Secureworks®

Threat Intelligence Executive Report

Volume 2021, Number 6

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

- Qakbot resurrected and returning to ransomware
- Cobalt Strike benefits penetration testers and malicious attackers alike
- Law enforcement has ransomware in its sights

Qakbot resurrected and returning to ransomware

A ransomware attack comprises a number of different stages between initial access and final deployment of ransomware. The attack could involve several threat actors, a variety of techniques, and complex chains of tools and malware. Loader malware and botnets such as Qakbot play a significant role in ransomware attack chains, making monitoring their activities vital.

On September 9, 2021, CTU researchers observed the Qakbot (also known as Qbot and Pinkslip) botnet resuming activity after a two-month hiatus. Qakbot is a modular malware framework that can steal credentials, deliver spam, and intercept and manipulate web traffic. Because infected hosts are recruited into the Qakbot botnet, the name is used for both the botnet and the malware. The GOLD LAGOON threat group has operated Qakbot almost continuously since 2007. There have been gaps in Qakbot activity when elements of its infrastructure idled and stopped communicating, but this was the first break when vital infrastructure was completely taken offline.

Loader malware and botnets are examples of ransomware 'enablers' or 'precursors', delivering additional elements of the attack chain. The threat actors associated with loaders and botnets may not themselves be ransomware operators or affiliates, but they may rent or sell their services to ransomware groups and other cybercriminals. Sometimes they diversify into ransomware activity. For example, GOLD DRAKE operates the Dridex botnet and multiple ransomware variants, including BitPaymer and PayloadBin.

There is no evidence that GOLD LAGOON is planning to diversify into ransomware, but the threat group is increasingly associated with ransomware delivery. Throughout 2021, CTU researchers have observed threat actors using Qakbot to deliver malware on compromised hosts as a precursor to ransomware deployment. Organizations must be able to detect and respond quickly to its presence.

If you do just one thing after reading this:
Deploy countermeasures that can detect Qakbot and other common precursor malware.

Cobalt Strike benefits penetration testers and malicious attackers alike

Malicious use of commercial tools offers many benefits to threat actors. The unexpected presence of Cobalt Strike on a system could be an indication that a threat actor is present.

Cobalt Strike is a commercially available and widely used penetration testing toolkit. Developed for teams conducting authorized security assessments, it is becoming more and more popular with cybercriminals and malicious government-sponsored actors. Increasingly, CTU researchers have observed threat actors using Cobalt Strike in the ransomware attack chain. For example, in September threat actors used it and other legitimate tools in a Hive ransomware attack.

Using publicly available products provides threat actors with multiple benefits. For example, Cobalt Strike is easily available and ubiquitous, making it hard to attribute. It is fully featured, well documented, and requires little additional development, making it easy to use. Its versatility means that threat groups can use it for many aspects of their attacks.

Despite all these benefits, one threat actor created a reimplementation of Cobalt Strike named Vermilion Strike. In addition to full Linux and Windows versions, there is a 'stripped-down' version that focuses on just one type of communication. It is possible that the threat actor wanted to retain Cobalt Strike's benefits while evading endpoint security solutions that check for Cobalt Strike code. The similarities could cause detected Vermilion Strike activity to be misidentified as Cobalt Strike, providing operational security for the threat actor.

Unexpectedly detecting Cobalt Strike activity on a system does not necessarily indicate an impending ransomware attack. However, if this activity is not attributable to an authorized penetration test, then it is likely to be a sign of threat actor activity that merits immediate response.

If you do just one thing after reading this:
Monitor for unauthorized use of Cobalt Strike and other commercial tools to detect signs of intrusions.

Law enforcement has ransomware in its sights

Law enforcement agencies are scoring wins against ransomware operators and affiliates. However, these victories should not cause network defenders to relax. Ransomware groups continue to adapt, and their attacks persist.

Law enforcement agencies aggressively pursued ransomware operators during September and October. At the beginning of September, the Irish police force disrupted the GOLD ULRICK group responsible for the May 2021 Conti ransomware attack on the Irish Health Service (HSE). This law enforcement operation, which included cooperation from Europol and Interpol, targeted Conti's IT infrastructure.

A multi-country law enforcement operation orchestrated the October 17 shutdown of GOLD SOUTHFIELD's REvil ransomware-as-a-service (RaaS) operation. REvil abruptly went offline on July 13 after one of its affiliates attacked Kaseya VSA Remote Monitoring and Management (RMM) software and cascaded ransomware out to Kaseya's customers. However, operations resumed in early September. The October shutdown so far appears to be holding, but this should not be a cause for complacency.

U.S. Federal Bureau of Investigation (FBI) Deputy Director Paul Abbate said in September that there is "no indication" that Russia is doing anything to stop ransomware attacks against U.S. organizations despite President Biden putting pressure on Russia's President Putin earlier in 2021. Ransomware groups and their affiliates operate freely within many of the former Soviet states, particularly Russia. Ukraine is the major exception. It participated in a multi-country operation at the end of October against a RaaS affiliate group that conducted multiple operations involving malware such as LockerGoga, MegaCortex, and Dharma. This affiliate allegedly carried out attacks on over 1,800 victims in 71 countries.

The general unwillingness of Russia and its satellite countries to assist international law enforcement has likely hampered investigations. Russia has demonstrated its ability to take swift and decisive action. In September, the partially government-owned Rostelecom long-distance telephone provider sinkholed parts of the Meris distributed denial of service (DDoS) botnet. This botnet had been used in a large-scale attack against Russian web giant Yandex.

CTU researchers expect more disruptive activity against ransomware operators, such as infrastructure takedowns and asset seizures, directed by the U.S. and its allies. However, ransomware groups have proven their ability to adapt. At least nine new groups added victims to leak sites for the first time in September and October. Established groups also remain highly active. Organizations must protect themselves as ransomware groups continue to adapt and promote their criminal interests.

If you do just one thing after reading this:
Practice vigilance and maintain good security hygiene. Despite law enforcement successes, the threat posed by ransomware attackers is not decreasing.

Conclusion

The attacks that lead to ransomware deployment involve multiple stages and many tools. Comprehensive monitoring for the presence of precursor malware like Qakbot and offensive frameworks like Cobalt Strike is an essential part of protecting against ransomware attacks. While law enforcement agencies are winning battles against ransomware, the war is by no means over. Organizations cannot afford to let their vigilance or security stance slip.

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 protects organizations in the digitally connected world. We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086

Japan
Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

If you need immediate assistance, call our 24x7 **Global Incident Response Hotline:**

+1-770-870-6343

