Secureworks®

Threat Intelligence Executive Report

Volume 2021, Number 2

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

- Emotet botnet disrupted by coordinated law enforcement action
- Florida water treatment facility compromised
- Scan-and-exploit victims listed on ransomware leak site

Emotet botnet disrupted by coordinated law enforcement action

The botnet is gone for now, but organizations should not drop their guard

In late January 2021, European and North American law enforcement agencies worked together to disrupt the Emotet botnet. The operation was coordinated by Europol, which called Emotet "one of the most significant botnets of the past decade." Since 2016, the botnet has been operated as a pay-per-install service that distributed malware on behalf of threat actors. It has consistently been one of the top cybercrime threats affecting Secureworks customers.

Investigators took control of the infrastructure, causing the GOLD CRESTWOOD threat group that operates Emotet to lose access to the entire botnet. As a result, existing Emotet infections are no longer operational and will not deliver additional malicious payloads. However, it is likely that existing infections already dropped second-stage malware such as TrickBot or Qakbot, depending on when the system was first infected.

The risk from Emotet may be neutralized as of this publication, but it is not unusual for GOLD CRESTWOOD to take extended breaks from operations. GOLD CRESTWOOD could start forming a new botnet using hosting providers that are less responsive to law enforcement action. The group's effectiveness at convincing victims to open phishing emails means it will likely retain phishing as an initial attack vector for future operations.

Key Takeaway

Despite the Emotet takedown, CTU researchers recommend that organizations maintain vigilance, as any second-stage malware that was dropped is capable of extensive damage when exploited by other threat actors. Organizations should apply a layered approach to defend against these types of attacks, including training personnel to recognize and report phishing attempts.

Florida water treatment facility compromised

The threat actor's identity may be murky, but the lessons are clear

On February 5, 2021, a threat actor accessed the computer network of a water treatment facility in Oldsmar, Florida, likely by abusing the TeamViewer desktop-sharing software. They then attempted to increase the quantity of water purification chemicals to toxic levels. The increase was immediately detected and reversed. The attack caused widespread media concern and is under investigation by federal law enforcement agencies.

This cyberattack is not the first against a water facility: Iranian threat actors were suspects in attacks on Israeli water infrastructure in April and June 2020. Critical infrastructure entities such as water facilities and other utility organizations are appealing targets for government-sponsored threat groups. Although most media coverage of the Oldsmar incident assumes a hostile country was responsible, authorities have not identified the attacker. It could have been a disgruntled insider or a prankster.

Initial reports suggest that the attacker employed elementary tradecraft, as a visibly moving cursor on the operator's workstation made the attacker's activities easily detectable. Multiple cybersecurity weaknesses, such as an outdated operating system, the lack of a firewall, and a shared TeamViewer password, exposed the facility to potential attackers of all skill levels.

Key Takeaway

Good security hygiene is essential for critical infrastructure entities, where breaches can potentially result in deaths. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides general mitigation guidance, recommendations for securing remote control software, and specific advice for water facilities.

Scan-and-exploit victims listed on ransomware leak site

Ransomware threat group experiments with encryption-free extortion

In mid-December 2020, unknown threat actors stole sensitive data from dozens of organizations. The attackers performed an opportunistic scan-and-exploit campaign and used a pair of new exploits against Accellion File Transfer Appliance (FTA) devices. Although Accellion responded swiftly and issued patches to address the vulnerabilities, the threat actors leveraged another pair of new exploits to conduct a second round of attacks in January 2021.

The impact of these attacks worsened when GOLD TAHOE, the threat group that operates the Clop ransomware, listed victims and stolen data on its Clop leak site. This site has previously been used to name and shame Clop ransomware victims and coerce them into paying the ransom. However, no ransomware was deployed in this campaign. The data was stolen from the files within the Accellion FTA solution and not from the organizations' networks, which had not been compromised. It is unclear if GOLD TAHOE conducted the data thefts or acted as a facilitator for the follow-on extortion, leveraging its leak site and reputation.

This activity could mark the beginning of a new phase in hybrid ransomware attacks. Threat actors may opt for fast-paced "smash-and-grab" data thefts instead of time-consuming intrusions and subsequent ransomware deployments. They then publicly leak data to coerce the victim and other potentially impacted stakeholders into paying to have the data returned or deleted.

Key Takeaway

Organizations can mitigate ransomware and data theft by hardening their network perimeter through patching systems, segregating the network, deploying multi-factor authentication, and reducing the attack surface to the minimum number of critical services. For on-premises and cloud environments, organizations should deploy enterprise detection and response (EDR) solutions and collect security telemetry via an extended detection and response (XDR) platform for visibility and early detection of intrusions before theft or ransomware deployment can occur. CISA Alert AA21-055A provides mitigation and remediation guidance for Accellion FTA users.

Conclusion

The threat landscape is constantly changing. Attackers evolve tactics to maximize returns and minimize investment. They may face disruption from law enforcement but then resume malicious activity using the same guise or a new approach. Incidents that appear similar on the surface could have different root causes. Despite these wide-ranging and disparate factors, the need for good security practice is constant. Regularly patching systems, implementing detection and response solutions, and employing multi-factor authentication can help protect organizations against a variety of threats.

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

