

# Threat spotlight: the curious case of Ryuk ransomware

---

[blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/](https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/)

Jovi Umawing

December 12, 2019



*Ryuk*. A name once unique to a fictional character in a popular Japanese comic book and cartoon series is now a name that appears in several rosters of the nastiest ransomware to ever grace the wild web.

For an incredibly young strain—only 15 months old—Ryuk ransomware gaining such notoriety is quite a feat to achieve. Unless the threat actors behind its campaigns call it quits, too—Remember GandCrab?—or law enforcement collars them for good, we can only expect the threat of Ryuk to loom large over organizations.

First discovered in mid-August 2018, Ryuk immediately turned heads after disrupting operations of all Tribune Publishing newspapers over the Christmas holiday that year. What was initially thought of as a server outage soon became clear to those affected that it was actually a malware attack. It was quarantined eventually; however, Ryuk re-infected and spread onto connected systems in the network because the security patches failed to hold when tech teams brought the servers back.

## Big game hunting with Ryuk ransomware

---

Before the holiday attack on Tribune Publishing, Ryuk had been seen targeting various enterprise organizations worldwide, asking ransom payments ranging from 15 to 50 Bitcoins (BTC). That translates to between US\$97,000 and \$320,000 at time of valuation.

This method of exclusively targeting large organizations with critical assets that almost always guarantees a high ROI for criminals is called “big game hunting.” It’s not easy to pull off, as such targeted attacks also involve the customization of campaigns to best suit targets and, in turn, increase the likelihood of their effectiveness. This requires much more work than a simple “spray-and-pray” approach that can capture numerous targets but may not net such lucrative results.

For threat actors engaged in big game hunting, malicious campaigns are launched in phases. For example, they may start with a phishing attack to gather key credentials or drop malware within an organization’s network to do extensive mapping, identifying crucial assets to target. Then they might deploy second and third phases of attacks for extended espionage, extortion, and eventual ransom.

To date, Ryuk ransomware is hailed as the costliest among its peers. According to a report by Coveware, a first-of-its-kind incident response company specializing in ransomware, Ryuk’s asking price is 10 times the average, yet they also claim that ransoms are highly negotiable. The varying ways adversaries work out ransom payments suggests that there may be more than one criminal group who have access to and are operating Ryuk ransomware.

## **The who behind Ryuk**

---

Accurately pinpointing the origin of an attack or malware strain is crucial, as it reveals as much about the threat actors behind attack campaigns as it does the payload itself. The name “Ryuk,” which has obvious Japanese ties, is not a factor to consider when trying to discover who developed this ransomware. After all, it’s common practice for cybercriminals to use handles based on favorite anime and manga characters. These days, a malware strain is more than its name.

Instead, similarities in code base, structure, attack vectors, and languages can point to relations between criminal groups and their malware families. Security researchers from Check Point found a connection between the Ryuk and Hermes ransomware strains early on due to similarities in their code and structure, an association that persists up to this day. Because of this, many have assumed that Ryuk may also have ties with the Lazarus Group, the same North Korean APT group that operated the Hermes ransomware in the past.

---

*Recommended read: [Hermes ransomware distributed to South Koreans via recent Flash zero-day](#)*

---

However, code likeness alone is insufficient basis to support the Ryuk/North Korean ties narrative. Hermes is a ransomware kit that is frequently peddled on the underground market, making it available for other cybercriminals to use in their attack campaigns. Furthermore, separate research from cybersecurity experts at [CrowdStrike](#), [FireEye](#), [Kryptos Logic](#), and [McAfee](#) has indicated that the gang behind Ryuk may actually be of Russian origin—and not necessarily nation-state sponsored.

As of this writing, the origins of Ryuk ransomware can be attributed (with high confidence, per some of our cybersecurity peers) to two criminal entities: [Wizard Spider](#) and [CryptoTech](#).

The former is the well-known Russian cybercriminal group and operator of [TrickBot](#); the latter is a Russian-speaking organization found selling [Hermes 2.1](#) two months before [the \\$58.5 million cyber heist](#) that victimized the Far Eastern International Bank (FEIB) in Taiwan. According to reports, this version of [Hermes was used as a decoy or “pseudo-ransomware,”](#) a mere distraction from the real goal of the attack.

## **Wizard Spider**

---

Recent findings have revealed that Wizard Spider upgraded Ryuk to include a Wake-on-LAN (WoL) utility and an ARP ping scanner in its arsenal. WoL is a network standard that allows computing devices connected to a network—regardless of which operating system they run—to be turned on remotely whenever they’re turned off, in sleep mode, or hibernating.

ARP pinging, on the other hand, is a way of discovering endpoints in a [LAN](#) network that are online. According to CrowdStrike, these new additions reveal Wizard Spider’s attempts to reach and infect as many of their target’s endpoints as they can, demonstrating a persistent focus and motivation to increasingly monetize their victims’ encrypted data.

## **CryptoTech**


---

Two months ago, Gabriela Nicolao ([@rove4ever](#)) and Luciano Martins ([@clucianomartins](#)), both researchers at Deloitte Argentina, attributed Ryuk ransomware to CryptoTech, a little-known cybercriminal group that was observed touting Hermes 2.1 in an underground forum back in August 2017. Hermes 2.1, the researchers say, is Ryuk ransomware.

hermes 2.1 ransomware , crypto-fiber, ransomware

Subscribe to this thread | print version

**Cryptotech**



08.22.2017, 15:33

## Hermes 2.1 Ransomware

Software did not work and will not work for RU, UA, BY.

- \* Work offline, email communication.
- \* Written in C.
- \* Weight 45-55kb (each build is unique).
- \* Work on x86 / x64, servers: 2003 and above, XP, 7,8,10.
- \* Easy to creep.
- \* Encryption AES256 + RSA2048, a unique key for each system, and each file.
- \* Only the owner of the private RSA key can decrypt the files, BleepingComputer agree with this.
- \* [\\_\\_ https://www.bleepingcomputer.com/forums/t/640086/hermes-ransom-help-support-topic-decrypt-informationhtml-ransom-note/](https://www.bleepingcomputer.com/forums/t/640086/hermes-ransom-help-support-topic-decrypt-informationhtml-ransom-note/)
- \* Restoring work after a reboot if encryption has not been completed.
- \* Drop user key and instructions in each folder.
- \* 809 file extensions, detailed information in the archive.
- \* Encrypt files of any size.
- \* Data is written over the current file, which makes it difficult to recover data using R-studio, Recuva, etc.
- \* Request for increasing privileges from the user, deleting shadow copies and backups
- \* Set price: \$ 300
- \* Price for email addresses: \$ 50
- \* Included: build with 2 email addresses, decoder builder, unique RSA key pair.

PS: implementation / change of almost any functional is discussed, on a separate financial component.

Manibekov not.  
We reserve the right to refuse to sell without explanation.

AV scan at the moment: [\\_\\_https://viruscheckmate.com/id/NuASrGO3je1V](https://viruscheckmate.com/id/NuASrGO3je1V)

- \* Software does not work in RU, UA, BY countries.
- \* work offline, communication by e-mail.

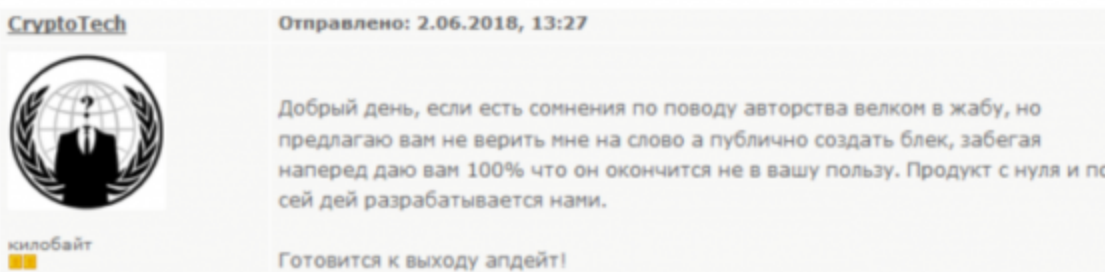
The

CryptoTech post about Hermes version 2.1 on the dark web in August 2017 (Courtesy of McAfee)

In a Virus Bulletin [conference paper](#) and [presentation](#) entitled *Shinigami's revenge: the long tail of the Ryuk ransomware*, Nicolao and Martins presented evidence to this claim: In June 2018, a couple of months before Ryuk made its first public appearance, an underground forum poster expressed doubt on CryptoTech being the author of Hermes 2.1, the ransomware toolkit they were peddling almost a year ago that time. CryptoTech's response was interesting, which Nicolao and Martins captured and annotated in the screenshot below.

#### d. June 2018: Hermes/Ryuk Authorship Questioned

In June 2018, one of Dark Web's exploit[.]in forum users expressed concerns that Hermes ransomware had not been developed by forum user "CryptoTech", who had been selling the ransomware. CryptoTech responded (in Russian) that Hermes was developed by his team from scratch and offered to provide proof via either private jabber communications, or public arbitration process. CryptoTech also shared that his team was getting ready to release a new version of Hermes. That version (i.e. Hermes v2.1) was released a month later, and it was dubbed Ryuk by IT security researchers.



**Key Point:** Willingness to go through exploit[.]in forum's arbitration process, along with a demonstration of inside knowledge on the upcoming release, further lends weight to CryptoTech team's sole involvement in the Hermes/Ryuk ransomware development and maintenance.

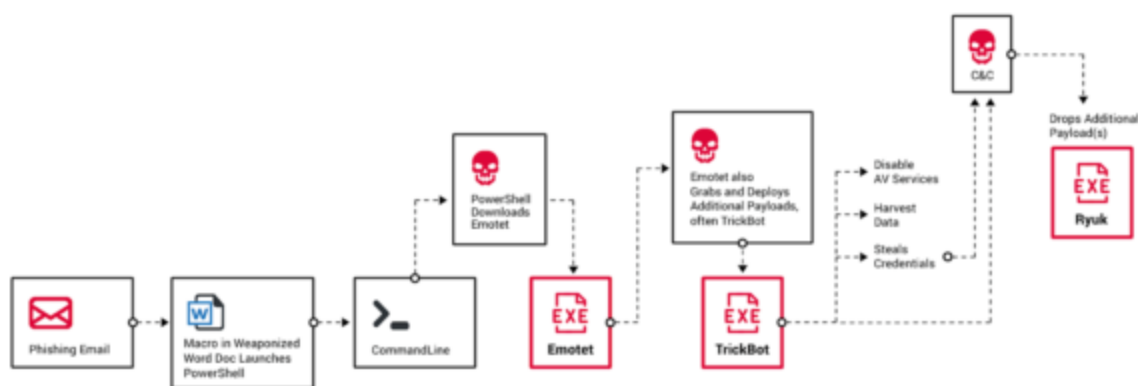
CryptoTech: Yes, we developed Hermes from scratch.

The Deloitte researchers also noted that after Ryuk emerged, CryptoTech went quiet.

CrowdStrike has estimated that from the time Ryuk was deployed until January of this year, their operators have netted a total of 705.80 BTC, which is equivalent to US\$5 million as of press time.

### Ryuk ransomware infection vectors

There was a time when Ryuk ransomware arrived on clean systems to wreak havoc. But new strains observed in the wild now belong to a multi-attack campaign that involves Emotet and TrickBot. As such, Ryuk variants arrive on systems pre-infected with other malware—a “triple threat” attack methodology.



Emotet, TrickBot, and Ryuk triple threat attack works (Courtesy of Cybereason)

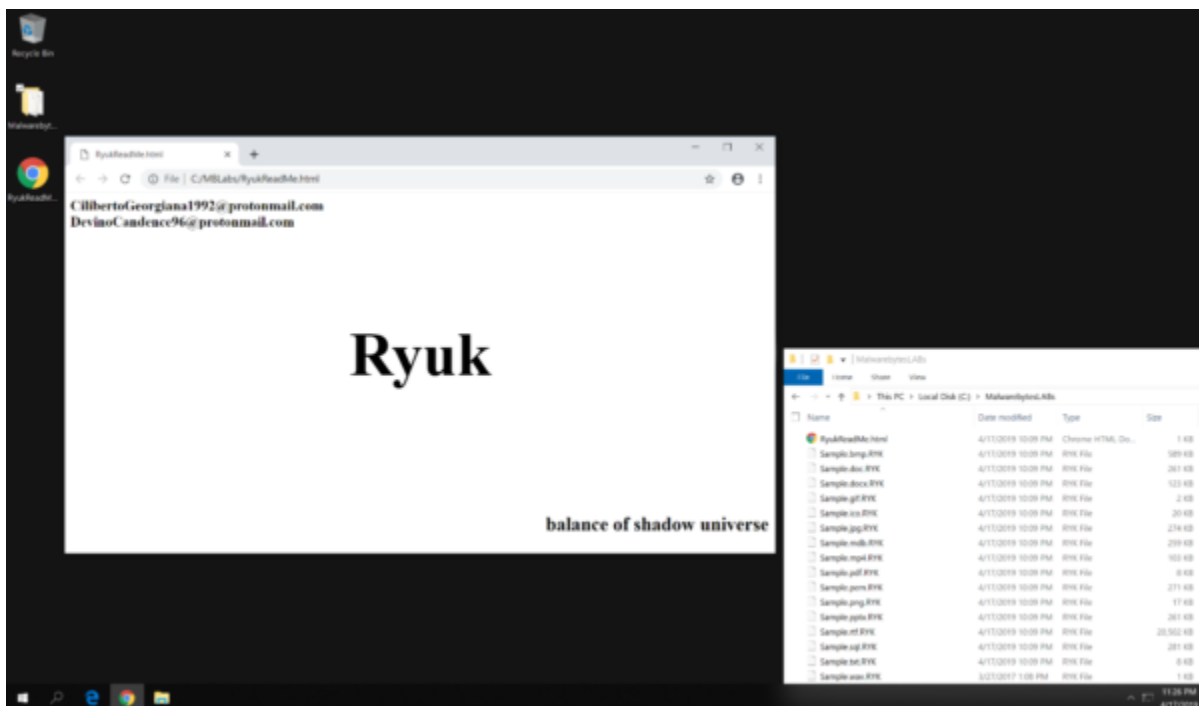
The first stage of the attack starts with a weaponized Microsoft Office document file—meaning, it contains malicious macro code—attached to a phishing email. Once the user opens it, the malicious macro will run `cmd` and execute a PowerShell command. This command attempts to download Emotet.

Once Emotet executes, it retrieves and executes another malicious payload—usually TrickBot—and collects information on affected systems. It initiates the download and execution of TrickBot by reaching out to and downloading from a pre-configured remote malicious host.

Once infected with TrickBot, the threat actors then check if the system is part of a sector they are targeting. If so, they download an additional payload and use the admin credentials stolen using TrickBot to perform lateral movement to reach the assets they wish to infect.

The threat actors then check for and establish a connection with the target's live servers via a remote desktop protocol (RDP). From there, they drop Ryuk.

## Symptoms of Ryuk infection



Systems infected with the Ryuk ransomware displays the following symptoms:

**Presence of ransomware notes.** Ryuk drops the ransom note, *RyukReadMe.html* or *RyukReadMe.txt*, in every folder where it has encrypted files.

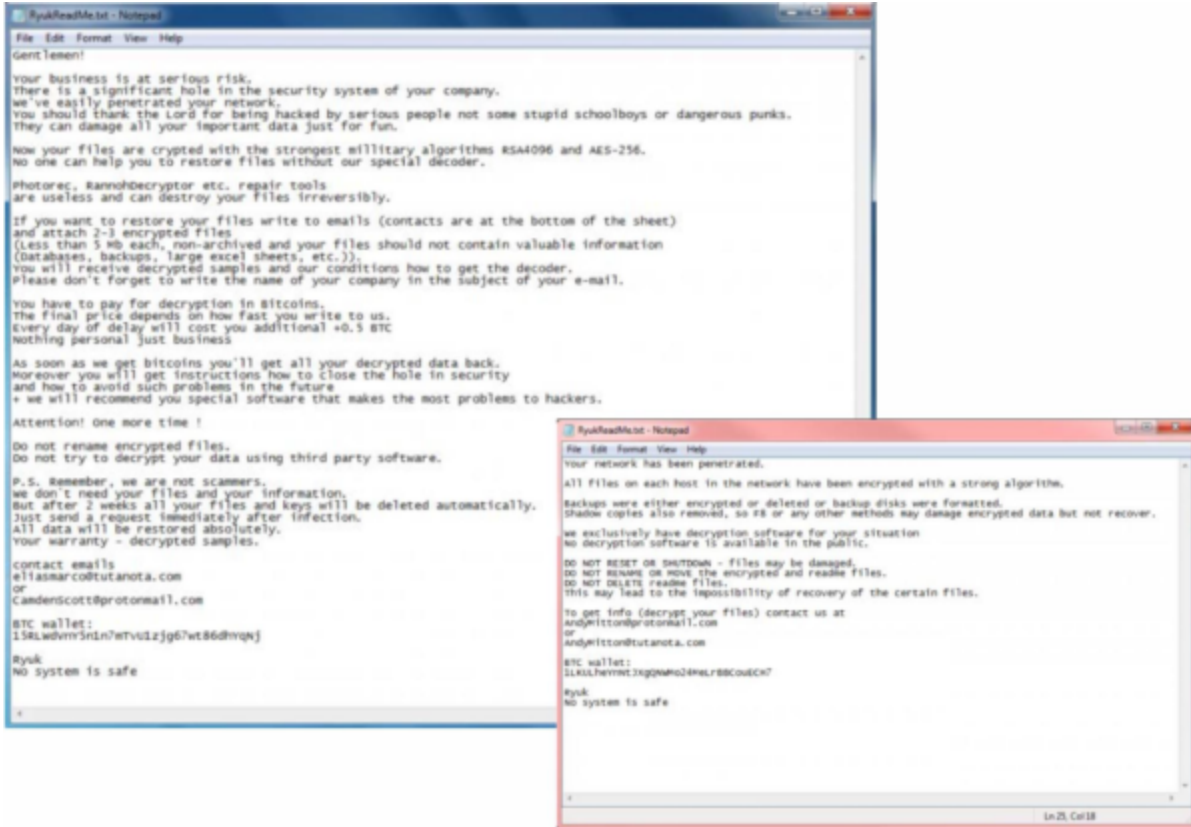
The HTML file, as you can see from the screenshot above, contains two private email addresses that affected parties can use to contact the threat actors, either to find out how much they need to pay to get access back to their encrypted files or to start the negotiation process.

On the other hand, the TXT ransom note contains (1) explicit instructions laid out for affected parties to read and comply, (2) two private email addresses affected parties can contact, and (3) a Bitcoin wallet address. Although email addresses may vary, it was noted that they are all accounts served at Protonmail or Tutanota. It was also noted that a day after the



unsealing of the indictment of two ransomware operators, Ryuk operators removed the Bitcoin address from their ransom notes, stating that it will be given to those affected once they are contacted via email.

There are usually two versions of the text ransom note: a polite version, which past research claims is comparable to BitPaymer's due to certain similar phrasings; and a not-so-polite version.



ransom notes. Left: polite version; Right: not-so-polite version

Greetings!

There was a significant flaw in the security system of your company.  
You should be thankful that the flaw was exploited by serious people and not some rookies.  
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.  
Without our special decoder it is impossible to restore the data.  
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.  
will lead to irreversible destruction of your data.

To confirm our honest intentions.  
Send us 2-3 different random files and you will get them decrypted.  
It can be from different computers on your network to be sure that our decoder decrypts everything.  
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.  
DO NOT RENAME the encrypted files.  
DO NOT MOVE the encrypted files.  
This may lead to the impossibility of recovery of the certain files.

To get information on the price of the decoder contact us at:  
{Redacted}

The payment has to be made in Bitcoins.  
The final price depends on how fast you contact us.  
As soon as we receive the payment you will get the decryption tool and  
instructions on how to improve your systems security

BitPaymer ransom note: polite version (Courtesy of Coveware)

```
HOW_TO_DECRYPT.txt - Notepad
File Edit Format View Help
your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
We exclusively have decryption software for your situation.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.
To get info(pay-to-decrypt your files) contact us at:
You have 48 hours for feedback or decryption keys will be deleted
| @protonmail.com
or
| @tutanota.com
BTC wallet:
To confirm our honest intentions.
Send 2 different random files and you will get it decrypted.
It can be from different computers on your network to be sure we decrypts everything.
Files should have .LOCK extension of each included.
2 files we unlock for free.
```

BitPaymer ransom note: not-so-polite version (Courtesy of Symantec)



**Encrypted files with the RYK string attached to extension names.** Ryuk uses a combination of symmetric (via the use of AES) and asymmetric (via the use of RSA) encryption to encode files. A private key, which only the threat actor can supply, is needed to properly decrypt files.

Encrypted files will have the .ryk file extension appended to the file names. For example, an encrypted *sample.pdf* and *sample.mp4* files will have the *sample.pdf.ryk* and *sample.mp4.ryk* file names, respectively.

This scheme is effective, assuming that each Ryuk strain was tailor-made for their target organization.

While Ryuk encrypts files on affected systems, it avoids files with the extension .exe, .dll, and .hrmlog (a file type associated with Hermes). Ryuk also avoids encrypting files in the following folders:

- AhnLab
- Chrome
- Microsoft
- Mozilla
- Recycle.bin
- Windows

## **Protect your system from Ryuk**

---

Malwarebytes continues to track Ryuk ransomware campaigns, protecting our business users with real-time anti-malware and anti-ransomware technology, as well as signature-less detection, which stops the attack earlier on in the chain. In addition, we protect against triple threat attacks aimed at delivering Ryuk as a final payload by blocking downloads of Emotet or TrickBot.



## Malware automatically quarantined

It is no longer a threat to your computer

Type: Malware

Name: Ransom.Ryuk

Path: C:\MBLabs\Ryuk.exe

Close

We recommend IT administrators take the following actions to secure and mitigate against Ryuk ransomware attacks:

- Educate every employee in the organization, including executives, on how to correctly handle suspicious emails.
- Limit the use of privilege accounts to only a select few in the organization.
- Avoid using RDPs without properly terminating the session.
- Implement the use of a password manager and single sign-on services for company-related accounts. Do away with other insecure password management practices.
- Deploy an authentication process that works for the company.
- Disable unnecessary share folders, so that in the event of a Ryuk ransomware attack, the malware is prevented from moving laterally in the network.
- Make sure that all software installed on endpoints and servers is up to date and all vulnerabilities are patched. Pay particular attention to patching CVE-2017-0144, a remote code-execution vulnerability. This will prevent TrickBot and other malware exploiting this weakness from spreading.
- Apply attachment filtering to email messages.
- Disable macros across the environment.

For a list of technologies and operations that have been found to be effective against Ryuk ransomware attacks, you can go here.

### Indicators of Compromise (IOCs)

---

Take note that professional cybercriminals sell Ryuk to other criminals on the black market as a toolkit for threat actors to build their own strain of the ransomware. As such, one shouldn't be surprised by the number of Ryuk variants that are wreaking havoc in the wild. Below is a list of file hashes that we have seen so far:

- cb0c1248d3899358a375888bb4e8f3fe
- d4a7c85f23438de8ebb5f8d6e04e55fc
- 3895a370b0c69c7e23ebb5ca1598525d
- 567407d941d99abeff20a1b836570d30
- c0d6a263181a04e9039df3372afb8016

As always—stay safe, everyone!