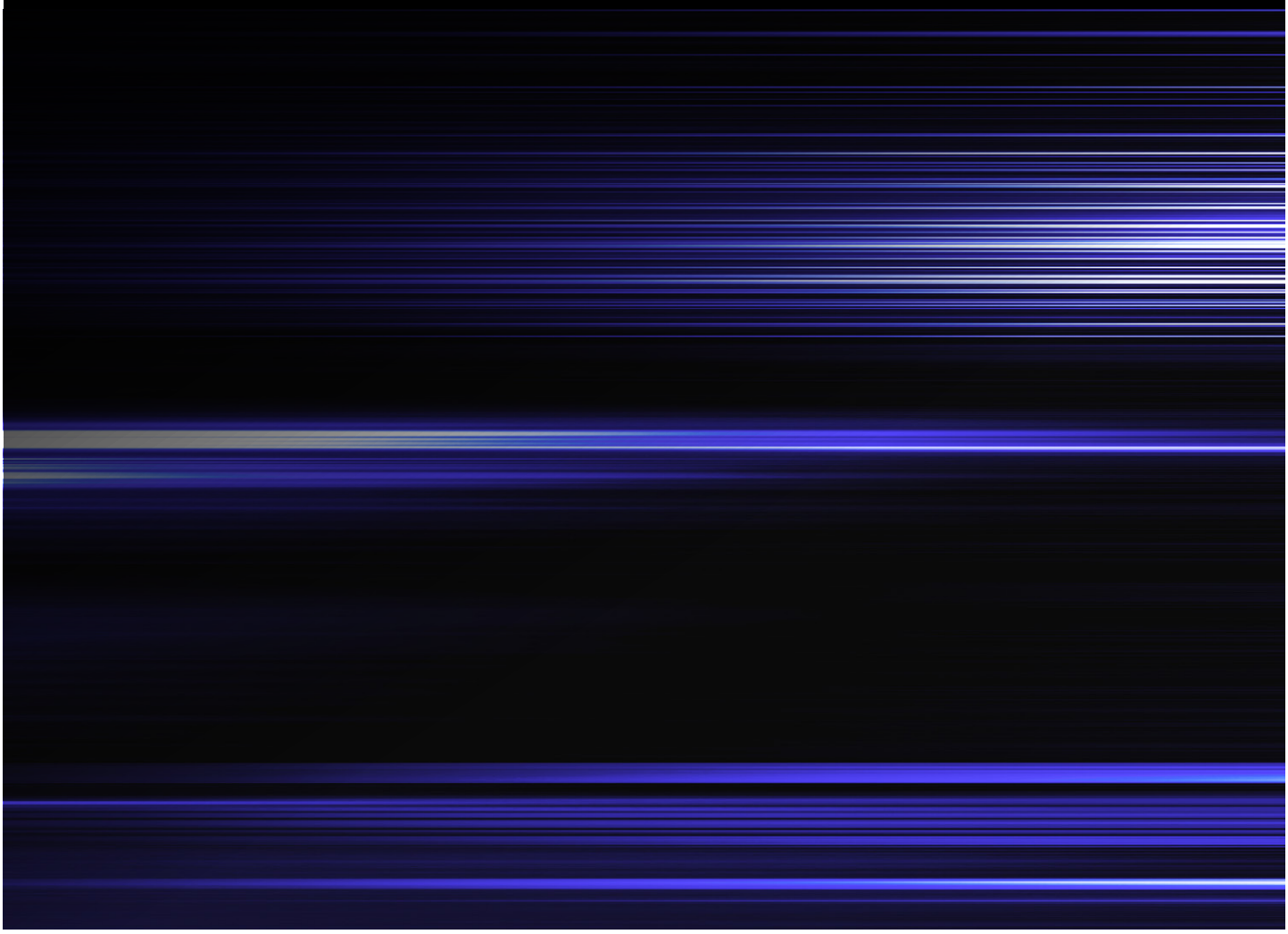
Secureworks®

Threat Intelligence Executive Report

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

- COVID-19 vaccine research becomes advanced persistent threat (APT) target
- Business email compromise adopted by broader variety of threat actors
- The ransomware threat matures and grows

COVID-19 vaccine research becomes APT target

Attackers endeavor to steal data and intellectual property rather than disrupt activity

As the COVID-19 pandemic continues to affect countries globally, the world's primary goal is to develop a vaccine in order to control the virus and return life to normal. Many pharmaceutical, biotechnology, and healthcare companies are involved in the research effort alongside universities and government organizations.

During July and August, there were multiple reports of cyber intrusions from government-sponsored advanced persistent threat (APT) groups targeting this research. The UK National Cyber Security Centre published a report in partnership with Canadian and U.S. agencies that highlighted Russian efforts to access COVID-19 vaccine development details using custom malware. This report followed earlier advisories from the U.S. Federal Bureau of Investigation (FBI) and Interpol that detailed how criminal and government-sponsored threat actors were targeting organizations around the world. Other reports suggest that groups from Russia, China, and Iran have also been involved in malicious activity.

CTU analysis corroborates public reporting of attempts to access this data. However, there have been no indications of an intent to disrupt or manipulate research efforts. As of this publication, observed campaigns have been highly targeted and focused on identifying and exfiltrating sensitive information. During one engagement, Secureworks incident responders investigated an Office 365 compromise at a biotechnology organization involved in the COVID-19 response. Analysis revealed the threat actor downloading technical data, product development files, and the corporate address book.

As expected with such a broad range of threat actors, these attacks employ a variety of tactics. While some incidents involve sophisticated custom malware, the majority of these attacks use simple tactics: exploiting unpatched vulnerabilities on public-facing applications, leveraging credentials previously stolen by other threat actors, or acquiring credentials through brute-force or password-spraying attacks.

Key Takeaway

Organizations involved in the COVID-19 response should be highly vigilant against cyberespionage attacks stealing intellectual property. As with any targeted network intrusion, defenders should focus on patching systems, implementing multi-factor authentication (MFA) for all external access, and monitoring for unusual behavior on servers and endpoints.

Business email compromise adopted by broader variety of threat actors

Business email compromise (BEC) is the most common incident type observed during Secureworks incident response engagements, second to ransomware. BEC also ranks second to ransomware as one of the most lucrative threats.

Likely Russian threat group adopts high-reward threat activity

BEC schemes are typically the modus operandi of West African criminal gangs. For example, the FBI arrested Nigerian Ramon Olorunwa Abbas (also known as Hushpuppi) in June 2020 in Dubai. British Nigerian dual citizen Habeeb Audu was extradited to the U.S. from the UK on BEC charges in July 2020.

However, a July 2020 report described a new entrant into the BEC arena: a likely Russian criminal group named Cosmic Lynx. Since July 2019, this group has targeted senior executives in multiple global organizations. The executives had job titles such as vice president, general manager, and managing director. The threat actors hijacked the identities of legitimate UK-based corporate acquisition attorneys to trick the targeted executives into directing payments, supposedly for confidential acquisitions of Asian companies, to money mule accounts in Hong Kong.

The entry of Russian criminal threat actors into BEC activity is unsurprising given their ubiquity when it comes to conducting ransomware attacks. FBI data suggests that BEC accounted for over $1.7 billion USD of losses in 2019. According to the Anti-Phishing Working Group's Q2 2020 report, the average wire transfer loss from a BEC attack in the second quarter of 2020 was $80,183, a substantial increase from $54,000 in the first quarter. Given that BEC often requires less technical development resources than malware-based attacks, it is likely that other Russian criminal threat groups will follow Cosmic Lynx's example.

Key Takeaway

While BEC scams affect individuals and organizations of all sizes, Cosmic Lynx's victimology is a reminder that large organizations and their senior executives are just as vulnerable as the more typically targeted small enterprises, junior employees, and private individuals. Organizations should educate employees responsible for approving wire transfers about BEC tactics and techniques, mandate MFA on all significant financial transactions, verify payment requests using previously established non-email channels such as phone or secure messaging, and maintain lists of known-good accounts.

Ransomware threat matures and grows

Specialization is one factor behind the evolution and expansion

Since late 2019, the potential for higher payouts from post-intrusion ransomware attacks has motivated more and more threat actors to switch from commodity ransomware campaigns.

In addition, new groups operating these schemes are identified every week. Because the underground economy offers nearly all the services and tools needed for a post-intrusion ransomware attack, the required components are readily available to anyone who is willing to pay. As a result, the barrier to entry is continually lowered for carrying out ransomware attacks that are highly destructive and costly to remediate.

This increase in the number of ransomware operators is not the only development – 'business' practices are shifting from generalization to specialization. The original post-intrusion ransomware groups such as GOLD LOWELL, which controlled the SamsamCrypt ransomware, operated all parts of the attack cycle. These tasks included authoring the malware, performing the initial infection, and negotiating ransom payments. In 2019, threat groups developed

other approaches. The apparent partnership between TrickBot operator GOLD BLACKBURN and Ryuk operator GOLD ULRICK introduced division of labor. GOLD BLACKBURN used TrickBot to perform the initial infections through mass-phishing emails and gathered stolen credentials from infected networks. GOLD ULRICK then purchased access to the most attractive targets. GOLD SOUTHFIELD later launched an affiliate model that provided the REvil ransomware to a wide variety of other threat actors, who then attacked organizations across the world.

As multiple threat groups specialize in specific elements of the ransomware attack chain, the threat continues to grow at an alarming pace. Threat groups that operate automated portions of the attack chain are recruiting individuals to manually expand access across a compromised network and prepare the ransomware for execution. In addition, CTU researchers have observed multiple listings in underground forums listings in 2020 seeking network administrators and advertising ransomware.

The "name-and-shame" approach often leads to larger ransoms because the theft of sensitive data and the threat of disclosure or sale increase the potential risk to victims. The tactic also creates additional extortion opportunities. Not only can the threat actors demand money to release the decryptor, they can also demand an extra fee to destroy the data.

Key Takeaway

Ransomware has grown into one of the most dangerous threats organizations face today. As the groups running these attacks specialize in specific portions of the attack chain and become more efficient, they increase the number of possible attacks. There is no evidence that this trend is decreasing. Organizations should ensure they are prepared to defend against both the number and range of attacks they could experience.

Conclusion

While organizations in sectors like biotech and pharmaceuticals can expect to be the targets of cyberespionage attacks due to COVID-19, all sectors are vulnerable to increasingly common ransomware and BEC attacks. Financially driven criminal threat groups are more likely to prioritize a victim's ability to pay rather than a product or service type. Understanding what attacks your organization might attract is an important initial element of defense.

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) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs. With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience. 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

