Secureworks®

Threat Intelligence Executive Report

Volume 2021, Number 1

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

- SolarWinds compromise affects large number of organizations
- Russian offensive cyber operations persist, global and undeterred
- Maze bows out, Egregor steps in

SolarWinds compromise affects large number of organizations

Attack targeted the U.S. government and its supply chain

On December 13, 2020, FireEye and Microsoft described a sophisticated attack that leveraged compromised SolarWinds Orion business software. A threat group added malicious code to the Orion product, which was then distributed to customers via normal software update mechanisms. This SUNBURST backdoor contacted a command and control server, where the threat actors triaged victims and selected those of interest for follow-on exploitation activity.

While a large number of organizations installed the malicious SolarWinds update, only a few have experienced follow-on activity. CTU analysis suggests that a threat group linked to the Russian SVR foreign intelligence agency, likely IRON HEMLOCK (also known as Cozy Bear or APT29), is responsible for this campaign. This type of threat group has very specific intelligence objectives, so any follow-on activity will likely be highly targeted. On December 17, Microsoft reported that only around 40 of its customers were impacted. All confirmed victims have been U.S. government agencies, political organizations, and think tanks, along with the technology companies in those organizations' supply chains. The risk to companies outside of these sectors is likely to be very low.

The threat group has developed a range of intrusion methods and capabilities that enable it to continue to operate effectively in spite of multiple public disclosures. Its focus on technology companies beyond SolarWinds suggests that additional supply-chain compromises may be possible. Organizations should follow best practices to harden systems, such as restricting servers from communicating directly to the internet. CTU researchers also recommend that organizations apply security-related software updates in a timely manner, as the risk of unpatched vulnerabilities outweighs the risk of a supply-chain attack.

A notable aspect of this campaign was the threat actors' abuse of identity federation in their follow-on activity. Identity federation links a user's electronic identity and attributes across multiple distinct identity management systems. Many organizations rely on it for single sign-on across on-premises and cloud resources, passing signed authentication tokens between systems to grant users access. If a threat actor steals the relevant keys used to sign those tokens, the trust model collapses and the threat actor can gain unrestricted access to any related systems. Organizations should protect these keys, as detecting this type of abuse after the keys are compromised is challenging. Keys should be changed if there is any suspicion that they are no longer private.

Key Takeaway

While this campaign has prompted significant media attention and concern, the impact to most organizations has been very low. The incident demonstrates the actions that sophisticated and determined attackers can perpetrate to achieve objectives, draws attention to the dangers of supply-chain attacks, and brings awareness to the abuse of trust in identity federation. Organizations should consider the lessons learned and apply appropriate protections.

Russian offensive cyber operations persist, global and undeterred

A busy year for Russian threat groups

Throughout 2020, offensive cyber operations by Russia's military and intelligence services were met with public rebuke by victims throughout Europe, the Middle East, and the Americas. There were multiple criticisms in December alone:

- Norway publicly accused Russia's military intelligence agency of breaching Norwegian Parliament email accounts earlier in 2020. A Norwegian Police Security Service investigation claimed that the incident was associated with a larger Office365 credential-harvesting campaign that began in 2019. The investigation attributed the campaign to Russia's General Staff Main Intelligence Directorate (GRU), which CTU researchers associate with the IRON TWILIGHT threat group.
- The U.S. National Security Agency cited unidentified Russian government-sponsored threat actors for exploiting VMWare Access and VMWare Identity Manager vulnerabilities to compromise a target network, establish persistence, and gain access to protected data.
- Russian threat actors were blamed for the SolarWinds supply chain compromise that was discovered in December.

These accusations show that Russia continued to present a credible and potent cyber threat to governments and organizations worldwide throughout 2020. While the multiple sanctions, indictments, and arrest warrants did not deter Russian activity, they publicly reveal Russia's capabilities, targeting, and intent.

For example, the Russian IRON HEMLOCK threat group was responsible for espionage operations against COVID-19 vaccine research and development organizations during 2020. In a July advisory, the United Kingdom's GCHQ detailed the tactics, techniques, and procedures used in these attacks. CTU analysis indicates that IRON HEMLOCK was also likely responsible for the SolarWinds compromise.

U.S. and German governments initiated criminal cases in 2020 against IRON TWILIGHT members:

- Germany issued an arrest warrant for an IRON TWILIGHT member's alleged involvement in the large-scale 2015 breach of the German Parliament (Bundestag).
- A U.S federal grand jury indicted six GRU military intelligence officers for their purported roles in destructive and disruptive attacks against Ukrainian critical infrastructure, a French political campaign, the 2018 Winter Olympics in South Korea, and NotPetya malware victims.

Key Takeaway

In Russia's international cyberespionage and targeting, its military and foreign intelligence cyber units prioritize organizations that support government bodies, military forces, international organizations, diplomatic or consular units, and political parties. Organizations that fit these criteria should adopt a defense-in-depth strategy and understand relevant threat indicators and behavior. By applying this strategy and knowledge to on-premises and cloud-based systems, organizations can mitigate the threats posed by Russia as it seeks to protect and expand its power and influence on the world stage.

Maze bows out, Egregor steps in

Threat actors and their activities may change, but remedies and protective measures remain the same

GOLD VILLAGE was the first threat group to operationalize data theft prior to encrypting systems. In November 2019, it was also the first threat group to launch a 'name-and-shame' leak site to disclose data the threat actors stole prior to encrypting files via their Maze ransomware. One year later, on November 1, 2020, the threat actors announced the closure of their ransomware operation. The melodramatically worded proclamation criticized the world for its failure to secure data, denied the existence of the Maze Cartel collaboration with LockBit and RagnarLocker ransomware, and asserted that GOLD VILLAGE never had partners or official successors.

In November and December, GOLD VILLAGE's assertion that it did not have a successor was questioned when GOLD PHANTOM, the operator of Egregor ransomware, rose to prominence through increasingly aggressive activity. Egregor shares traits with both the Maze and Sekhmet ransomware families, such as encryption methods, code elements, and the use of both dark web and surface web leak sites.

By early December 2020, GOLD PHANTOM had listed 187 victims on the Egregor leak site. The average of 62 victims per month in the leak site's first three months made GOLD PHANTOM the most prolific name-and-shame ransomware operator. Egregor is operated as ransomware-as-a-service (RaaS), is distributed through phishing campaigns, and has been observed following Qakbot infections. The ransomware operator ensures that the target host is not located in one of the countries in the Commonwealth of Independent States (CIS), a strong indicator that GOLD PHANTOM, like GOLD VILLAGE, is based in one the CIS member countries.

There were other notable ransomware changes in November and December:

- The MountLocker RaaS operation broadened its targeting and improved its ability to evade security software.
- GOLD DUPONT, distributor of the 777 ransomware, established a Tor-based leak site to name and shame victims.
- A previously unobserved ransomware family dubbed RegretLocker encrypted virtual hard drives and closed open files for encryption.
- The Darkside ransomware group launched an affiliate program, announcing details on two Russian-language cybercrime forums.

Key Takeaway

Ransomware operators work diligently to extend their reach and evade detection by recruiting affiliates or by updating their tools. An increasing number are pursuing name-and-shame tactics to extort maximum payments from their victims. However, the initial access vectors, such as unprotected internet-facing services and phishing spam, rarely change. Many malware families, including Egregor, use common tools such as Cobalt Strike for post-exploitation activity. Organizations should implement good security practices, use multi-factor authentication to protect RDP and other internet-facing access, perform regular and timely patching, and leverage endpoint and network monitoring and detection to identify unusual behaviors.

Conclusion

Although government-sponsored threat actors frequently lead the way in leveraging new tactics, techniques, and procedures, the indiscriminate targeting by criminal threat actors and ransomware operators is a greater threat to most organizations. Ransomware groups regularly gain access using traditional techniques and common tools, but they are often quick to adopt effective techniques and may leverage the identity federation abuse used in the SolarWinds compromise. Although only a small number of organizations have been impacted by SolarWinds follow-on exploitation activity, all organizations can benefit by understanding these intrusion methods and taking protective actions before other threat actors adopt them.

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

