Secureworks®

Threat Intelligence Executive Report

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

- Cybercriminal group uses DDoS attacks to extort businesses
- Microsoft TrickBot takedown leverages legal action
- U.S. puts pressure on hostile APT groups

Cybercriminal group uses DDoS attacks to extort businesses

The threat actors are not who they claim to be

On August 28, 2020, the U.S. Federal Bureau of Investigation (FBI) published a report describing distributed denial of service (DDoS) attacks against thousands of global organizations. The attacks were followed by emails threatening a second, much larger attack if a ransom was not paid. The sender claimed to be a member of the Russian government-sponsored Fancy Bear threat group, which CTU researchers track as IRON TWILIGHT. Similar activity occurred in 2017 and 2019, likely from the same threat actor.

The initial DDoS attacks typically lasted between 20 and 90 minutes and were targeted to cause disruption to the victims' systems. A focused attack is often more effective than one that relies exclusively on size. These attacks also had large traffic volumes of 20 to 180 GB per second. This size can cause problems for most organizations that do not have mitigating DDoS controls in place.

The follow-up email demanded a Bitcoin (BTC) ransom with an approximate value of $300,000 USD to be paid within six days from the attack. If payment was not received, the threat actors threatened to increase the ransom and unleash a second larger sustained DDoS attack. In the vast majority of cases, there was no second attack. However, the small number of second attacks that occurred were sustained, reasonably large, and well-targeted, indicating that organizations cannot ignore this threat.

These threat actors are not members of Fancy Bear, Lazarus Group, or any of the other advanced persistent threat (APT) groups they claim to represent. CTU researchers attribute the activity to the financially motivated GOLD FLANDERS threat group.

Key Takeaway

Organizations that experience these attacks are not being targeted by a hostile government-sponsored threat group. Because there have been a few follow-up attacks, organizations must consider whether to accept the risk or implement DDoS mitigation. The most efficient defense against DDoS attacks is to implement mitigation measures in advance. Organizations that consider DDoS a threat to their business should work with their network provider to protect the availability of business-critical data.

Microsoft TrickBot takedown leverages legal action

Botnet is reconstituted, but a return to full strength may be delayed

TrickBot is a versatile and modular malware family that the GOLD BLACKBURN cybercrime threat group has distributed since August 2016. This threat group is well-versed in all aspects of malware development and botnet operation to perpetrate financial fraud and extortion. TrickBot's affiliate business model leases its centrally operated botnet to other cybercrime threat groups, magnifying its global financial damage.

In late September 2020, CTU researchers observed several cyberattacks to disrupt the operation of the TrickBot botnet. On October 9, the Washington Post reported that U.S. Cyber Command had orchestrated a large and significant TrickBot takedown. On October 12, Microsoft and a coalition of industry partners announced a separate legal action against TrickBot in U.S. courts. The similar timing suggests there may have been coordination between the government and industry groups. In an October 20 update, Microsoft announced that it had taken down 120 of the 128 servers it identified as TrickBot infrastructure around the world.

GOLD BLACKBURN's response to the U.S Cyber Command action was to deploy TrickBot samples using a different set of command and control (C2) servers. The outcome was a separate and independently functioning botnet segment. After Microsoft's action, the threat group continued rebuilding its botnet using the new segment.

Key Takeaway

By early November 2020, the original TrickBot botnet appeared to be abandoned. Activity on the new botnet segment decreased, suggesting a possible strategic withdrawal. CTU researchers have observed a corresponding increase in use of BazarLoader malware that is also attributed to GOLD BLACKBURN.

The size of the TrickBot botnet has historically fluctuated. The malware's automated lateral movement capabilities made it a primary infection vector for the Ryuk and 777 ransomware. As of this publication, TrickBot likely remains a long-term and prominent threat to all organizations despite the takedown efforts. Organizations can protect their networks by implementing appropriate security controls and countermeasures. In addition, the success of Microsoft's legal strategy could prompt other companies to adopt a similar approach for future botnet takedowns.

U.S. puts pressure on hostile APT groups

A series of alerts expose APT activity prior to U.S. elections

During September and October 2020, multiple U.S. government agencies, including the Department of the Treasury, the Department of Justice (DOJ), the FBI, and the Cybersecurity and Infrastructure Security Agency (CISA) issued an unusually high number of alerts and sanctions related to hostile activity from government-sponsored threat actors. The number of government actions during this two-month timeframe exceeded the amount during a typical year.

For example, the Treasury sanctioned a Russian research institute connected with the Triton malware. The DOJ charged six Russian GRU military intelligence officers in connection with attacks that involved destructive malware. Other actions covered hostile activity from every major Russian government-sponsored group. Five members of the Chinese BRONZE ATLAS (also known as APT41) APT group were charged in connection with computer intrusions. The FBI and CISA jointly warned that Iranian APT actors had obtained voter registration data. Domain names used by Iran's Islamic Revolutionary Guard Corps (IRGC) were seized. In September, the DOJ unveiled charges against Iranian threat actors.

These actions were a clear response to hostile APT activity and a warning prior to the U.S. presidential election. The Chinese BRONZE VINEWOOD and Iranian COBALT ILLUSION threat groups reportedly targeted U.S. election campaigns earlier in 2020, likely to influence and interfere in the elections and undermine public confidence in the U.S. electoral process.

Government-sponsored APT activity is not limited to U.S. presidential election years. These threat actors consistently target organizations in multiple sectors to collect bulk personal information, intellectual property, and intelligence that aligns with their national priorities. Coronavirus-related research has been a highly desirable cyberespionage target in 2020. Malicious activity patterns also reflect specific periods of heightened geopolitical tensions between the U.S. and other nations.

Key Takeaway

The increased number of threat group reports by the U.S. intelligence community and the actions of the DOJ are a collective signal to hostile government-sponsored threat actors that the U.S. has the capability to track and identify their activity and the inclination to publish some of their findings. The increase appears to mark a change in the risk calculations made by the U.S. government, shifting to a perception that limited disclosure does not affect the government's ability to monitor threat group activity. However, this shift does not necessarily indicate a change in strategy.

Despite these disclosures and actions, hostile government-sponsored threat groups will continue to operate largely unimpeded from their respective countries. Organizations should review the published information about these groups to understand the threat landscape and devise a cybersecurity strategy to mitigate APT activities.

Conclusion

The degree of risk arising from specific threat activities and actors can fluctuate over time for multiple reasons. A lull in activity may be temporary, and threat actors are often motivated to regroup and return. Organizations should maintain close attention to the threat landscape so they can assess and respond to sudden changes in a timely fashion.

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

