Cybereason vs. Ryuk Ransomware

cybereason.com/blog/cybereason-vs.-ryuk-ransomware

Written By
Cybereason Nocturnus

December 10, 2020 | 3 minute read

What is Ryuk Ransomware?

Ryuk ransomware has been infecting victims since around 2018, and is believed to be based on the source code of Hermes ransomware, which was sold on an internet hacking forum back in 2017. Since its inception, Ryuk has been used to target large organizations to great effect, having accumulated as much as $61.26 million (as of Feb 2020) in ransom payments according to federal investigations.

One of the reasons behind Ryuk's unfortunate success is the threat actor's capacity to evolve their tactics, techniques and procedures (TTPs). Since early last year, the TrickBot information stealer trojan has been a more or less constant partner-in-crime, with many campaigns also including other malware, frameworks and tools. The mentioned campaign utilized the EMPIRE framework, and in later campaigns the same year Cybereason observed Emotet downloading TrickBot deploying Ryuk.

In March of 2020, the threat actors temporarily stopped deploying Ryuk, and a new ransomware called Conti was introduced. Researchers found that the code bases were similar, implying this could be the successor to Ryuk. However, in September 2020 Ryuk made a swift return, and with Conti infections still happening alongside it, the evidence pointed to Conti not being a successor so much as a new, different strain of malware.

Shortly after the start of Ryuk's hiatus, a new malware called BazarLoader was observed being delivered by TrickBot. Currently, evidence suggests that Ryuk, Conti and BazarLoader are used by the same threat actor.

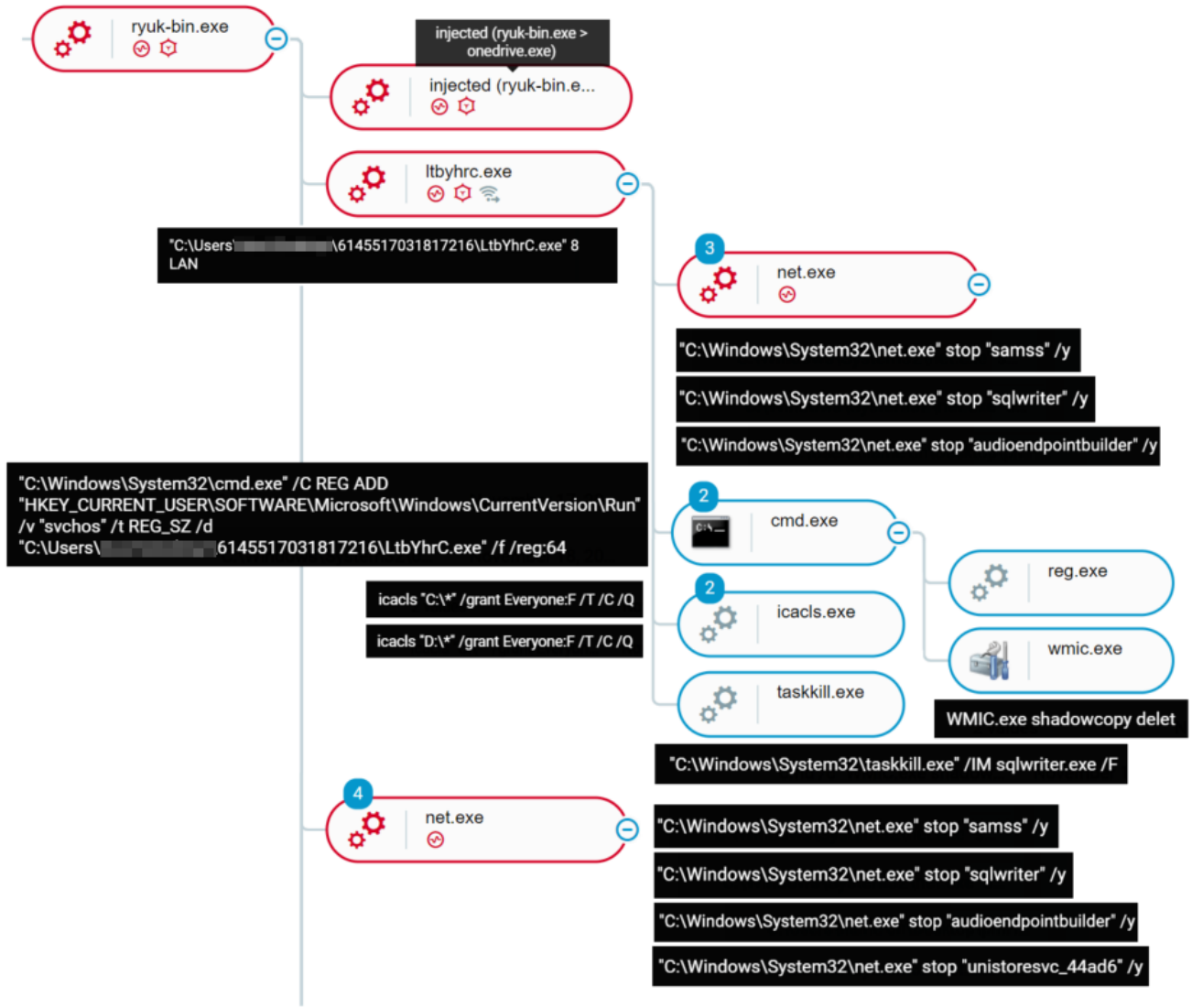
Ryuk ransomware is most often seen as the final payload in a larger targeted attack against a corporation, and since its return in September, it has been mainly via TrickBot or BazarLoader infections.

Cybereason Detects and Blocks Ryuk Ransomware

Cybereason detects the various execution phases of Ryuk in detail, including process injection, persistence creation and shadow copy deletion as detailed below in the *Execution Overview* section. With the proper settings applied to sensors in the customer environment, Cybereason can stop the Ryuk ransomware before it encrypts user files.

With Anti-Ransomware mode enabled, the Ryuk execution is stopped before encrypting the hard drive. A ransom note can be found in folders where the malware attempted to encrypt files, but the user's files were saved. If Anti-Malware is enabled the sample will be removed before execution. The following video provides a quick demonstration of Cybereason's detection and prevention capabilities against Ryuk ransomware:

Execution Overview



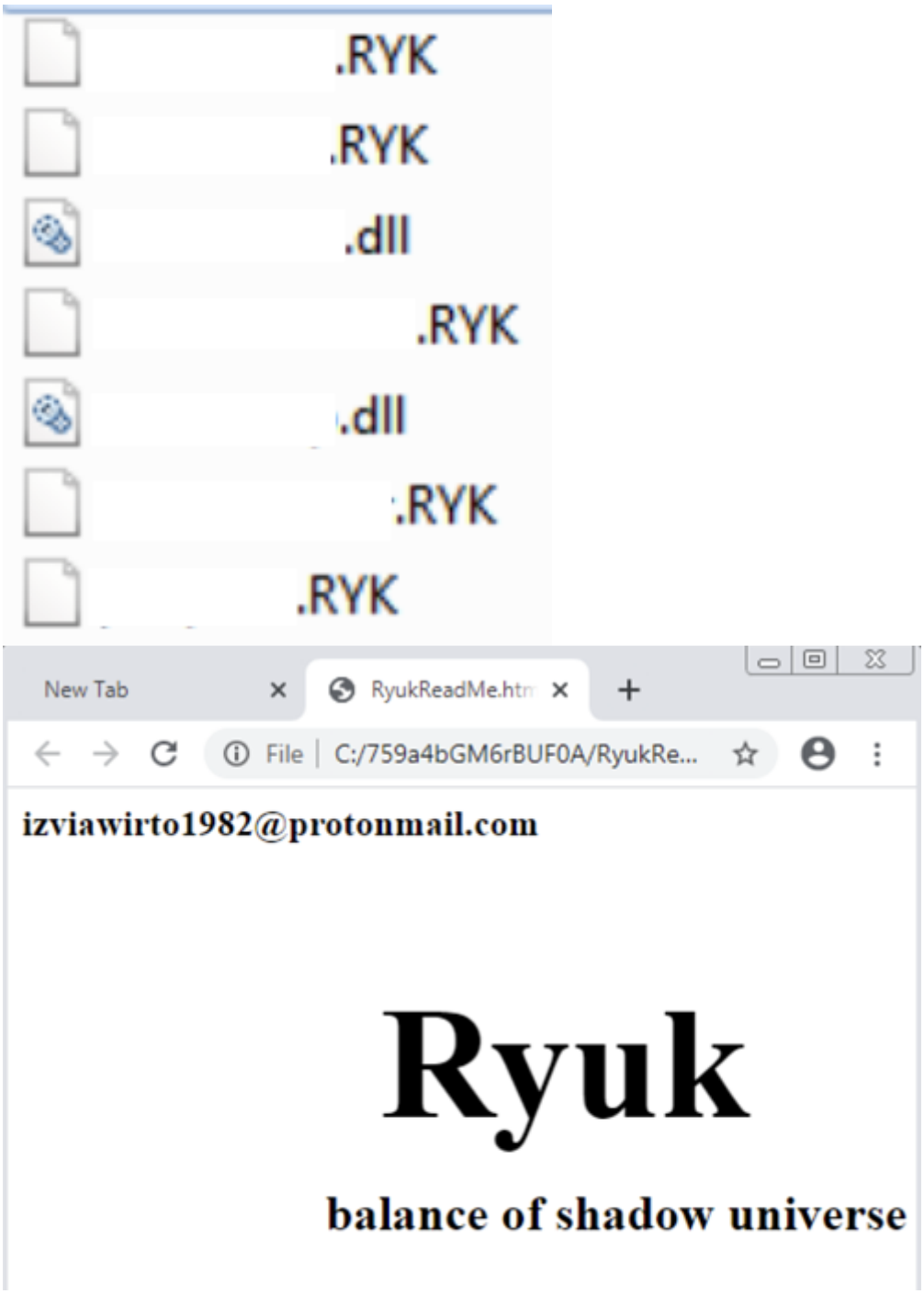
Ryuk ransomware execution as detected by the Cybereason sensor

Once the Ryuk binary is executed, the sample creates a copy of itself (the randomly named child process of Ryuk in the screenshot below is a copy of Ryuk - ltbyhrc.exe) to execute with argument “8 LAN”. This function uses the device’s ARP table to find machines on the local LAN and send Wake-on-Lan packets to them, which if successful mounts the C$ share on the machine and proceeds to encrypt the remote drive.

Both the original binary and the dropped copy (ltbyhrc.exe) perform the same tasks - attempting to stop the services “audioendpointbuilder”, “samss” and “sqlwriter”, then attempting to delete shadow copies and create persistence. Before encryption, the malware also utilizes icacls.exe - a program to change Access Control Lists - to give itself full control over all files and folders on the C: and D: drives.

The original binary can also be seen injecting into other processes which Cybereason detects and tags with floating executable code suspicions.

Successful execution will encrypt the user files and append a .RYK extension to them. In order to avoid corrupting the system, certain files such as .DLL and .EXE files are not encrypted. Folders that are traversed by Ryuk contain a “RyukReadMe.html” file, which in this sample is very barebones, simply contains the name of the malware and a mail address without any further instructions. Perhaps the threat actors believe their reputation precedes them?



Left: encrypted files with .RYK name extensions. Right: Ryuk ransom note

For a more in-depth analysis of Ryuk, please refer to this Cybereason report: *Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk*.

MITRE ATT&CK Breakdown

Impact	Execution	Privilege Escalation	Persistence	Discovery	Defense Evasion
Service Stop	Command and Scripting Interpreter: Windows Command Shell	Process Injection	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	System Network Configuration Discovery	Impair Defenses: Disable or Modify Tools
Inhibit System Recovery	Native API			File and Directory Discovery	
Data Encrypted for Impact				Process Discovery	
Inhibit System Recovery					

INDICATORS OF COMPROMISE

Ryuk executables

SHA-256

92f124ea5217f3fe5cbab1c37a961df0437d5a9cbde1af268c60c4b3194b80ed

d0d7a8f588693b7cc967fb4069419125625eb7454ba553c0416f35fc95307cbe

4023a9849ee7d0c7bd80fc779e1d929c69112e324456578136c159e40449cc15

df3b813d049f8cbd0c8a3b9bb54fba9d385837dc6cced6186157c2adae56ad0e

8a75b7f15ad770bb5a95b7900ac866a1845b3f20f5d22b8918d1f300435b4fc6

0bb18ca131a6ee05ef081f008330d8075369a66a3e034f2412c70405d1397608

44f0da753b38e9ac80f420855d40c4368a906cecb16630d80719e8f758a8c68a

f266f0a4c5213f23a42787a88cd2e8df76d71b3397ed7cc45b6b535fe34a57dd

Bae0d9f0625000dd028c3a747b461c28e5fb5412e0de23a1f2fc2d754ac0d0fa

da83298aae66af3e646b1d9aea2ce8b79514e4681e97faa020d403ca980534fd

1d40658975e461af39f142b2eec149a3ec1d0071bbaf53020d8068e72243322b

B624b3b297c5ebac42fabe2371b42d3add17bdb8c811ca5b51e5f27a96360a2e

---

SHA-1

E62135254b3a51f0180e70a11e4c3ad4a59f81c4

71015f9c281038d63bf7cd45894550c1a26c6b53

A6caaa8f8ab2680ce2179a7571a466beb1b60447

3780f5828fc05bf74649393169f70fafb0ffed25

7ad297507ca71d65c46013e02fc635bc75b0e3a2

F155befc8c3c054f3858a6d3e86a7b04c0a4f5dc

0a5b7330c1e06837b7d47936297f80a87c9057d9

2584992238615ecbfdb83b2d86f6227d07ae4f96

B1f6e6eed8dcdf4d354660c2dbec141ada621eb8

845c2c82415669f8c8b3f565519e29d26d3b1f8a

7ddbc35d1612162538496eb5ece5fc1b6bce6eb8

834d876b47ae8e595ae417a370cd47cc8e061131

Joakim Kandefelt

Joakim Kandefelt is a Security Analyst at Cybereason and part of the Nocturnus Research Team.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus