CYBERSECURITY DIVE

Ryuk wakes from hibernation; FBI, DHS warn of healthcare attacks

Researchers found that threat group UNC1878 is responsible for one-fifth of Ryuk intrusions. “Herein lies our monster,” said Mandiant’s Aaron Stephens.

Published Oct. 29, 2020

Samantha Schwartz
Reporter

Stock Photo via Getty Images

Ryuk ransomware fell off the radar when the coronavirus began its global spread. Its silence hinted at its expiration or a rebrand in the form of the Conti ransomware.

Really, Ryuk was just in hibernation between April and August.

On a call with the FBI, Department of Homeland Security and Department of Health and Human Services, the agencies warned the healthcare industry of a potential ransomware attack. ”CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers,” the alert said.

The expected onslaught of Ryuk ransomware could reach up to 400 hospitals, Alex Holden, CEO of Hold Security, told cybersecurity journalist Brian Krebs.

“Maybe Ryuk’s time had come and gone. Obviously, we were really, really wrong,” said Aaron Stephens, senior threat analyst on

Mandiant's FLARE Advanced Practices Team, while speaking during a SANS Institute webcast Wednesday.

Mandiant found that threat group UNC1878 is responsible for one-fifth of Ryuk intrusions. "Herein lies our monster," said Stephens during the webcast. The cybersecurity firm released research on UNC1878's indicators Wednesday following news of attacks on hospitals.

Mandiant researchers coined "UNC," shorthand for uncategorized, as part of their research processes, they needed "UNCs" to help organize unique malicious activity.

"At a fundamental level UNCs serve as labels for which you can bucket indicators and techniques into. This labeled bucket would then act as technical anchor for what we are seeing is related activity," said Van Ta, senior threat analyst on Mandiant's FLARE Advanced Practices Team, speaking on the webcast. "Instead of labeling an evidence bag, 'the Overlook Hotel', we're labeling it UNC1878."

> **"We began to see Ryuk make its harrowing return. It wasn't dead. It was undead."**
>
> Aaron Stephens
> *senior threat analyst on Mandiant's FLARE Advanced Practices Team*

When enough UNCs are identified, researchers can cross section overlaps or see where UNCs graduate into different classifications, or threat groups. UNC1878 was created in January and within two months Mandiant picked up UNC1878's "formative years," where it developed its strategies, said Ta.

In September, “we began to see Ryuk make its harrowing return. It wasn’t dead. It was undead,” Stephens said.

The actors behind Ryuk are credited with collecting more than $61 million between February 2018 and October 2019, according to the FBI, making it one of the most profitable strains. Retirement didn’t seem likely.

Ryuk-related incidents increased from 5,123 in Q3 2019 to 67.3 million in Q3 2020, according to research from SonicWall Capture Labs. The company relied on more than 1 million global sensors to collect cyberattack data through September.

Ryuk reportedly targeted Universal Health Services (UHS) in September and French IT services firm Sopra Steria earlier this month. Last week, furniture manufacturer Steelcase disclosed a cyberattack on its IT systems in an SEC filing. Sources told Bleeping Computer Ryuk was behind the attack.

Steelcase “implemented a series of containment measures to address this situation,” including system and operational shutdowns, to mitigate the attack. “Although cyberattacks can be unpredictable, the company does not currently expect this incident will have a material impact on its business operations or its financial results,” Steelcase said.

UNC1878’s Ryuk gameplan

UNC1878 traditionally relied on Trickbot, which provides initial access and visibility, and used Cobalt Strike with everyone of its intrusions. UNC1878 obtains credentials using Mimikatz, LaZagne and Kerbrute.

“With legitimate credentials UNC1878 extended their access by connecting to network shares and directly to systems over RDP

and SSH," said Ta.

This month, Microsoft was granted permission to disable Trickbot's critical infrastructure. A week into the disruption, Microsoft claimed to have eliminated "94% of Trickbot's critical operational infrastructure including both the command-and-control servers in use at the time our action began and new infrastructure Trickbot has attempted to bring online."

However, Microsoft acknowledged the maturity of Trickbot and impending threats, saying "this is challenging work, and there is not always a straight line to success."

Ryuk typically uses Emotet for a phishing or RDP attack, but Sophos studied a September Ryuk attack which showcased a different tactic outside of Emotet and Trickbot. "It marked the return of Ryuk with some minor modifications" and next-generation attack tools, according to Sophos' report.

"People think ransomware, and the malware cocktails, they're just re-flavoring. But if you look at Ryuk, they're using it as a malware cocktail, not just changing the ingredients," said Bill Conner, CEO of SonicWall.

In the September attack Sophos investigated, the malicious document in the phishing email executed Buer Loader, a modular malware as a service downloader, to get access.

Time to Ryuk

The September Ryuk incident Sophos investigated uncovered a quick infection-to-deployment time after someone opened the phishing email. It took 3 1/2 hours. While each installment attempt failed, Ryuk's operators persevered, "including renewed phishing attempts to re-establish a foothold," according to

Sophos.

Operators behind Ryuk are “really recreating these malware cocktails and bundles, if you will, to make them much more lethal,” which increases their speed and scalability, said Conner.

UNC1878’s “time to Ryuk,” or intrusion to execution time, was on average about five days and 17 hours. It is demonstrably faster than other ransomware’s “dwell time,” roughly 72 days and 12 hours, according to data from 2019. UNC1878 could “ransom 13 environments in the same amount of time,” said Stephens.

When UNC1878 is ready to deploy Ryuk, it will drop the zip file into the PerfLogs directory. “They’ll then unzip into a directory they create named “share$,” said Ta. Coupled with text files are the ransomware binary and patch files for malware propagation. There are three ”.bat” scripts used for iterating computer names to execute Ryuk.

At the beginning of the year, UNC1878 used Trickbot, Cobalt Strike and Ryuk. But Ryuk’s return doesn’t necessarily mean UNC1878 returned too.

“This new wave of Ryuk intrusions have essentially replaced Trickbot with Kegtap, a similar but distinctly different malware family,” said Stephens. Kegtap is among campaigns sent to targets with ever-changing ”delivery tactics, techniques and procedures,” according to Mandiant. Campaigns like Kegtap have shifted from delivery via Sendgrid to having URLs host malware payload “associated with one or more of these legitimate services.”

Even the use of Cobalt Strike isn’t the same as it once was, particularly seen in TLS certificates.

Mandiant noticed differentiation in certificates, nuances in domain patterns, and general overlaps in activity. Researchers identified a

newly-minted UNC2352 as the successor to UNC1878. “If these two groups should really be the same, the data will tell us and in this case, it did,” said Stephens.