

Big breaches begin with small intrusions

CTU researchers continue to monitor numerous post-intrusion ransomware operations that use commodity malware infections or remote access systems as the foothold in a network. Time is money for these threat groups. They appear to continually strive to identify potential victims quickly, reduce dwell times, and deploy ransomware to the maximum number of endpoints in the least amount of time.

Minor incidents can quickly escalate into major crises, making constant monitoring and fast detection vital.

In malware-facilitated attacks, the malware often reports host and network attributes to its command and control (C2) servers. This data helps attackers choose targets that are high value or are easily exploitable, providing attackers with a head start before they interact with the victim's network. Combining this information with previous access to a network entry point, stolen credentials, and network topology details helps a threat actor quickly move laterally and deploy ransomware.

Remote access systems such as RDP or virtual desktop infrastructure (VDI) servers can provide immediate access to an organization's internal network. Threat groups distributing ransomware frequently purchase brute forced or stolen credentials for these systems on underground forums.

Organizations should not discount a single antivirus alert or spurious login to a forgotten cloud server as a sign of a minor intrusion. They can quickly escalate into a destructive attack and leaked data on the public Internet.

Key Takeaway

Organizations must prioritize remediation efforts when security controls identify malware infections, especially those associated with ransomware. A process that enables rapid recognition of an infection and automates isolation of the malware is most likely to prevent attacks from succeeding. Tracking asset inventory and monitoring network ingress points can identify poorly defended systems that could allow unauthorized remote access.

Conclusion

Few aspects of life today have escaped the impact of COVID-19. Cybersecurity is no exception, whether it's threat actors leveraging the pandemic as an opportunity or organizations having to quickly switch to secure remote working. To minimize the risk of major security events during this crisis, organizations should employ good, fundamental security practices:

- Maintain awareness about coronavirus-related threats and train employees to recognize and report them.
- Apply appropriate patches as soon as possible, especially for remote access technology.
- Implement protection, detection, and remediation processes to prevent minor breaches from turning into major incidents.

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 keeps organizations safe in a digitally connected world. By combining our visibility into threat behavior across customer environments with our expertise and a powerful processing platform, we help organizations anticipate emerging threats, detect malicious activity in real time, assess risk, and take appropriate action to avoid or mitigate risk of a security breach. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™ 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

