REvil, Ryuk and Tycoon Ransomware: How They Work and How to Defend Against Them

Archived: 2026-04-05 13:09:56 UTC

It is the Tuesday morning after a long weekend. You come into work early to get caught up on emails only to find you are completely locked out. You have been hit by a ransomware attack. You ask yourself, “What happened? And how do I fix it?”

This post will explore three of the most significant ransomware families of 2020: Tycoon, Ryuk and REvil. After discussing how these strains work, we’ll share some best practices that organizations can use to defend themselves against a ransomware infection.

Tycoon is compiled in the Java image format, ImageJ, and is deployed using a trojanized version of Java Runtime Environment (JRE). This is an odd methodology for ransomware that is not often seen. The Tycoon ransomware often uses an insecure connection to an RDP server as its way into the network. Once inside the network, it will disable anti-malware software so that it can remain undetected on the system until the attack is finished.

This crypto-malware strain has been around since December of 2019. Tycoon’s code is written to be used against both Windows and Linux systems and is used to target small- and medium-sized businesses (SMBs), primarily in the software and education industries. It is believed that Tycoon may be linked to Dharma (Crysis) due to similarities in the naming conventions and email addresses used.

According to TechRadar, Tycoon has a very limited number of victims due to its specified targets. In early versions of the Tycoon ransomware, some victims were able to recover their encrypted data with the use of an RSA key bought from other victims because the ransomware repeated the use of some keys. However, this is not the case with more recent versions.

Ryuk

Ryuk works in two parts. The first is a dropper that places Ryuk malware onto a system. The second is an executable payload that carries out the encryption. Part of the executable payload’s code is to delete the dropper from the system so that it cannot be retrieved and analyzed.

Unlike most other ransomware, Ryuk doesn’t have an extensive allow list to prevent it from encrypting system files that ensure the running stability of the systems. Ryuk only allows files with the exe, dll, and hrmlog extensions as well as a few folders such as Windows, Microsoft, and Chrome. The issue with this is that files that have the sys extension are not allowed, and if these files are encrypted, it could cause the system to become unstable and potentially crash.

The Ryuk ransomware has been around since August of 2018 and is operated by a Russian eCrime group who call themselves Wizard Spider. Wizard Spider’s sole targets for Ryuk have been large organizations that are capable of paying high ransom fees. This has made Ryuk one of the most profitable ransomware to date as according to

ZDNet, with the average ransom demand for Ryuk estimated at around $290,000. Ryuk ransomware is not an originally coded ransomware; instead, it is derived from the Hermes ransomware.

REvil

REvil, named after the Resident Evil franchise, is also known as Sodinokibi and is a Ransomware-as-a-Service (RaaS). It is distributed using several different methods including malicious spam emails, exploit kits and RDP vulnerabilities. This malware also adds a twist in its ransom note in that it tells the victim that if the ransom is not paid by the specified time, the demand will be doubled. The REvil gang even offers a "trial" decryption to prove to the victim that their files can be decrypted.

REvil was first identified in April of 2019 and is considered to be one of the most widespread ransomware families in 2020. Like many other crypto-malware families, REvil exfiltrates data and threatens to release it if the victim doesn't pay the ransom in time.

A member of the group behind REvil, who goes by the name "Unknown," has said that REvil is built upon an older codebase, most likely GandCrab. REvil is very configurable, allowing each user to modify the code to their end goal. According to Secureworks, malicious actors can use the ransomware to exploit CVE-2018-8453 to elevate privileges and exfiltrate host information.

Preventing a Ransomware Attack

For anyone looking to keep their network secure, you need to make sure that they KNOW their network. Knowing the network means that you have an inventory of every connected device and system as well as how the traffic flows between them. On top of that, the network needs to be constantly monitored, which can be made easier by utilizing Security Information and Event Management (SIEM) tools. Monitoring the network allows abnormalities to be discovered much more quickly, and it saves precious time during an incident to react and remediate the situation. It is also a strong recommendation to make traversing the network difficult for attackers in order to prevent the spread of any malware that may have found its way into your network.

Organizations also need to consider vulnerability management. Patches and updates to software and devices are created to fix any vulnerabilities that were discovered in those software and devices. One of the first things attackers look for is vulnerable systems, so if updates are neglected, it provides the attackers with an avenue to use those known vulnerabilities to gain access to your systems and carry out their malicious deeds.

You need to accept at some point that malware will find a way into the network or systems. It is not a matter of if but when. Keeping this fact in mind, it is important to create a response plan for when malware is found in the system or network so that when it happens, the response can be quick and efficient to limit the exposure and damage. Along with having a response plan, it is important to test the plan periodically so that all staff know what to do during an incident and to identify any updates to the plan that may be needed. Part of this plan should be to have up-to-date backups of the system and data so that in the case of a ransomware attack, there is little to no data loss, as it can be restored from the backups.

Organizations can't stop there. They also need to remember the importance of managing their secure configurations, blocking phishing attacks and other email-based operations as well as controlling the use of

administrative privileges. Click here to learn more.

About the Author: *Brett McFadden is a new entrant to the world of cyber security. With advanced diplomas in both Cyber Security (Fanshawe College) and Mohawk College (Television Broadcasting), he brings a unique insight to a world where streaming accounts for one fifth of all television viewing. Brett is currently a Cyber Security Analyst with Western University in London, Ontario and worked previously as a Cyber Security Analyst with Linamar corporation and as a Business System Analyst with TD Bank's Cloud Security and Data Protection team. Brett has spent time running internal mock phishing campaigns and ensuring that cloud migrations were compliant with industry standards. In his free time, Brett is an avid Twitch streamer and works toward his career goal of red teaming for either a large corporation or a penetration testing company.*

Editor's Note: *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*
