RYUK RANSOMWARE

2.1
25/02/2021

Table of contents

1 Background

1.1 Origins

The Ryuk ransomware was first observed in August 2018 [1]. It is a variant of the Hermes 2.1 ransomware, sold on the underground forum exploit.in from February 2017 by the cybercriminal group CryptoTech for around 300 dollars [2].

In June 2018, when a member of the forum expressed doubts as to whether the group was the developer of Hermes 2.1, CryptoTech confirmed that it was behind the ransomware and announced the forthcoming release of a new version of Hermes. However no new version of Hermes, other than Ryuk, appeared following this announcement [3].

Unlike Hermes, Ryuk has not been made available for sale on exploit.in, and CryptoTech ceased its activities on the forum following this announcement [4]. A doubt therefore remains as to the origins of Ryuk.

Comment: CryptoTech's disappearance could be due to a change of business model, leading to a smaller circle of users of its new Ryuk ransomware. The appearance of Ryuk could also be a result of the acquisition of the Hermes 2.1 source code by another attacker group, which may have developed Ryuk from this starting point.

Deloitte researchers believe Ryuk is sold as a toolkit to attacker groups. There could therefore be as many variants as there are attackers groups that buy the code to generate their binaries [4].

Comment: This hypothesis cannot be confirmed by the ANSSI (French National Cyber Security Agency), which has not noted Ryuk being promoted on underground forums in the way that Hermes 2.1 was.

A connection with the tactics, techniques and procedures (TTPs) of the Bluenoroff intrusion set, reportedly linked to North Korea, had been momentarily established by some editors due to the use of the Hermes ransomware in the attack on Taiwan's Far Eastern International Bank in October 2017. However, it was concluded that Bluenoroff had used Hermes having obtained it from the Dark Web.

1.2 Characteristics

Ryuk does not have the capacity for automatic lateral movement within a network, hence the need for access *via* a first payload [1] or manual lateral movement.

A Ryuk sample with worm-like capabilities allowing it to spread automatically within networks it infects, was discovered during an incident response handled by the ANSSI in early 2021 (see appendix 5.2).

Ryuk consists of a dropper that drops one of the two versions of a data encryption module (32- or 64-bit) on the victim's computer. The dropper then executes the payload. After a few minutes of inactivity, Ryuk seeks to stop more than 40 processes and 180 services, in particular those related to antivirus softwares, databases and backups. It ensures its persistence through the creation of a registry key [5].

Using a combination of the symmetric (AES) and asymmetric (RSA) encryption algorithms serves both to encrypt the files and to protect the encryption key, making it impossible for a third party to decrypt the data [5].

After recursive scanning of the disks and network sharing in the infected system, the malicious payload is injected into trusted processes. Ryuk then encrypts all files, with the exception of certain Windows, Mozilla, Chrome and Ahnlab files [5].

Comment: Ahnlab is a South Korean IT threat analysis and response company. The reason for its inclusion in Ryuk's white list, inherited from Hermes 2.1, is unclear.

Internet browsers and the basic components of the operating system are left intact to allow victims to read the ransom demand, purchase cryptocurrencies and pay the ransom [6]. However, sometimes Ryuk encrypts Windows base files, making it difficult or even impossible to reboot compromised machines [7].

Ryuk appends .RYK to the encrypted files and drops the RyukReadMe.txt file in the encrypted directories.

Since October 2019, workstations on the local network that have been powered off can be switched on by Ryuk using a Wake-on-LAN feature allowing it to increase its attack surface [8].

It then destroys all shadow copies on the system to prevent the users from restoring their system *via* vssadmin commands or by running a .bat file[1] [9].

Comment: The Raccine tool available on GitHub can intercept the use of vssadmin, prevent the deletion of shadow copies and even, in some cases, block the chain of infection. Raccine is a temporary solution only to be implemented as a last resort in the face of an imminent threat of encryption. Its use is not a substitute for the implementation of technical security measures and defence in depth. [10].

In 2018, Ryuk's short ransom demand format was very similar to that of the BitPaymer ransomware, operated by the cybercriminal group Evil Corp since 2017 [4]. However, the ransom demands were reportedly ten times greater than the average demand from other ransomware [11].

Ryuk does not have a data exfiltration feature or a dedicated leak website to publish data stolen from their victims unlike many other ransomwares. However:

- in mid-2019, a stealer type of malware with code similarities to Ryuk was identified by Malware Hunter Team. This code is believed to be used to extract .docs and .xlsx files containing certain keywords from the financial, military or legal lexical fields ("tank", "defence", "military", "classified", "federal", "finance", "IBAN", "Swift", *etc.*). It is thought to be programmed to avoid files relating to Ryuk, in other words the RyukReadMe.txt ransom demand and files with the .RYK extension [12];

- according to the editor FireEye [13], attackers using Ryuk sometimes exfiltrate data from their victims by means other than the ransomware itself. However, this data is believed to be limited to internal reconnaissance data or data extracted from the Active Directory, allowing attackers to move laterally and escalate their privileges.

1.3 Victimology

Ryuk has compromised many entities since August 2018, targeted for their profitability and their ability to pay high ransoms (Big Game Hunting).

Although no specific sector targeting can be identified, Ryuk appears in particular to be impacting the United States and Canada.

In October 2020, Ryuk was reportedly responsible for 75% of attacks on the American healthcare sector [14]. Actors deploying Ryuk are believed to have been attacking this sector since the first half of 2019.

According to Prevailion, as of 3 November 2020, approximately 1,400 entities are thought to be communicating with Cobalt Strike command and control (C2) servers associated with UNC1878, a Ryuk user [15]. These entities are believed to be American hospitals and government agencies, pharmaceutical companies and universities in the rest of the world [14].

---

[1]Extension to an MS-DOS command file allowing you to design scripts, used here for maintenance tasks such as file deletion.

2 Chains of infection involving Emotet, TrickBot and BazarLoader

2.1 Sequence of the initial chains of infection

Some victims were infected by TrickBot starting in June 2018, then compromised by Ryuk as of August [2]. According to FireEye, the TrickBot-Ryuk chain of infection may even have existed since December 2017 [16].

Comment: However, with FireEye confirming that Ryuk's public appearance dates from August 2018, the reference to December 2017 suggests that this is the date that TrickBot opened access, followed by encryption by Ryuk as of August 2018.

Since this date, TrickBot is the loader most responsible for the distribution of Ryuk. TrickBot can be distributed upstream via the Emotet malware-as-a-service. The Emotet-TrickBot-Ryuk and TrickBot-Ryuk chains of infection have therefore frequently been encountered, and persist at least until September 2020.

The infection vector has often been to be a phishing email delivering either Emotet [16] or TrickBot [17].

Once legitimate post-exploitation tools are distributed by TrickBot (Cobalt Strike, Empire, BloodHound, Mimikatz, LaZagne), attackers obtain privileged access to a domain controller (or other systems with privileged access) and deploy Ryuk (for example *via* PsExec) within the victim's information system (IS) [18].
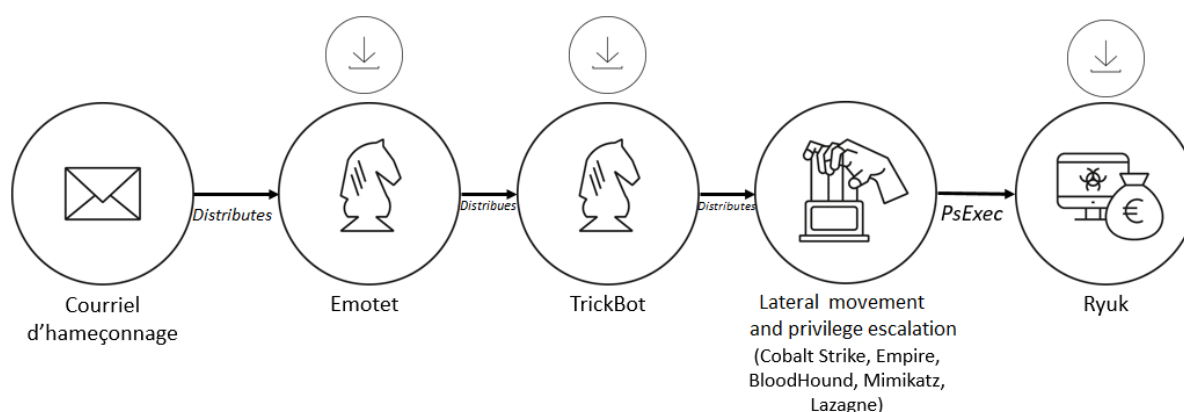

Fig. 2.1: Simplified sequence of the Emotet-TrickBot-Ryuk infection chain

2.2 Evolution towards the Bazar-Ryuk chain of infection

By March 2020 infection chains involving TrickBot were reportedly fewer, and may even have temporarily ceased. In July 2020, the Emotet-TrickBot infection chain emerges again, after several months of inactivity from Emotet. This chain has since resulted in the distribution of Ryuk or Conti ransomware [19].

From mid-September 2020, the BazarLoader-Ryuk chain of infection appears to replace those involving TrickBot.

BazarLoader is generally distributed through phishing campaigns. Emails can be sent using the SendGrid marketing platform. They contain links to Google Docs pages of document previews, prompting the victim to download the file as the preview does not usually work [20, 21, 22]. Recent campaigns identified by FireEye [13] no longer use the SendGrid platform, but instead use the infrastructure of attackers or compromised email servers to send phishing emails containing links to documents. These documents sometimes include references to the entity for

which the target works. The files concerned are executables signed with revoked certificates, hosted on legitimate web services (Google Drive, Basecamp, Slack, Trello, Yougile, JetBrains, cdn77 and others) [13].

Once the IS is compromised, BazarLoader downloads from the C2 server[2] a payload (encrypted in XOR): BazarBackdoor. The backdoor then downloads post-exploitation frameworks, most frequently Cobalt Strike, to enable latterstages of the intrusion leveraging tools such as Anchor, PowerTrick[3] [13], BloodHound, PowerSploit and AdFind [25]. Reconnaissance data (in particular recovered *via* AdFind) is exfiltrated *via* FTP [25].

Privileges have been escalated using Mimikatz, Rubeus[4] [13], or by exploiting a Zerologon vulnerability (CVE-2020-1472) [26].

BazarBackdoor, although not exclusively dedicated to this purpose, can be used to enable the distribution of Ryuk ransomware.
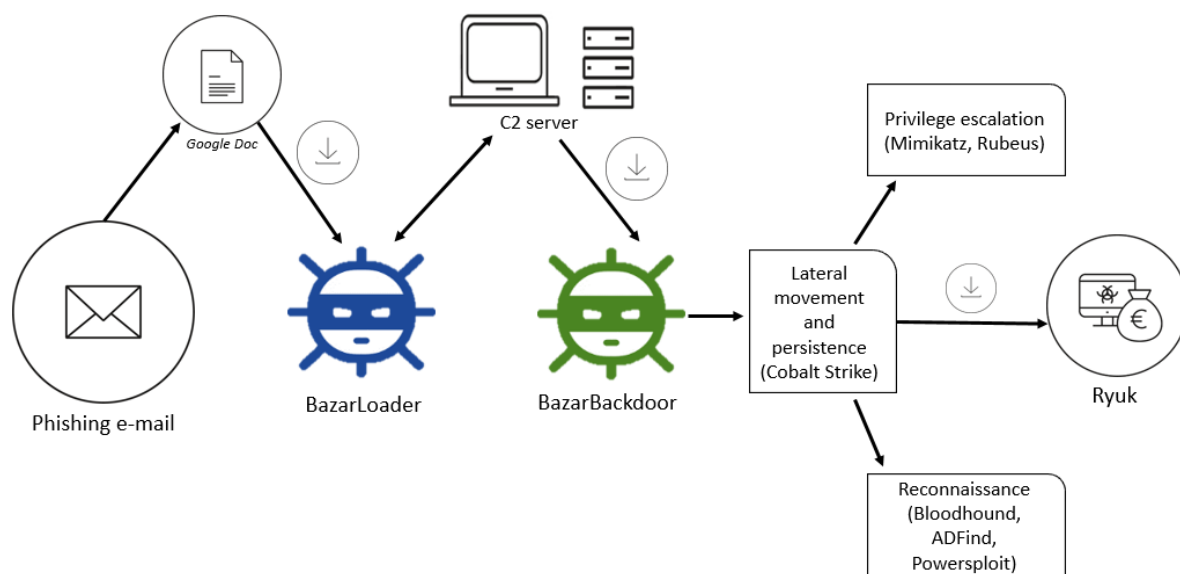

Fig. 2.2: Simplified sequence of the Bazar-Ryuk chain of infection

2.3 Attacker groups involved

2.3.1 Wizard Spider

Origins

The group operating the TrickBot malware is called Wizard Spider by Crowdstrike, and "the TrickBot gang" by other editors. It is also thought to be behind the Anchor backdoor and PowerTrick.

This group is believed to include members of the Gold BlackBurn group, developers and operators of the Dyre banking trojan [27], which ceased activities in November 2015 following action by the Russian police.

Dyre emerged in June 2014. Its specific characteristics were as follows:

- Dyre is believed to have the same developer as Gozi Neverquest (alias Vawtrak) [28]. Gozi Neverquest was based on the source code of the Gozi malicious code, leaked in 2010. The cyber crime group responsible for

---

[2]BazarLoader uses EmerDNS .bazar domains for its C2s. This allows decentralised domain names to be registered on a blockchain [23]. The DNS resolutions of Bazar's C2 servers thus make dismantling and sinkholing [24] impossible.

[3]Post-exploitation framework.

[4]Mimikatz Kerberos module.

TLP:WHITE

Ryuk ransomware

its development, Gold Swathmore, is reported to have collaborated with Gold BlackBurn. This collaboration is believed to have continued after the arrest of members of Gold BlackBurn in 2015 and the leader of Gold Swathmore in 2017, through their respective successors Wizard Spider and Lunar Spider [29];

- certain attacks involving Dyre could be connected to the Business Club cybercriminal group. It is then possible that from 2014, this group may have diversified its activity, using Dyre to steal money from corporate bank accounts and Dridex to steal money from retail bank accounts (Evil Corp) [28]. Like Dridex, Dyre emerged two weeks after the dismantling of the GameOverZeuS botnet, operated by M. Bogatchev, the developer of the banking trojan ZeuS, and the Business Club cybercriminal group.
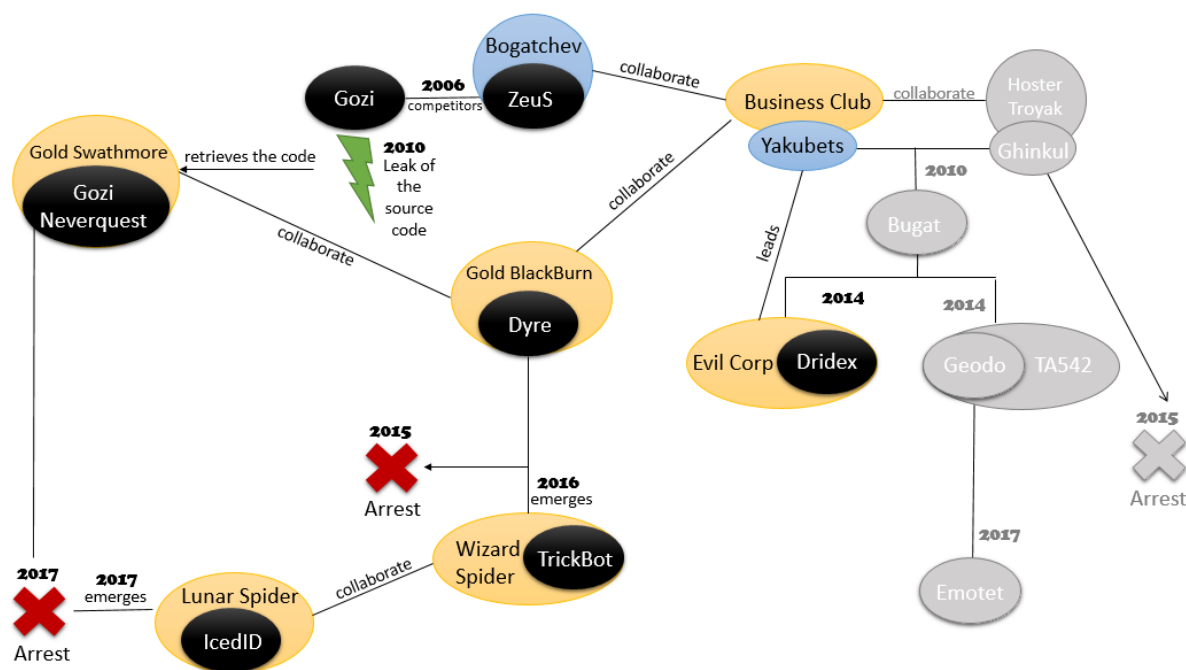

Fig. 2.3: Origins of Wizard Spider

The banking Trojan and *loader* TrickBot

TrickBot, which appeared one year after the dismantling of Dyre, is operated on the basis of an affiliate model involving its distribution by independent groups [30]. Although TrickBot affiliates cannot be identified, campaigns involving TrickBot are distinguished by their infection vector and a hard-coded parameter : the Group Tag or Gtag [31].

Different Gtags are associated with the TrickBot-Ryuk chains of infection :

- "serXXX" (ser0918us for example) [18];

- "libXXX", "totXXX" and "jimXXX": several Gtags can cohabit on the same infected IS; this is the case for example for the Gtags "libXXX", "totXXX" and "jimXXX" (373 and 369 or 371), which can therefore be found following a "serXXX" Gtag and/or a phishing email [16, 18];

- "morXXX": this is the Gtag associated with primary infections by Emotet since September 2019 (mor 84 [32] or mor114 [33] for example).

  Comment: Nevertheless, as Ryuk has been active since at least August 2018, and already distributed as the final payload in the Emotet-TrickBot chain of infection, Gtags other than morXXX have contributed to attacks by this ransomware. It has not been possible to identify whether these attacks, perpetuated for more than two years now, are the work of a single attacker group, or of several groups whose Gtag has evolved.

The BazarLoader and the BazarBackdoor

Wizard Spider is believed to have started distributing the BazarLoader and BazarBackdoor malwares in March 2020 [30]. Several technical aspects suggest that Wizard Spider is also the developer of these codes:

- use of the same crypter by TrickBot and BazarBackdoor and very similar decryption routines between the Bazar and TrickBot loaders (use of the same WinAPIs, custom RC4, API-hammering);

- use by Anchor and Bazar of the Emercoin DNS resolution for C2 communications;

- reuse of compromised domains, for example machunion[.]com, bakedbuns[.]com and ruths-brownies[.]com, which have in the past hosted TrickBot and more recently BazarLoader.

Bazar, like TrickBot, is believed to be used as an access-as-a-service to compromise an IS on behalf of other attacker groups. It is not known whether BazarLoader, like TrickBot, also works on an affiliate model.

Comment: TrickBot and Bazar are regularly used to distribute Ryuk. However, it is not possible for the ANSSI to determine whether these attacks, or some of them, are the work of Wizard Spider, TrickBot affiliates, Bazar clients, or a Ryuk end operator using attackers specialising in access-as-a-service or buying compromised or qualified access on the Dark Web.

2.3.2 UNC1878

UNC1878, also known as One group [34], is an activity *cluster* discovered by FireEye at the end of January 2020 and involved in TrickBot-Ryuk infection chains since January 2020, then in Bazar-Ryuk infection chains from September 2020 [35, 36].

Its targeting is indiscriminate[5], and its infections are opportunistic [35, 36]. They are characterised by:

- their infection vector, which is based on phishing emails generally containing links;

- their speed of execution, with the time between initial infection and encryption recently reduced from a few (2 to 5) days to three hours [25];

- the constant use of self-signed Cobalt Strike samples [35];

- the use of legitimate tools throughout the post-compromise infection chain (Cobalt Strike Beacon, Empire, Meterpreter, Mimikatz, LaZagne, Kerbrute, Kerberoast, BloodHound, AdFind, PowerSploit) [35];

- the absence of exfiltration of information from its victims' IS [35].

According to FireEye, a fifth of all ransomware-related intrusions in 2020 are due to Ryuk. 83% of them are the work of UNC1878, of which 27% were successful [35].

Therefore UNC1878 may not be responsible for all cyberattacks involving the Ryuk ransomware [37], but it is thought to be behind the attacks against American hospitals since October 2020 [35].

Comment: UNC1878 could rely on different TrickBot affiliates or different attackers with access to BazarLoader to open up access to its victims. It could itself be an affiliate/client of these two loaders, but this would not explain why different Gtags could be encountered during TrickBot-Ryuk infections when it is commonly accepted that each Gtag (or at least the prefix consisting of letters) corresponds to a single affiliate.

---

[5]One reason for this could be that UNC1878's accesses are obtained as-a-service from TrickBot or Bazar's operators.

3 Other identified chains of infection and associated attacker groups

Emotet-TrickBot-Ryuk, TrickBot-Ryuk and Bazar-Ryuk are not the only infection chains leading or having led in the past to the deployment of the Ryuk ransomware.

3.1 Buer and SilentNight

According to Sophos, in September 2020, Buer loader was used to gain a foothold in an intrusion where Ryuk was deployed [38]. Buer is a malware-as-a-service used to distribute banking Trojans and ransomware. It is available on the Dark Web for 350 dollars.

The Buer loader and Ryuk droppers use the same shellcode loader to inject the decompressed malicious code into the memory [38]. Lastly, Buer is believed to have already distributed TrickBot [20], without having been able to identify the Buer-TrickBot-Ryuk chain of infection.

SilentNight is also involved in attacks aimed at distributing Ryuk ransomware. This trojan, sold on Russian-speaking underground forums since the end of 2019, is a variant of the Zloader malware (from the ZeuS source code) whose last activity dates back to 2018 [39].

These two malwares, like BazarLoader, were observed as being distributed through phishing emails sent *via* Send-Grid and then through a Russian host, directing to malicious Google Docs [38].

Comment: *The same Ryuk user could, for example, use these three distribution services to carry out their attacks.*

3.2 Infection chain involving the FIN6 cyber crime group

3.2.1 Involvement of FIN6 or affiliated parties in Ryuk incidents

The involvement of the Russian-speaking cybercriminal group FIN6 or affiliated parties in Ryuk incidents is thought by FireEye to date back to July 2018 [40, 4].

Active since 2015, FIN6 traditionally targeted point of sale (POS) terminals and eCommerce payment servers in order to exfiltrate and resell banking data. From mid-2018, technical and operational evidence suggests that FIN6 or affiliated parties were distributing the Ryuk and LockerGoga ransomware (which appeared in January 2019).

The editor Morphisec [41] reported intrusions in early 2019 in India, Japan and the United States into POS systems belonging to the financial and healthcare sectors, using Cobalt Strike and the FrameworkPOS malicious code. According to the editor, this campaign could be attributed to FIN6 due to their similar TTPs.

Based on analyses carried out by the ANSSI and its partners, two IOCs found during this campaign targeting POS systems, IP addresses 185.202.174.91 and 93.115.26.171, also appear in incidents handled by the ANSSI involving Ryuk and LockerGoga ransomware. Therefore:

- The ANSSI's analysis of the command and control infrastructure related to LockerGoga found the IP address 185.202.174.91 downloading Metasploit payloads or payloads linked to the Empire attack *framework*:

IP address	AS	AS name	AS country	CIDR	CIDR name	CIDR country
185.202.174.91	174	COGENT-174- Cogent Communications	US	185.202.174.0/24	H129	Canada

- The IP address 93.115.26.171 was also found during these investigations, downloading a payload on the compromised machine. It was discovered during a LockerGoga incident and a Ryuk incident handled by the

ANSSI.

IP address	AS	AS name	AS country	CIDR	CIDR name	CIDR country
93.115.26.171	16125	CHERRYSERVERS1-AS	LT	93.115.26.0/24	CHERRYSERVERS-LT-DEDICATED	Lithuania

The technical links identified here, which are not exhaustive, support FireEye's hypothesis that FIN6-affiliated parties have been involved in attacks using Ryuk and LockerGoga ransomware.

The infection vector observed during the incidents handled by the ANSSI is the same as that identified by FireEye: the attackers are thought to have compromised their targets by exploiting an exposed service on the Internet. After the initial compromise, they appear to have used stolen credentials to move laterally using RDP [40].

Comment: It is however hard to say whether FIN6 was the final operator of the LockerGoga and Ryuk ransomware in these infection chains, or an intermediate attacker.

3.2.2 Assumed links between FIN6 and Wizard Spider

IBM [42] believes FIN6 and Wizard Spider to be working together. The reasons for this assumption are as follows:

- in late 2019-early 2020, TrickBot and the Anchor backdoor were used for intrusions at companies, some of which had POS systems. These intrusions were similar to FIN6's traditional tactics, techniques and procedures;

- it was found that during infection chains involving PowerTrick and Anchor, TerraLoader had installed the backdoor More_Eggs[6], of which FIN6 is one of the main users (together with the Cobalt Gang cybercriminal group). In addition, the attackers are believed to have used PowerShell to download and execute TerraLoader, in turn responsible for installing More_Eggs, a method specific to FIN6 according to IBM;

- the *Rkey* of one of the samples contained the text "wearenotcobaltthanks", a message similar to others found in More_Eggs samples attributed to FIN6 ("We are not cobalt gang, stop associating us with such skids!").

Comment: Since FIN6 seems to have used Wizard Spider's access services, it is possible that it has been used in incidents where Ryuk was deployed. However, this would not explain why TrickBot distributed Ryuk but never LockerGoga, whereas FIN6 is thought to have distributed these two ransomware as well as MegaCortex and Maze.

3.3 Links between Ryuk and the Conti ransomware

After emerging in December 2019 [43], the Conti ransomware is believed to have been made available to affiliates based on a ransomware-as-a-service (RaaS) model. It was deployed in parallel with Ryuk during Emotet-TrickBot-Ryuk/Conti or BazarLoader-Ryuk/Conti chains of infection.

Furthermore, FireEye has noted intrusions involving the Anchor backdoor and the distribution of Conti and Maze ransomwares [13]. Conti, which unlike Ryuk has a dedicated site for the disclosure of data stolen from victims, even published the data of two victims listed on the Maze dedicated leak site.

Comment: Similarities in code and ransom message, along with distribution by TrickBot, suggest that Conti may have been created by the developers of Ryuk. However, no link seems to exist between Ryuk and Maze, while Maze was also distributed by TrickBot. It is therefore possible that the same Ryuk and Conti user may use or be affiliated with the TrickBot distribution service. Overlaps between Ryuk and Conti could also be plausibly due to a common initial access provider between various ransomware operators.

---

[6]Alias SpicyOmelette and Skid, More_Eggs is a JavaScript backdoor made available to certain affiliates by the service provider as malware-as-a-service Venom Spider (alias badbullzvenom), active since 2012.

4 Conclusion

Ryuk is not officially a RaaS. However, it appears that several different attackers are involved in infection chains leading to the deployment of Ryuk. There are several arguments in favour of this hypothesis:

- The Hermes kit sold on the Dark Web did not contain any exploitation tool, forcing its buyers to compromise the victims using their own resources or those of an intermediary. The same scenario could apply for Ryuk . Potential intermediaries could be TrickBot, Bazar, Buer and SilentNight. These loaders are thought to be used by the final operator of Ryuk or by attackers responsible for opening access for it;

- FIN6 or affiliated parties would clearly have been involved in Ryuk incidents in 2019 in which no intermediate payload of the type seen with previous *loaders* was observed;

- The various Ryuk ransom demands suggest, according to MalwareBytes, that there could be more than one group with access to the ransomware [44];

- According to FireEye, UNC1878 is responsible for 83% of Ryuk infections in 2020 and is not believed to exfiltrate any information, unlike other Ryuk operators that may exfiltrate internal reconnaissance information from their victims' networks [35].

In view of these elements and the exclusive use of legitimate post-compromise tools during the infection chains leading to the deployment of Ryuk, preventing the identification of distinct TTPs, it is possible that :

- that a single Ryuk operator is making the ransomware available to trusted partners. Trusted partners would then be able to distribute Ryuk *via* the Wizard Spider distribution services (TrickBot and Bazar) or using their own resources. This hypothesis could be strengthened by the possible collaboration between FIN6 and Wizard Spider;

- that several malicious parties are using Ryuk (including FIN6 in 2019) independently, and that one or more of them are affiliated to TrickBot or at least a client of its distribution service and/or that of Bazar (including UNC1878);

- that a single Ryuk operator is using different distribution services (TrickBot, Bazar, Buer, SilentNight) or one or more hackers-for-hire (which could include FIN6), which would explain the differences in TTPs between incidents leading to encryption by Ryuk.

The Ryuk ransomware remains particularly active in the second half of 2020. It differs from most other ransomwares in that at least one of its operators attacked hospitals during a pandemic, the absence of a dedicated data disclosure site and the extreme speed of execution (around a few hours) of the Bazar-Ryuk chain of infection.

5 Appendices

5.1 Significant symptoms summary

5.1.1 Main effects of Ryuk on the system

Ryuk encrypts some files present on the machine and appends `.RYK` to the filename. The ransom note is written in each directory containing encrypted files. This ransom note can appear under two formats:

- a text file named `RyukReadMe.txt`;

- an HTML file named `RyukReadMe.html`.

Its content may vary but some patterns are always present like the Ryuk signature followed by the sentence *no system is safe*.

Ryuk's persistence is achieved by setting the registry key `HKEY_CURRENT_USER\SOFTWARE\Microsoft \Windows\CurrentVersion\Run\svchost` with Ryuk's filepath as value.

The Ryuk variant analyzed in this document does have self-replication capabilities. The propagation is achieved by copying the executable on identified network shares. This step is followed by the creation of a scheduled task on the remote machine. The content of this scheduled task is described in the analysis present in this document. Some filenames were identified for this copy: `rep.exe` and `lan.exe`.

Finally, Ryuk deletes the Volume Shadow Copies to prevent file recovery.

5.1.2 Main Ryuk's network effects

Ryuk looks for network shares on the victim IT infrastructure. To do so, some private IP ranges are scanned:

- `10.0.0.0/8`;

- `172.16.0.0/16`;

- `192.168.0.0/16`.

For each identified host, Ryuk will attempt to mount possible network shares using SMB enumeration.

Before this scan step, Ryuk reads through the victim's ARP table and sends a Wake-On-LAN paquet to each host. The purpose is to wake up powered off computers.

These operations are easily visible in network logs.

5.2 Analysis of a new version of the Ryuk ransomware

5.2.1 Summary

The analyzed malware is a new version of the Ryuk ransomware.

On top of its usual functions, this version holds a new attribute allowing it to self replicate over the local network.

Through the use of scheduled tasks, the malware propagates itself - machine to machine - within the Windows domain.

Once launched, it will thus spread itself on every reachable machine on which Windows RPC accesses are possible.

It would appear that this specific Ryuk version does not carry any exclusion mechanism (MUTEX like) preventing infections of the same machine over and over again.

5.2.2 Description

The malware is based on a randomly-chosen open source software. It is then recompiled and backdoored.

The malicious code is stored in the resource 11/943 of the binary and encrypted with the RC4 algorithm using the key `pDkz^q#+(2w&95`.

The code contains the string `Fuck def`.

The ransomware contains lines of code allowing files and subfolders encryption.

No mechanism for blocking the execution of the ransomware has been identified (MUTEX like or else).

5.2.3 Functions

The malware can launch `icacls <path> /grant Everyone:F /T /C /Q` to delete every access-based restrictions on files and directories.

It locally creates `ryukreadme.html` files, most likely with a .onion TOR URL for negociation.

It locally creates `<random>.dll` files actually containing a *Rich Text File* format document.

The fake DLL is locally launched through a scheduled task executing `wordpad.exe <random>.dll`.

The RTF file contains the usual Ryuk message:: « `balance of shadow universe` ».

The program also allows for an autonomous propagation of the encrypting binary.

5.2.4 Propagation

The program copies itself with a `rep.exe` or `lan.exe` suffix.

It generates every possible IP addresses on local networks and sends an ICMP ping to each of them.

It lists the IP addresses of the local ARP cache and sends them a packet (most likely the Wake-on-LAN which has already been documented for this ransomware).

The program then lists all the sharing resources opened on the found IPs, mounts each of them and can encrypt their content.

This malware can also create a ryukreadme.html file as well as a copy of itself on the targeted host.

Finally, it can remotely create a scheduled task to execute itself on this host.

Launch of the scheduled task

The scheduled task is created through a call to the `schtasks.exe` system tool, a native-Windows tool.

The following pseudo-code sums up the structure of the command line as well as the call :

```
// creates the scheduled task
args = "/Create /S " // programs the scheduled task on a remote system
args += remote_computername
```

```
args += " /TN " // name of the scheduled task
args += randalnum(8)
args += " /TR \"" // name of the program to be launch
args += < string manipulation, replacing $ by : >?
args += "\" /sc once /st 00:00 /RL HIGHEST" // launches the task once, at midnight

ShellExecute("open", "SCHTASKS", args);

// attend ~1mn

Sleep(55000)

// then immediatly launches

args = "/S "
args += remote_computername
args += " /Run /TN "
args += rand_taskname

ShellExecute("open", "SCHTASKS", args);
```

Containment

As the malware does not check if a machine has already been infected, no simple system object creation that could prevent infection.

A privileged account of the domain is used for malware propagation.

If this user's password is changed, the replication will continue as long as the Kerberos tickets are not expired. If the user account is disabled, the issue will remain the same

One way to tackle the problem could be to change the password or disable the user account (according to the used account) and then proceed to a double KRBTGT domain password change. This would induce many disturbances on the domain - and most likely require many reboots but would also immediately contain the propagation.

Other propagation containment approaches could also be considered, especially through the targeting of the malware execution environment. They have yet not been tested thus far.

Nota bene: none of these methods could restrain the encryption of an already infected machine.

5.2.5 Encryption

The malware interrupts multiple programs based on hardcoded lists :

- a list of 41 processes to be killed (*task kill*) ;
- and a list of 64 services to stop.

The files are encrypted using Microsoft CryptoAPI with AES256 algorithm.

A unique AES key is generated for each file.

The AES key is wrapped with a RSA public key stored in the binary code.

5.2.6 Scheduled tasks and parameters

Exécution

Multiple propagation scheduled tasks have been observed on the infected machines, executing program binaries stored in C:\Users\Public under a pseudo-random name.

Depending on the infected machines, twenty to more than a hundred of tasks were observed.

Found binaries are named using two types of conventions: `xxxxxxxrep.exe` and `xxxxxxxlan.exe`.

On the compromised systems, we noticed command line executions of the following type :

```
- LAN: xxxxxxxlan.exe 8 LAN
- REP: xxxxxxxrep.exe 9 REP
```

Marqueurs

```
Nom : xxx.exe
Taille : 552960
MD5 : 544900a527328f2e4fe7598985bc688f
SHA-1 : 453d355037fabfc9c200022d189b91310fc2577a
SHA-256 : 2820bf6bb2a2d0670c6233301b414ae293cf85536127ac63b2ebd07d8616ae89
PE timestamp : 2021-02-09 01:28:50 UTC
```

Example of scheduled tasks created by the propagation

```xml
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.1" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
<Author>DOMAINE\administrateur</Author>
</RegistrationInfo>
<Triggers>
<TimeTrigger>
<Enabled>true</Enabled>
<StartBoundary>2021-02-09T00:00:00</StartBoundary>
</TimeTrigger>
</Triggers>
<Settings>
<Enabled>true</Enabled>
<ExecutionTimeLimit>PT259200S</ExecutionTimeLimit>
<Hidden>false</Hidden>
<WakeToRun>false</WakeToRun>
<DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
<StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<Priority>9</Priority>
<IdleSettings>
<Duration>PT600S</Duration>
<WaitTimeout>PT3600S</WaitTimeout>
<StopOnIdleEnd>true</StopOnIdleEnd>
<RestartOnIdle>false</RestartOnIdle>
</IdleSettings>
</Settings>
<Principals>
<Principal id="Author">
<UserId>DOMAINE\administrateur</UserId>
<RunLevel>HighestAvailable</RunLevel>
```

```
<LogonType>InteractiveToken</LogonType>
</Principal>
</Principals>
<Actions Context="Author">
<Exec>
<Command>C:\Users\Public\XkIiKWrgErep.exe</Command>
</Exec>
</Actions>
</Task>
```

List of the 41 killed processes

```
virtual
vmcomp
vmwp
veeam
backup
Backup
xchange
sql
dbeng
sofos
calc
ekrn
zoolz
encsvc
excel
firefoxconfig
infopath
msaccess
mspub
mydesktop
ocautoupds
ocomm
ocssd
onenote
oracle
outlook
powerpnt
sqbcoreservice
steam
synctime
tbirdconfig
thebat
thunderbird
visio
word
xfssvccon
tmlisten
PccNTMon
CNTAoSMgr
Ntrtscan
mbamtray
```

List of the 64 stopped services

```
vmcomp
```

Ryuk ransomware

```
vmwp
veeam
Back
xchange
ackup
acronis
sql
Enterprise
Sophos
Veeam
AcrSch
Antivirus
Antivirus
bedbg
DCAgent
EPSecurity
EPUpdate
Eraser
EsgShKernel
FA_Scheduler
IISAdmin
IMAP4
MBAM
Endpoint
Afee
McShield
task
mfemms
mfevtp
mms
MsDts
Exchange
ntrt
PDVF
POP3
Report
RESvc
sacsvr
SAVAdmin
SamS
SDRSVC
SepMaster
Monitor
Smcinst
SmcService
SMTP
SNAC
swi_
CCSF
TrueKey
tmlisten
UIODetect
W3S
WRSVC
NetMsmq
ekrn
EhttpSrv
```

```
ESHASRV
AVP
klnagent
wbengine
KAVF
mfefire
```

6 Bibliography

[1]   NCSC-UK. *Advisory: Ryuk Ransomware Targeting Organisations Globally*. June 22, 2019.

[2]   Kivu Threat Intelligence. *Kivu Myth Busters: Ryuk vs. North Korea*. Feb. 1, 2019. URL: `https://kivuconsulting.com/kivu-myth-busters-ryuk-vs-north-korea/`.

[3]   Xakep. *Operators of the New Ransomware Ryuk Have Already Earned over $640,000*. Aug. 22, 2018. URL: `https://xakep.ru`.

[4]   Virus Bulletin. *The Long Tail of the Ryuk Malware*. Jan. 1, 2019. URL: `https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-shinigamis-revenge-long-tail-ryuk-malware/`.

[5]   CERT Nazionale Italia. *Il Nuovo Ransomware Ryuk Diffuso in Attacchi Mirati*. Aug. 23, 2018. URL: `https://www.certnazionale.it/news/2018/08/23/il-nuovo-ransomware-ryuk-diffuso-in-attacchi-mirati/`.

[6]   Sophos. *After SamSam, Ryuk Shows Targeted Ransomware Is Still Evolving*. Dec. 18, 2018. URL: `https://nakedsecurity.sophos.com/2018/12/18/after-samsam-ryuk-shows-targeted-ransomware-is-still-evolving/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29`.

[7]   Red Canary. *Detecting Ryuk Ransomware*. Feb. 1, 2020. URL: `https://redcanary.com/blog/ryuk-ransomware-attack/`.

[8]   Crowdstrike. *WIZARD SPIDER Adds New Features to Ryuk*. Nov. 1, 2019.

[9]   Bank Info Security. *Alert: « Ryuk » Ransomware Attacks the Latest Threat*. Sept. 7, 2018. URL: `https://www.bankinfosecurity.com/alert-ryuk-ransomware-attacks-latest-threat-a-11475`.

[10] Github. *Raccine*. Jan. 1, 2020. URL: `https://github.com/Neo23x0/Raccine`.

[11] Coveware. *Ryuk Ransomware Recovery, Payment & Decryption Statistics*. URL: `https://www.coveware.com/ryuk-ransomware`.

[12] Bleeping Computer. *Ryuk Related Malware Steals Confidential Military, Financial Files*. Sept. 11, 2019. URL: `https://www.bleepingcomputer.com/news/security/ryuk-related-malware-steals-confidential-military-financial-files/`.

[13] FireEye. *Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser*. Oct. 28, 2020.

[14] Bloomberg. *Hackers Bearing Down on U.S. Hospitals Have More Attacks Planned*. Oct. 30, 2020. URL: `https://www.bloomberg.com/news/articles/2020-10-30/hackers-bearing-down-on-u-s-hospitals-have-more-attacks-planned`.

[15] Prevailion. *On the Trail of UNC1878*. Nov. 3, 2020. URL: `https://www.prevailion.com/on-the-trail-of-unc1878/`.

[16] FireEye. *A Nasty Trick: From Credential Theft Malware to Business Disruption*. Jan. 11, 2019. URL: `https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html`.

[17] ANSSI. *Le Malware-as-a-Service Emotet*. Oct. 29, 2020.

[18] Intel 471. *Understanding the Relationship between Emotet, TrickBot and Ryuk*. Apr. 14, 2020.

[19] Bleeping Computer. *Emotet-TrickBot Malware Duo Is Back Infecting Windows Machines*. July 20, 2020. URL: `https://www.bleepingcomputer.com/news/security/emotet-trickbot-malware-duo-is-back-infecting-windows-machines/`.

[20] AT&T cybersecurity. *TrickBot BazarLoader In-Depth*. May 19, 2020. URL: `https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-in-depth`.

[21] The DFIR Report. *Ryuk's Return*. Oct. 8, 2020. URL: `https://thedfirreport.com/2020/10/08/ryuks-return/`.

[22] Cybereason. *A Bazar of Tricks: Following Team9's Development Cycles*. July 16, 2020. URL: `https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles`.

[23] Medium. *5 Features Making EmerDNS the Only Truly Decentralized DNS*. Feb. 20, 2020. URL: `https://medium.com/@emer.tech/5-features-making-emerdns-the-only-truly-decentralized-dns-4c513bb13850`.

[24] Advanced-Intel. *"Front Door" into BazarBackdoor: Stealthy Cybercrime Weapon*. Oct. 13, 2020. URL: https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon.

[25] The DFIR report. *Ryuk Speed Run, 2 Hours to Ransom*. Nov. 5, 2020. URL: https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/.

[26] Bleeping Computer. *Hacking Group Is Targeting US Hospitals with Ryuk Ransomware*. Oct. 29, 2020. URL: https://www.bleepingcomputer.com/news/security/hacking-group-is-targeting-us-hospitals-with-ryuk-ransomware/.

[27] Crowdstrike. *"Sin"-Ful SPIDERS: WIZARD SPIDER and LUNAR SPIDER Sharing the Same Web*. Feb. 15, 2019. URL: https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/.

[28] Dell Secureworks. *Evolution of the GOLD EVERGREEN Threat Group*. May 15, 2017. URL: https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group.

[29] Dell Secureworks. *Gold Swathmore*. URL: https://www.secureworks.com/research/threat-profiles/gold-swathmore.

[30] Dell Secureworks. *Gold Blackburn*. URL: https://www.secureworks.com/research/threat-profiles/gold-blackburn.

[31] SANS Internet Storm Center. *InfoSec Handlers Diary Blog - Trickbot*. Dec. 11, 2019. URL: https://isc.sans.edu/diary.html?storyid=25594.

[32] SANS Internet Storm Center. *Emotet Epoch 1 Infection with Trickbot Gtag Mor84*. Jan. 28, 2020. URL: https://isc.sans.edu/forums/diary/25752/.

[33] Twitter. *@cryptolaemus1*. Aug. 26, 2020. URL: https://twitter.com/GossiTheDog/status/1298486442159677440.

[34] AdvIntel. *Anatomy of Attack: Inside BazarBackdoor to Ryuk Ransomware "One" Group via Cobalt Strike*. Nov. 6, 2020. URL: https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike.

[35] FireEye. *STAR Webcast: Spooky RYUKy: The Return of UNC1878*. Oct. 28, 2020. URL: https://www.youtube.com/watch?v=BhjQ6zsCVSc.

[36] FireEye. *"It's Your Money and They Want It Now — The Cycle of Adversary Pursuit"*. Mar. 31, 2020. In: (Mar. 31, 2020).

[37] Twitter. *@anthomsec*. Oct. 29, 2020. URL: https://twitter.com/anthomsec.

[38] Sophos. *Hacks for Sale: Inside the Buer Loader Malware-as-a-Service*. Oct. 28, 2020. URL: https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/.

[39] Infosec Institute. *ZLoader: What It Is, How It Works and How to Prevent It*. Aug. 19, 2020. URL: https://resources.infosecinstitute.com/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/.

[40] FireEye. *Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware*. Apr. 5, 2019. URL: https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html.

[41] Morphisec. *New Global Attack on Point of Sale Systems-FIN6*. Feb. 27, 2019. URL: http://blog.morphisec.com/new-global-attack-on-point-of-sale-systems.

[42] Security Intelligence. *ITG08 (Aka FIN6) Partners with TrickBot Gang, Uses Anchor Framework*. Apr. 7, 2020. URL: https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/.

[43] Bleeping Computer. *Conti Ransomware Shows Signs of Being Ryuk's Successor*. July 9, 2020. URL: https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/.

[44] Malwarebytes Labs. *The Curious Case of Ryuk Ransomware*. Dec. 12, 2019. URL: https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION