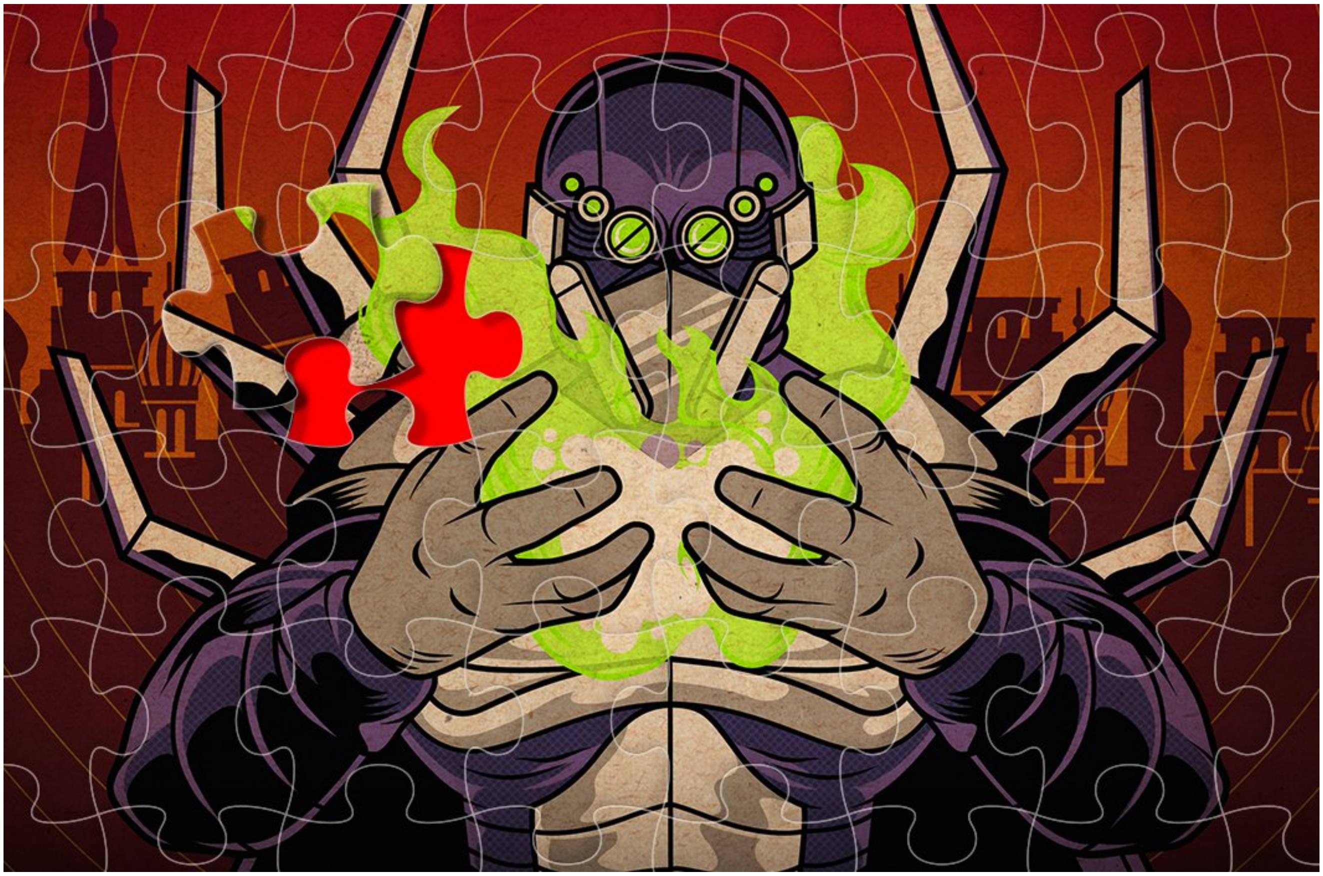
Wizard Spider Modifies and Expands Toolset [Adversary Update]

crowdstrike.com/blog/wizard-spider-adversary-update/

The CrowdStrike Intel Team

October 16, 2020



WIZARD SPIDER is an established, high-profile and sophisticated eCrime group, originally known for the creation and operation of the *TrickBot* banking malware. This Russia-based eCrime group originally began deploying TrickBot for the purpose of conducting financial fraud in 2016, but has since evolved into a highly capable group with a diverse and potent arsenal, including *Ryuk, Conti* and *BazarLoader.* Their toolset covers the entirety of the kill chain, from delivery to post-exploitation tools and big game hunting (BGH) ransomware, enabling them to conduct a wide range of criminal activities against enterprise environments.

WIZARD SPIDER has developed their tools over a number of years, and they continue to evolve the tactics, techniques and procedures (TTPs) needed to monetize their criminal operations in an efficient and effective manner.

Over recent months, WIZARD SPIDER has demonstrated their resilience and dedication to criminal operations by operating multiple ransomware families with differing modi operandi, using TrickBot and BazarLoader to infiltrate victim environments and reacting to attempts to stop them in their tracks. The group has made significant improvements to their arsenal recently and has both developed new tools and modified existing ones. The key observations covered below are based on CrowdStrike® Intelligence analysis of BazarLoader, Conti and Ryuk operations.

TrickBot

TrickBot has remained a primary tool for WIZARD SPIDER and has grown to infect upward of one million systems worldwide. TrickBot has played an integral part in enabling BGH operations and poses a severe threat across all sectors and geographies. This has made WIZARD SPIDER's TrickBot malware an extremely prevalent and widely tracked target.

On September 21 and 22, 2020, CrowdStrike Intelligence observed a non-standard configuration file being distributed to victims infected with TrickBot. The configuration files instructed infected hosts to communicate with the command-and-control (C2) server address `0.0.0.1` on TCP port `1`. This action resulted in an unknown number of bots being isolated from the TrickBot network and unreachable through the standard C2 channel.

This week, widespread public reporting has attributed this disruption attempt against TrickBot to multiple cybersecurity vendors. The operation against the TrickBot network was orchestrated to take down the botnet, thus reducing BGH infections by WIZARD SPIDER's Ryuk and Conti ransomware families, with an ultimate goal of protecting the forthcoming U.S. elections from ransomware operations.

Since the disruption operation began on September 21, 2020, we have observed a definite impact on the TrickBot network, with almost 10,000 unique downloads of the non-standard configuration identified. However, in spite of this, TrickBot activity has returned to its usual rapid pace, and the impact of the disruption operation was manifested as a short-term setback for WIZARD SPIDER.

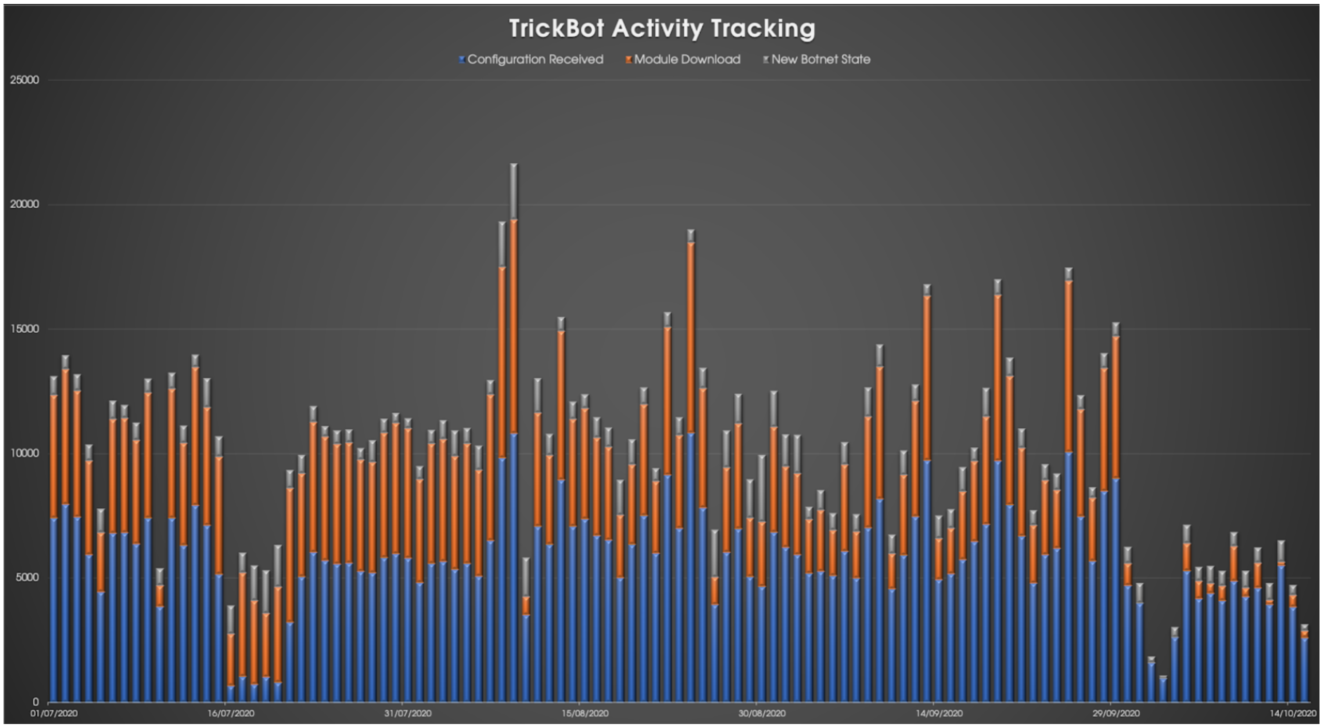
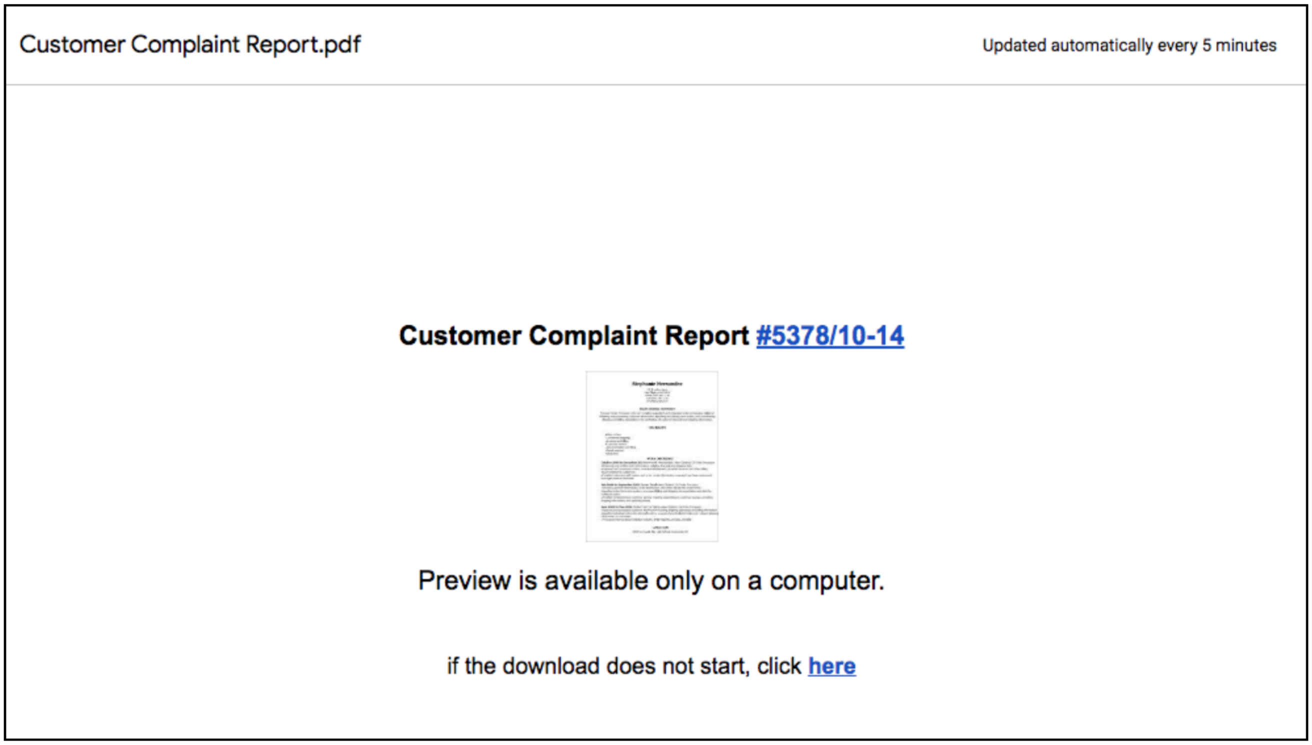


Figure 1. TrickBot Activity Tracking (July 1 to October 14, 2020) (click image to enlarge)

In a timely turn of events following a short break, MUMMY SPIDER's *Emotet* malware has resumed spamming activity this week, and we have since observed MUMMY SPIDER deploying TrickBot to Emotet-infected hosts. Downloaded TrickBot samples since October 14 have used group tags prefixed with `mor` — for example, `mor131` . This is very likely an attempt by TrickBot to replenish their victim base to offset any losses they may have experienced as a result of the takedown attempt.

BazarLoader Takes to the Stage

In addition to the continuation of TrickBot activity, WIZARD SPIDER has increased their use of the initial access tool BazarLoader, which is now being distributed in spam operations and used as an additional infection vector to enable WIZARD SPIDER's post-exploitation activity. Newly identified BazarLoader spam runs consist of emails containing a link to a Google Docs file (Figure 2). The Google Docs file commonly contains a link to the BazarLoader payload hosted on an external site.



Customer Complaint Report.pdf

Updated automatically every 5 minutes

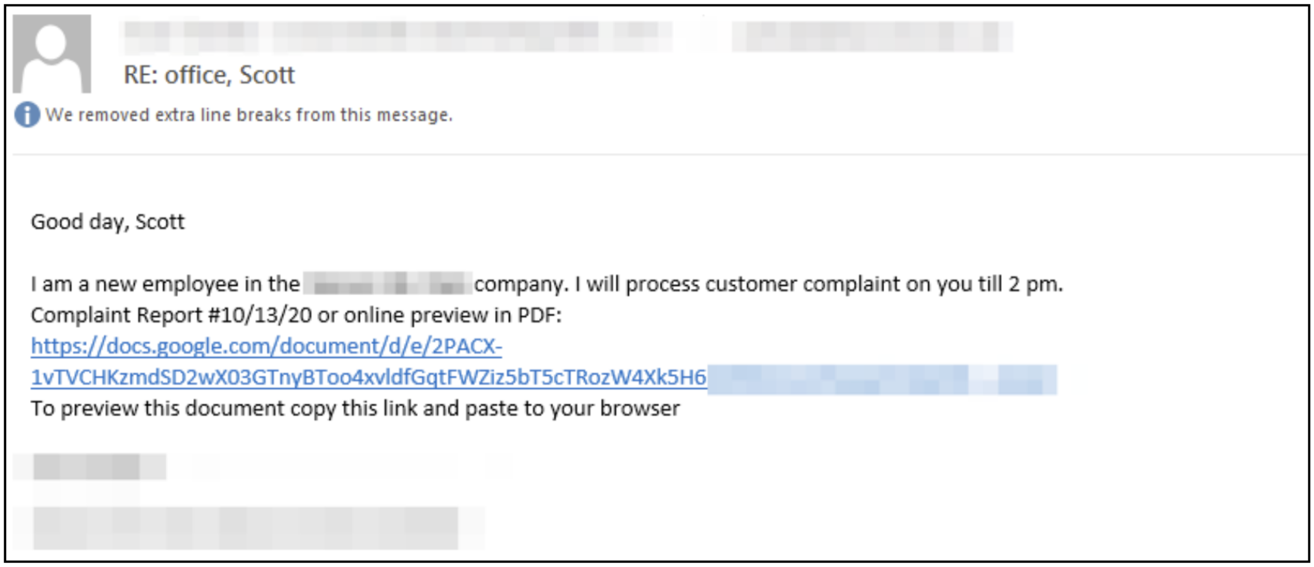
Customer Complaint Report #5378/10-14

Preview is available only on a computer.

if the download does not start, click here

Figure 2. Example BazarLoader Google Docs File (click image to enlarge)

The spam emails are often business-related, with themes that reference purported phone calls, meetings, customer complaints or employment termination. An example email is provided in Figure 3.



[redacted]

RE: office, Scott

ⓘ We removed extra line breaks from this message.

Good day, Scott

I am a new employee in the [redacted] company. I will process customer complaint on you till 2 pm.
Complaint Report #10/13/20 or online preview in PDF:
https://docs.google.com/document/d/e/2PACX-1vTVCHKzmdSD2wX03GTnyBToo4xvldfGqtFWZiz5bT5cTRozW4Xk5H6[redacted]
To preview this document copy this link and paste to your browser

[redacted]

Figure 3. BazarLoader Spam Email with Google Docs Link (click image to enlarge)

BazarLoader (aka *Kegtap*) consists of a loader and a backdoor component. The loader is responsible for installing and executing the backdoor element. The latest version of the loader contains a large amount of string and code obfuscation, and it has been observed utilizing a novel technique of mimicking legitimate software for persistence. CrowdStrike technical analysis has specifically revealed the loader mimicking communications software such as Softphone.

The backdoor component is capable of executing arbitrary payloads, batch and PowerShell scripts, exfiltrating files from a victim, and terminating running processes. In addition to the backdoor component, we have observed WIZARD SPIDER deploying and utilizing the *CobaltStrike* post-exploitation framework.

In September 2020, the group distributed a PowerShell version of BazarLoader that contains similar functionality to that of the executable version and is likely a pursuit to be compatible with their extensive, PowerShell-friendly toolset.

Ryuk's Return

Since September 2018, WIZARD SPIDER's Ryuk ransomware has been the group's most lucrative operation for siphoning money from its victims through extortion. The U.S. Federal Bureau of Investigation (FBI) has estimated that victims have paid over USD $61 million to recover files encrypted by Ryuk. In March 2020, WIZARD SPIDER ceased deploying Ryuk until mid-September.

From March to September 2020, WIZARD SPIDER did not cease operating but instead switched to Conti ransomware. We first observed Conti being deployed in June 2020. It is unknown why WIZARD SPIDER paused operating Ryuk, but it is likely they took a break from their operations to reorganize and reevaluate their methodologies. It is also currently unclear how WIZARD SPIDER intends to use both Conti and Ryuk. It is possible that Conti and Ryuk may continue to be used simultaneously by WIZARD SPIDER, with either one being deployed depending on particular characteristics of the victim organization. What is clear is that WIZARD SPIDER is now running multiple ransomware operations.

From a code perspective, little has changed between Ryuk binaries compiled in March and those compiled in September. The functionality has remained overall static since introducing features for targeting hosts on a local area network (LAN). The most notable change to Ryuk is the introduction of code obfuscation. The code obfuscations appear to be designed to slow down the reverse engineering process by using anti-disassembly and code transformation obfuscation techniques.

These obfuscation techniques are not as advanced as those observed in Conti and BazarLoader. This is likely due to the age of the Ryuk code base and build process, which dates back to the end of 2018. Conti and BazarLoader are newer WIZARD SPIDER projects with obfuscation likely part of the build process. Ryuk's code obfuscation appears to be macro-based, with macros inserted at the start of a function or in-line.

Conti: New, Developing, Persistent

WIZARD SPIDER operations were notably reduced and sporadic during the first half of 2020, but recent months have seen a resurgence of WIZARD SPIDER activity and the introduction of Conti ransomware. In August 2020, the actor began using a data leak site (DLS) for Conti. Conti has been continually improved by WIZARD SPIDER and has already been used to compromise over 120 victim networks, with stolen data listed on the Conti DLS. Conti victims span multiple sectors and geographies, the vast majority of which are based in North America and Europe (Figure 4). This opportunistic targeting is indicative of WIZARD SPIDER and wider ransomware operations.

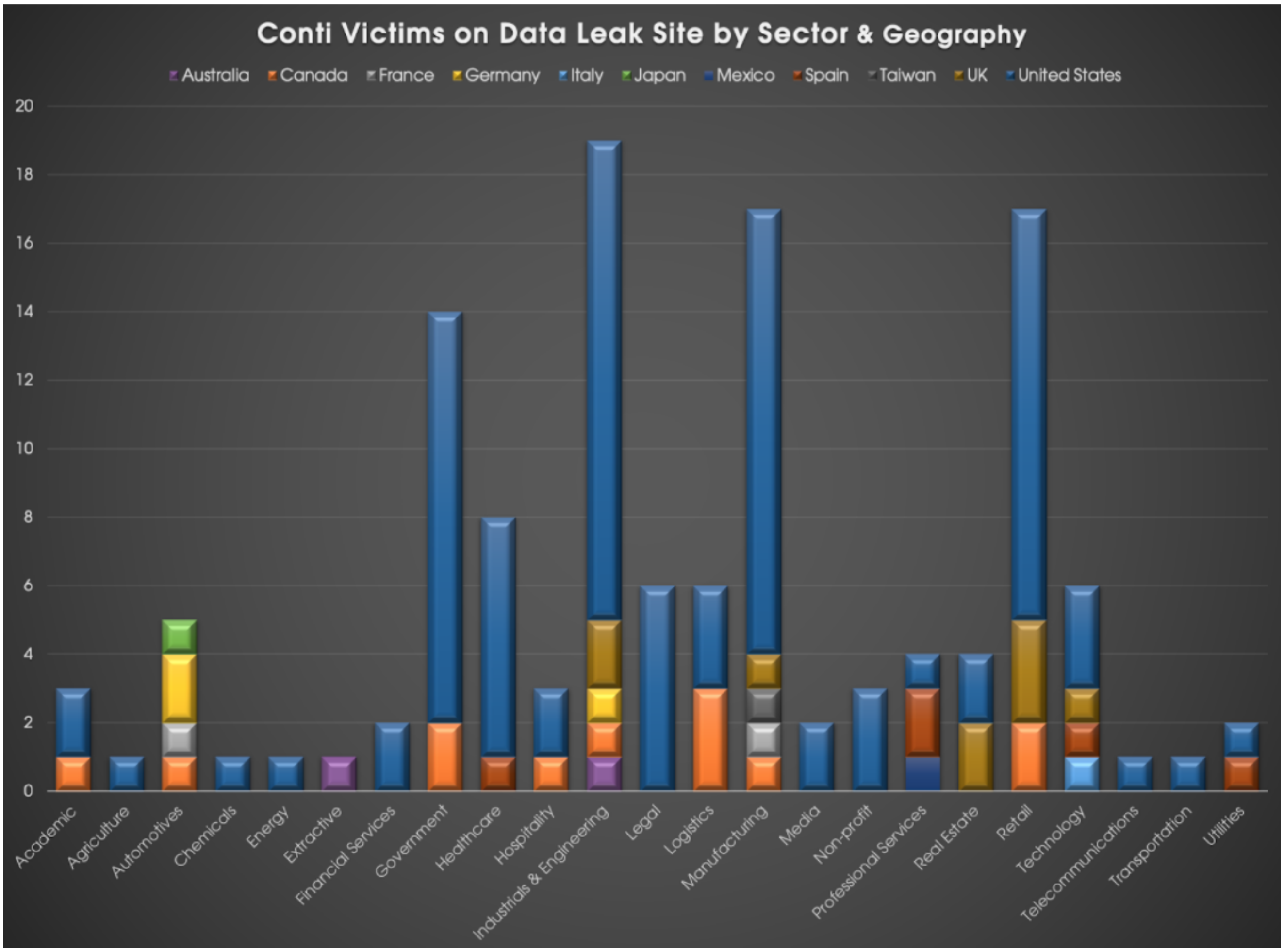


Figure 4. Conti Ransomware Victims by Sector and Geography (click image to enlarge)

Conti has been under active development throughout WIZARD SPIDER's deployment of the ransomware in BGH campaigns. Additional features, obfuscation techniques and code changes are integrated on an almost weekly basis. In August 2020, Conti's technique shifted from fully encrypting files with AES-256 to a more strategic and efficient approach of selectively encrypting files with the ChaCha stream cipher. Conti's host discovery and network share targeting functionality has also continued to evolve and is now comparable to that of Ryuk's.

WIZARD SPIDER’s ongoing development of Conti is equally focused on the evasion of traditional, signature-based antivirus software and to hinder malware analysis efforts. Conti’s utilization of compiler-based obfuscation techniques, such as *ADVobfuscator*, provide code obfuscation when the ransomware’s source code is built. Portions of Conti’s source code are restructured or rewritten regularly with the intention of avoiding detection and disrupting automated malware analysis systems.

Outlook

The ultimate goal of the disruption operation against the TrickBot network was to impact and prevent ransomware infections — however, Ryuk and Conti continue to be used in BGH campaigns against organizations across multiple sectors and geographies. Over a dozen confirmed WIZARD SPIDER ransomware cases have been identified since the disruption began. While the valiant efforts of the cybersecurity teams involved in this complex operation undoubtedly had a short-term impact on WIZARD SPIDER’s TrickBot network, the response by the criminal actors has been swift, effective and efficient. TrickBot activity continues at a progressive rate, BazarLoader is increasing in prevalence, and BGH ransomware operations proceed as normal with Ryuk and Conti.

WIZARD SPIDER, with its diverse and effective toolset, has proven to be a highly capable adversary and continues to be resilient, reactive and resolute as they continue to run their formidable criminal enterprise. The resilience of advanced criminal threat actors like WIZARD SPIDER make it increasingly important that we, as an industry, continue to fight back. Any attempt to increase the cost for the criminals contributes to a more secure cyberspace.

The CrowdStrike Falcon® endpoint protection platform detects and prevents against Ryuk. For Falcon endpoint customers, prevention settings should be set at a minimum to the following:

- Next-Gen Antivirus: Cloud/Sensor Machine Learning: Set “Prevention” slider to “Aggressive”
- Malware Protection: Execution Blocking: Toggle “Prevent Suspicious Processes” to “Enabled”
- Add any hashes to your custom blocklist for added protection

This blog was written by CrowdStrike Intelligence analysts Adam Podlosky, Alexander Hanel, Brendon Feeley and Sean Wilson.

Additional Resources

- *Download: CrowdStrike 2020 Global Threat Report.*
- *To learn more about how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Threat Intelligence page.*

- *Learn more about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*