Ryuk explained: Targeted, devastatingly effective ransomware

By by Lucian Constantin CSO Senior Writer

Published: 2021-03-19 · Archived: 2026-04-05 18:48:56 UTC

Ryuk ransomware attacks are targeted to the most vulnerable, most likely to pay companies and are often paired with other malware such as TrickBot.

What is Ryuk?

Ryuk is a sophisticated ransomware threat that has been targeting businesses, hospitals, government institutions and other organizations since 2018. The group behind the malware is known for using manual hacking techniques and open-source tools to move laterally through private networks and gain administrative access to as many systems as possible before initiating the file encryption.

Ryuk's history and success

Ryuk first appeared in August 2018 but is based on an older ransomware program called Hermes that was sold on underground cybercrime forums in 2017. Hermes was used by the North Korean state-sponsored Lazarus Group in an attack against the Taiwanese Far Eastern International Bank (FEIB) in October 2017, which led to reports that Hermes, and later Ryuk, were created by North Korean hackers.

Several security companies later disproved those claims and Ryuk is now generally believed to be the creation of a Russian-speaking cybercriminal group that obtained access to Hermes, just like Lazarus likely did. The Ryuk gang is tracked by some security companies as Wizard Spider or Grim Spider and is the same group that operates TrickBot, a much older and active credential theft Trojan program that has a relationship with Ryuk. Other researchers believe that Ryuk could be the creation of the original Hermes author or authors operating under the handle CryptoTech, who simply stopped selling their ransomware publicly after developing an improved version.

The Ryuk attackers demand higher ransom payments from their victims compared to many other ransomware gangs. The ransom amounts associated with Ryuk typically range between 15 and 50 Bitcoins, or roughly between $100,000 and $500,000, although higher payments have reportedly been paid. Because the attackers go after organizations with critical assets that are more likely to pay, a technique the security industry calls "big game hunting," the Ryuk gang is very successful at monetizing their campaigns.

In a presentation at the RSA Conference 2020, Joel DeCapua, a supervisory special agent with the FBI's Global Operations and Targeting Unit, revealed that organizations paid $144.35 million in bitcoin to ransomware groups between 2013 and 2019. The data doesn't include ransom payments in cryptocurrencies other than BTC. Of those payments, $61.26 million were sent to the Ryuk gang and the sum is almost three times larger than what Crysis/Dharma, the second most successful ransomware gang on DeCapua's list, managed to extract from victims in three years of operation.

Ryuk distribution and attack chain

Ryuk is almost exclusively distributed through TrickBot or follows an infection with the Trojan. However, not all TrickBot infections lead to Ryuk. When they do, the deployment of Ryuk happens weeks after TrickBot first shows up on a network. This is likely because attackers use the data collected by TrickBot to identify potentially valuable networks for Ryuk.

The target selection is followed by manual hacking activities that involve network reconnaissance and lateral movement with the goal of compromising domain controllers and gaining access to as many systems as possible. This ensures that when Ryuk is deployed, the damage is swift and widespread across the network, which is more likely to force an organization's hand than holding just a few of its endpoints hostage.

Microsoft refers to Ryuk as a human-operated ransomware attack, and it's part of a larger trend of ransomware gangs adopting highly targeted and stealthy techniques that were primarily associated with advanced persistent threat (APT) groups in the past. This includes relying on open-source tools and existing system administration utilities to evade detection, a technique known as living off the land.

Following a TrickBot infection and the identification of an interesting target, the Ryuk gang deploys post-exploitation frameworks such as Cobalt Strike or PowerShell Empire that allow them to perform malicious actions on computers without triggering security alerts. PowerShell is a scripting language meant for system administration that leverages the Windows Management Instrumentation (WMI) API and is enabled by default on Windows computers. Its powerful features and widespread availability on computers have made it a popular choice for hackers to abuse.

The Ryuk attackers also use the open-source LaZagne tool to steal credentials stored on compromised computers and BloodHound, a tool that allows penetration testers to analyze and reveal potentially exploitable relationships that exist in Active Directory environments. The end goal of the Ryuk attackers is to identify domain controllers and gain administrative access to them, which then gives them power over the entire network.

"In our investigations, we found that [Ryuk] activation occurs on TrickBot implants of varying ages, indicating that the human operators behind Ryuk likely have some sort of list of check-ins and targets for deployment of the ransomware," Microsoft researchers said in an analysis of human-operated ransomware attacks. "In many cases, however, this activation phase comes well after the initial TrickBot infection, and the eventual deployment of a ransomware payload may happen weeks or even months after the initial infection."

TrickBot itself remains one of the most prevalent Trojans and is distributed through malicious spam emails but is also delivered by another widespread Trojan program called Emotet. While the relationships between Ryuk, TrickBot and Emotet are not completely clear, over the years Emotet evolved into a malware distribution platform that's used by many cybercriminal groups. TrickBot is believed to follow a similar malware-as-a-service (MaaS) model, but is only available to a relatively small number of top-tier cybercriminals, according to a recent report by cybercrime intelligence firm Intel 471.

The US Cybersecurity and Infrastructure Security Agency (CISA) issued an alert about an increase in targeted Emotet malware attacks. The agency has maintained an advisory about Emotet since 2018, including a set of recommendations for protecting against the threat.

The group behind Ryuk used to deploy the final ransomware payload manually, but according to a report from CERT-FR, a more recent Ryuk variant contains code that allows it to spread to other computers on the local network automatically once the attackers obtain a privileged account on the domain.

The program first generates a list with every possible IP address on the local network and then sends an ICMP ping to them to discover which are reachable. It then lists the file sharing resources available on the online machines, mounts those resources and encrypts their contents. At the same time, it copies itself to those file shares and uses the privileged domain account credentials to set up a scheduled task on the remote computers to execute the copied version of itself.

The code doesn't check if a computer has already been infected, so the malware keeps reinfecting systems. This cannot be stopped if the password for the compromised domain account is changed or if the account is disabled, as long as Kerberos tickets remain active. To stop the propagation, the password for the KRBTGT user account needs to be changed twice to force a password history clean. This action might create some disturbances on the domain that require systems to be rebooted, but would also stop the ransomware propagation, CERT-FR said in its report.

The Ryuk encryption routine

Ryuk has diverged over time from the original Hermes code base. Some features such as the anti-forensics or persistence mechanisms have been reimplemented, simplified or removed. After all, a ransomware program that's manually deployed inside an environment where attackers already have administrative control over systems does not need the same self-protection features as ransomware programs that rely on automated propagation. Ryuk is also not as selective in the files it encrypts as other ransomware.

Once deployed, Ryuk encrypts all files except for those with the extensions dll, lnk, hrmlog, ini and exe. It also skips files stored in the Windows System32, Chrome, Mozilla, Internet Explorer and Recycle Bin directories. These exclusion rules are likely meant to preserve system stability and allow the victim to use a browser to make payments.

Ryuk uses strong file encryption based on AES-256. The encryption keys are stored at the end of the encrypted files, which have their extension changed to .ryk. The AES keys are encrypted with a RSA-4096 public private key pair that is controlled by the attackers. The whole process is a bit more complex and involves several keys being encrypted with other keys, but the result is that each Ryuk executable is tailor-made for each specific victim — even if used on multiple systems — and uses a private key generated by the attackers for that specific victim. This means that even if the private RSA key associated with one victim is published, it can't be used to decrypt files belonging to other victims.

No publicly available tool can decrypt Ryuk files without paying the ransom, and researchers warn that even the decryptor provided by the Ryuk attackers to paying victims can sometimes corrupt files. That usually happens on larger files where Ryuk intentionally performs only a partial encryption to save time. Furthermore, despite the whitelisting of certain system files and directories, Ryuk can still encrypt files that are critical for the system's normal operation, which sometimes results in unbootable systems after they are restarted. All these issues can complicate the recovery efforts and increase the cost incurred by victims as a result of Ryuk attacks.

Like most ransomware programs, Ryuk attempts to delete volume shadow copies to prevent data recovery through alternative means. It also contains a kill.bat script that disables various services including network backups and Windows Defender antivirus.

Protecting against Ryuk

While organizations can put in place specific technical controls to reduce the likelihood of Ryuk infections, defending against human-operated ransomware attacks in general requires correcting some bad practices among IT administrators.

“Some of the most successful human-operated ransomware campaigns have been against servers that have antivirus software and other security intentionally disabled, which admins may do to improve performance,” Microsoft said. “Many of the observed attacks leverage malware and tools that are already detected by antivirus. The same servers also often lack firewall protection and MFA, have weak domain credentials, and use non-randomized local admin passwords. Oftentimes these protections are not deployed because there is a fear that security controls will disrupt operations or impact performance. IT pros can help with determining the true impact of these settings and collaborate with security teams on mitigations. Attackers are preying on settings and configurations that many IT admins manage and control. Given the key role they play, IT pros should be part of security teams.”

Security teams should also take what are seemingly rare and isolated infections with commodity malware much more seriously. As Ryuk demonstrates, common threats like Emotet and TrickBot rarely come alone and can be a sign of much deeper problems. Simply removing common malware from a system without performing further investigations can have disastrous consequences a few weeks later.

“Commodity malware infections like Emotet, Dridex and Trickbot should be remediated and treated as a potential full compromise of the system, including any credentials present on it,” Microsoft warned.

Addressing the infrastructure weaknesses that allowed the malware to get in and propagate in the first place is also critically important, as well as hardening the network against lateral movement by practicing good credential hygiene and enforcing least-privilege access. Restricting unnecessary SMB traffic between endpoints and limiting the use of administrative credentials can also have a big impact on making the network more resilient against human-operated attack campaigns. The Microsoft advisory contains additional technical recommendations.

Editor’s note: This article, originally published in May 2020, has been updated to include information on a new Ryuk variant discovered by CERT-FR.
