SHINIGAMI'S REVENGE: THE LONG TAIL OF THE RYUK MALWARE

Gabriela Nicolao & Luciano Martins
Deloitte, Argentina

{gnicolao, lmartins}@deloitte.com

ABSTRACT

Ryuk is a ransomware family that, unlike regular ransomware, is tied to targeted campaigns where extortion may occur days or weeks after an initial infection. Ryuk was first observed in August 2018 and remains active as of July 2019.

Among its victims we find companies from different industries, including newspapers, restaurants, public institutions, and a cloud service provider. Ryuk has been observed as a second-stage payload delivered in campaigns that involved Emotet and Trickbot, two of the most widespread threats that are currently being used in malware campaigns.

Ryuk bears a strong code resemblance to the Hermes ransomware, and was likely developed and possibly distributed by the same threat actor(s). The code similarities found between Ryuk and Hermes – a payload that was allegedly linked to North Korean threat actors – led analysts initially to suspect that Ryuk was affiliated with the infamous Lazarus APT (Advance Persistent Threat) group. However, that attribution was discarded based on evidence that was collected from a dark web forum and the malware was later attributed to Russian-speaking actors possibly known as Grim Spider. This paper will review Ryuk's technical aspects and its evolution since its appearance.

ABOUT RANSOMWARE

Ransomware is a piece of software that denies access to a computer or data until an amount of money (a ransom) is paid. Ransomware variants include crypto-ransomware, which can encrypt files or even an entire disk; locker-ransomware, which also goes under the name of the police virus or support scammers; scareware, which pretends to encrypt files without actually doing it; and wipers, which are crypto-ransomware that encrypt files with a key that cannot be retrieved.

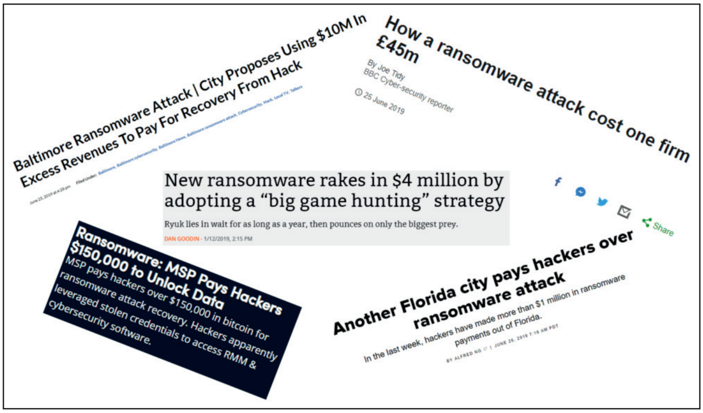
After an infection, ransomware usually displays a file known as a ransom note, which contains payment instructions that the victim of the infection must follow in order to recover access to the information that was denied.

TARGETED RANSOMWARE

Between 2016 and 2017 we observed an enormous growth in ransomware, where new variants and/or families were found on almost a daily basis.

In 2018, there was a significant decrease in ransomware attacks. However, that didn't mean that ransomware stopped being a threat, it just meant that ransomware became quieter and more targeted. Instead of using massive email campaigns, ransomware started to be delivered via RDP (Remote

Desktop Protocol). We can see this trend in ransomware families including SamSam, MegaCortex, LockerGoga, Dharma, BitPaymer and Ryuk.



Baltimore Ransomware Attack | City Proposes Using $10M In Excess Revenues To Pay For Recovery From Hack

June 25, 2019 at 4:28 pm Filed Under: Baltimore, Baltimore cybersecurity, Baltimore News, Baltimore ransomware attack, Cybersecurity, Hack, Local TV, Talkers

How a ransomware attack cost one firm £45m

By Joe Tidy
BBC Cyber-security reporter

25 June 2019

New ransomware rakes in $4 million by adopting a "big game hunting" strategy

Ryuk lies in wait for as long as a year, then pounces on only the biggest prey.

DAN GOODIN - 1/12/2019, 2:15 PM

Ransomware: MSP Pays Hackers $150,000 to Unlock Data

MSP pays hackers over $150,000 in bitcoin for ransomware attack recovery. Hackers apparently leveraged stolen credentials to access RMM & cybersecurity software.

Another Florida city pays hackers over ransomware attack

In the last week, hackers have made more than $1 million in ransomware payments out of Florida.

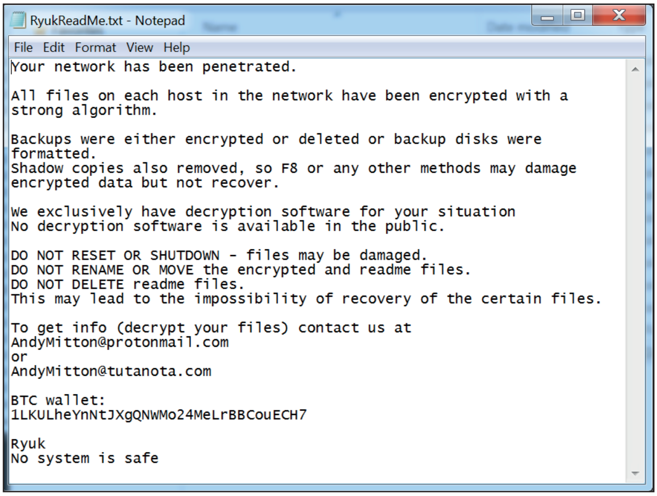
BY ALFRED NG | JUNE 26, 2019 7:16 AM PDT

Figure 1: Victims paying ransom fees often make the news headlines.

The news headlines in Figure 1 showing that victims are paying to recover their files confirm that ransomware remains a profitable threat – particularly when threat actors modify their approach to a more targeted campaign.

RYUK CHRONOLOGY

Ryuk is a crypto-ransomware that was first mentioned in a Tweet on 17 August 2018. It used 'RyukReadMe.txt' as a ransom note, hence the name. Ryuk is also the name of a fictional character known as Shinigami (God of Death) in a manga and anime series called *Death Note*.



```
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.
Shadow copies also removed, so F8 or any other methods may damage
encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

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

To get info (decrypt your files) contact us at
AndyMitton@protonmail.com
or
AndyMitton@tutanota.com

BTC wallet:
1LKULheYnNtJXgQNWMo24MeLrBBCouECH7

Ryuk
No system is safe
```

Figure 2: Ryuk ransom note from file cb0c1248d3899358a375888bb4e8f3fe.

At the time Ryuk was first reported, it had already hit three companies in different countries, and researchers pointed out that Ryuk was based on the infamous Hermes ransomware's source code and that it used the same ransom note format as BitPaymer.

The Hermes ransomware was used by Lazarus, a North Korean-sponsored threat actor group active since 2009. Due to the attribution of Hermes to Lazarus, researchers believed that Ryuk was also related to Lazarus.

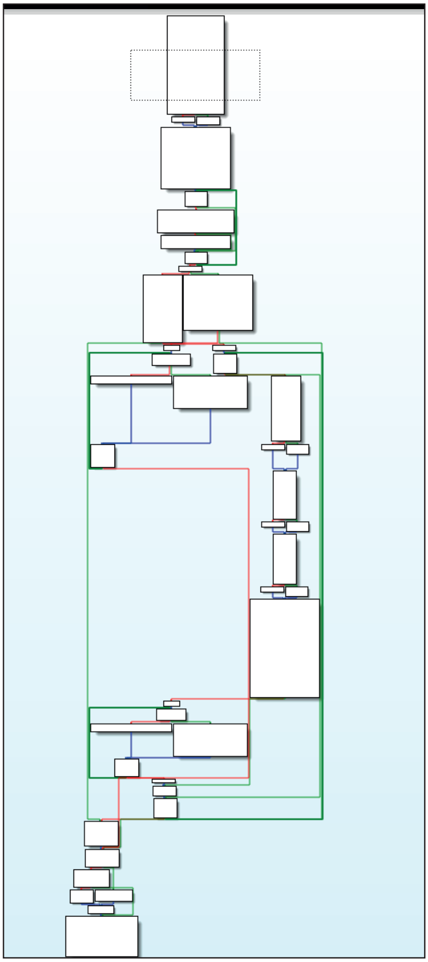
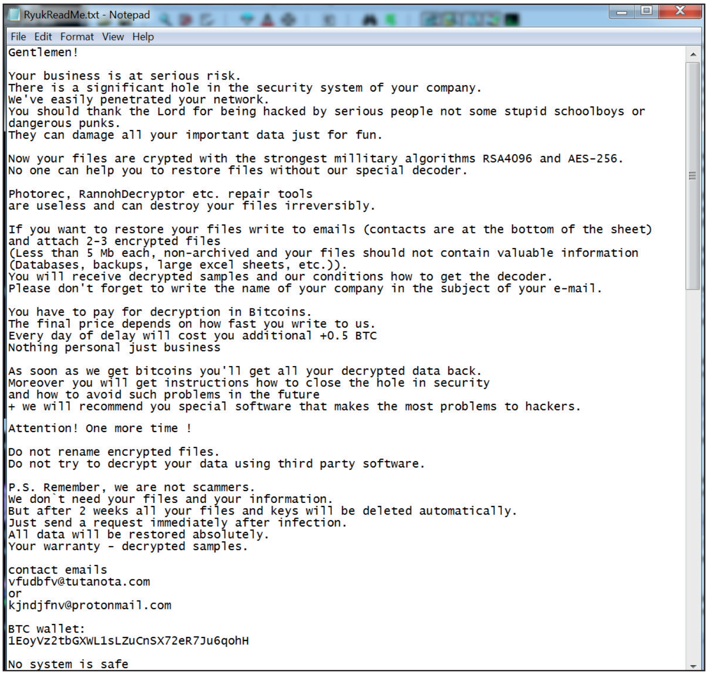


Figure 3: Hermes (code flow).

Victims

- In October 2018, Ryuk was used to infect a Canadian restaurant chain and a water and sewer authority in the USA. This last attack was delivered using Emotet, a banking trojan that evolved into a modular threat that delivers and runs other malware on the victim's machines.

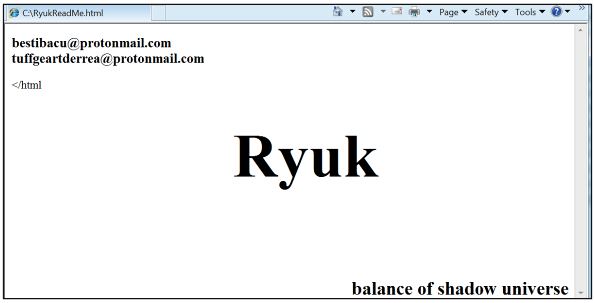
- In December 2018, Ryuk was used in an attack against the *Tribune Publishing* group that caused the disruption of the printing and delivery of newspapers in the USA. In addition, a US-based cloud-hosting provider was hit with Ryuk on Christmas Eve, affecting its service.
- In March 2019, the Jackson County email system was taken down after being compromised with Ryuk.



```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or
dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don`t need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
vfudbfv@tutanota.com
or
kjndjfnv@protonmail.com

BTC wallet:
1EoyVz2tbGXWL1sLZuCnSX72eR7Ju6qohH

No system is safe
```

Figure 4: Ryuk ransom note from file d4a7c85f23438de8ebb5f8d6e04e55fc.

In January 2019, Ryuk's supposed attribution to North Korea was discarded, based on the fact that Hermes code was offered in underground forums, and was attributed instead to Grim Spider. Grim Spider is suspected to be a cell of WIZARD SPIDER, a Russian-based group that spreads Trickbot, another banking trojan that evolved into a modular threat and was focused on wire fraud.



bestibacu@protonmail.com
tuffgeartderrea@protonmail.com

</html

Ryuk

balance of shadow universe

Figure 5: Ryuk ransom note from file b2b1e8ac6e211d0093fd0a3ae12001a8.

In April 2019, threat actor FIN6 was found to be using the LockerGoga ransomware and Ryuk in an attack against a company within the engineering industry. In addition, a campaign using Emotet to download Trickbot was observed delivering Ryuk.

In June 2019, Ryuk added an IP blacklist to avoid infecting hosts that had particular IP addresses.

Based on bitcoin transactions, we calculate that the threat actors behind Ryuk have been paid almost US$4 million since August 2018.

TECHNICAL ASPECTS

Ryuk is sold as a toolkit for threat actors that want to build their own malware. This means that there are as many variants as there are threat actors who bought the code to generate their binaries.

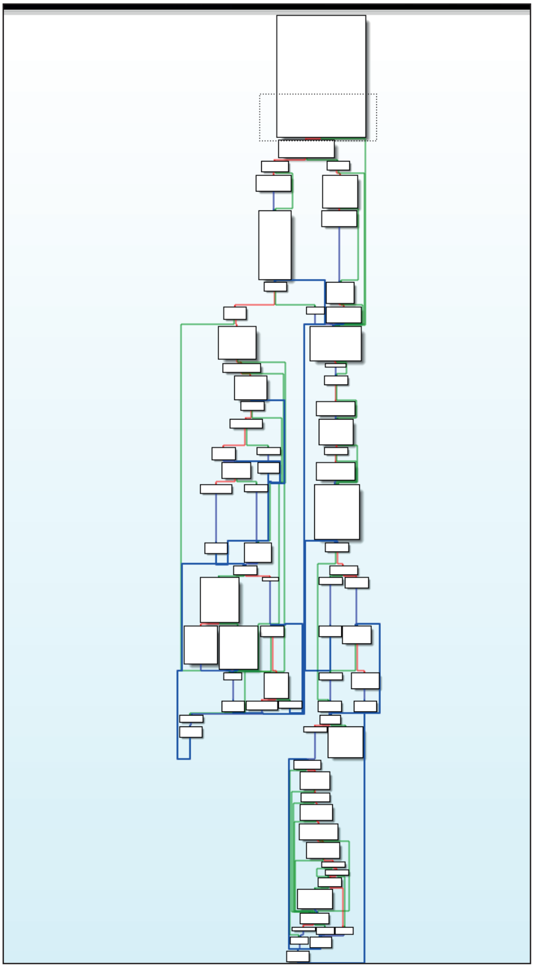


Figure 6: Ryuk (code flow).

Most of the binaries are 64-bit, and only a few are 32-bit. After executing Ryuk samples that had different but similar PDB strings, these are the main characteristics we found:

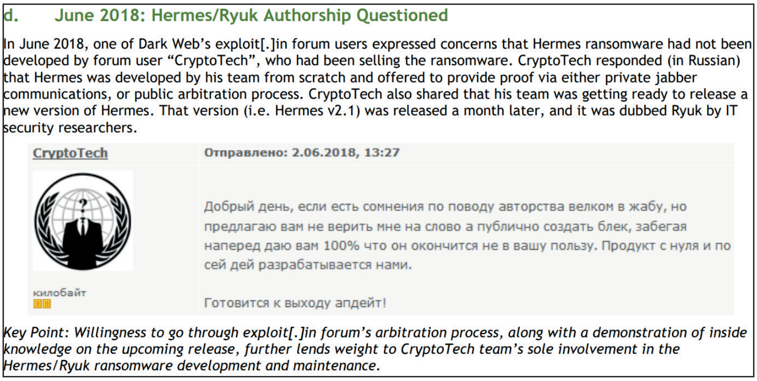
- Samples remove shadow copies and backups. One of the samples that was executed (MD5: cb0c1248d3899358a375888bb4e8f3fe) created a file called windows.bat in the 'C:\users\Public' folder to delete the shadow copies and backups. Other samples include the deletion of shadow copies and backup within their code.
- Some of the samples modify the Run registry key, adding the value 'svchos' and the path to the executable.
- Some of the samples encrypt the boot manager, which causes the machine to be unable to boot.
- Some of the samples (for example MD5: d4a7c85f23438de8ebb5f8d6e04e55fc) claim that files are encrypted using RSA4096 + AES 256.
- All analysed samples check for Russian, Ukrainian and Belarusian languages – if these are found, the sample exists without encrypting files.
- All analysed samples added the string 'HERMES' to the encrypted files.
- Ransom notes are called 'RyukReadMe.txt' or 'RyukReadMe.html'. Some contain a BTC address, and some don't, but all contain two emails to contact the threat actors.
- Some of the samples append .RYK to encrypted files, some do not append any extension.
- One of the samples (MD5: 3895a370b0c69c7e23ebb5ca1598525d) drops a file with a random name in the 'C:\Users\Public' folder (MD5: 567407d941d99abeff20a1b836570d30). This file is a deobfuscated version of Ryuk.
- Samples contain a list of services and processes that they will try to stop or kill. The list of services and processes has grown over time. One of the samples (MD5: 567407d941d99abeff20a1b836570d30) contains 184 services and 44 processes. The services are related to AV companies, backup, SQL and others. The processes are related to email services, word processors and others.
- One of the samples (MD5: c0d6a263181a04e9039df3372afb8016) checks for the following to avoid infection: 'SPB', 'Spb', 'spb', 'MSK', 'Msk' or 'msk' computer names, '10.30.4', '10.30.6' (repeated), '10.30.5' or '10.31.32' IP addresses.

ATTRIBUTION

Ryuk was first attributed to the North Korean APT group Lazarus because of code similarities shared with the Hermes ransomware.

A few months later, that theory was discarded as the Hermes ransomware's code was found being offered in underground forums by a Russian-speaking actor, which means that any threat actor could have modified the code to create Ryuk.

Ryuk was also attributed to a threat actor or group that use the handle 'CryptoTech', who claimed on the dark web forum exploit[.]in that they had developed Hermes and that they were going to release a new version. A month later, a new modified version of Hermes started to appear, which fits the timeframe for the new release mentioned by CryptoTech. This modified version is Ryuk.



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.

CryptoTech

Отправлено: 2.06.2018, 13:27

Добрый день, если есть сомнения по поводу авторства велком в жабу, но предлагаю вам не верить мне на слово а публично создать блек, забегая наперед даю вам 100% что он окончится не в вашу пользу. Продукт с нуля и по сей дей разрабатывается нами.

Готовится к выходу апдейт!

килобайт

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.

Figure 7: CryptoTech claimed they had developed Hermes.

CryptoTech defended themselves in Russian and announced in June 2018 that they would release a new version of Hermes.

Ryuk has also been attributed to Grim Spider, which consists of a single group or group of smaller groups that rent Trickbot on an access-as-a-service basis to deliver Ryuk.

HERMES AND RYUK TIMELINE

We collected almost 600 samples of both Hermes and Ryuk to try to determine a relationship between the two malware families.

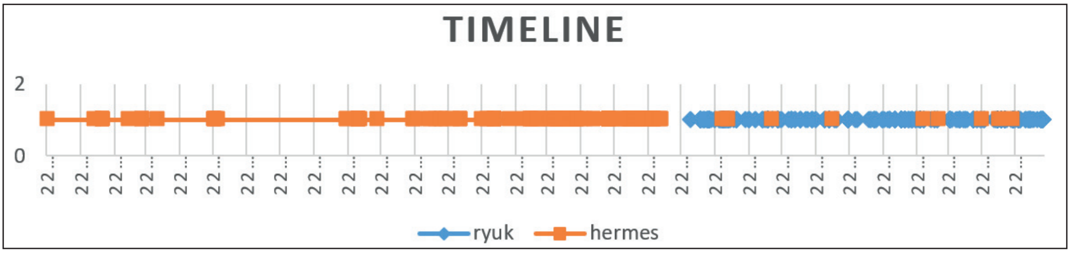


Figure 8: Hermes and Ryuk timeline.

The chart in Figure 8 represents when each of the samples was compiled. Between June and July 2018 there was a cessation of Hermes activities and then Ryuk appeared. That time fits the moment in which the user with the handle CryptoTech defended against accusations that they were selling Hermes without being its developer.

CONCLUSION

Ryuk continues to be an active threat, as newer versions of this family continue to be released. The new version of Ryuk released in June 2019 did not have any significant changes in terms of ransomware infection code or file encryption compared to the previous one. The core functionality remained unchanged while adding features to avoid detection.

After Ryuk emerged, CryptoTech went quiet on a highly vetted Russian-speaking cybercriminal forum, while in the past they had posted advertisements in both English and Russian.

In March 2019, Ryuk ransomware infected the machines of Rural Jackson County, Georgia. It was stated that the county paid $400,000 in ransom. These types of high payouts are likely to encourage threat actors to conduct more campaigns delivering Ryuk and other targeted ransomware.

RECOMMENDATIONS

- Do not rely on payment of ransom as a way to recover encrypted files from ransomware incidents, as threat actor(s) may be unwilling or unable to decrypt them after they receive payment. Also, ransom payments will encourage and finance future attacks.
- Implement Access Control (AC) and Identity Access Management (IAM) in order to limit network privileges and shared drive permissions to contain endpoint ransomware infections. Grant users the minimum local privileges that they need in their roles.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization's email environment.
- Adopt a layered security stack with defences and protection technologies deployed from the perimeter and inwards onto each host on your network.
- Use frequent, tested, segmented, and redundant backups to recover files from ransomware infections.
- Perform regular remote and local offline backups of sensitive data and conduct periodic review and validation of server backup processes.
- Verify that backups are not attached to potentially infected systems. Backup copies of sensitive data should not be readily accessible from local networks.
- Maintain incremental backups of all sensitive and proprietary data. Practise the 3-2-1 rule: create three backup copies on two different media sources with one copy stored offsite (local offline backup).

IOCS

The following files were detonated and analysed for this paper:

cb0c1248d3899358a375888bb4e8f3fe (PDB string: c:\users\admin\documents\visual studio 2015\projects\consoleapplication54\x64\release\consoleapplication54.pdb)

3895a370b0c69c7e23ebb5ca1598525d (PDB string: c:\users\admin\documents\visual studio 2015\projects\consoleapplication54new\x64\release\consoleapplication54.pdb)

d4a7c85f23438de8ebb5f8d6e04e55fc (PDB string: c:\users\admin\documents\visual studio 2015\projects\consoleapplication_54\x64\release\consoleapplication54.pdb)

df2584b96ede0e676bc488edeaf3ebbd (PDB string: c:\users\admin\documents\visual studio 2015\projects\consoleapplication54new crypted\x64\release\consoleapplication54.pdb)

958c594909933d4c82e93c22850194aa (PDB string: c:\users\admin\documents\visual studio 2015\projects from ryuk\consoleapplication54\x64\release\consoleapplication54.pdb)

70d26f34f324c21aa4ec6a9977f24c0e (PDB string: c:\users\admin\documents\visual studio 2015\projects\consoleapplication54new crypted try to clean\x64\release\consoleapplication54.pdb)

beccb227b0c2661c5ecfcfc9458e6253 (PDB string: c:\users\admin\documents\visual studio 2015\projects\consoleapplication54new crypted with process kill in another process\x64\release\consoleapplication54.pdb)

b2b1e8ac6e211d0093fd0a3ae12001a8 (PDB string: c:\users\admin\documents\visual studio 2015\projects\consoleapplication54new crypted with process kill in another process static buffer\x64\release\consoleapplication54.pdb)

b73d6af47bd63b87953279100d7baa00 (PDB string: c:\users\admin\documents\visual studio 2015\projects\consoleapplication54new process kill, static buffer, big data\x64\release\consoleapplication54.pdb)

c5f70c5197cdd350decc28cdc5498b20 (no PDB string)

REFERENCES

[1] US CERT. Ransomware. https://www.us-cert.gov/Ransomware.

[2] Hahn, K. Ransomware identification for the judicious analyst. G Data. 12 June 2019. https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst.

[3] MalwareHunterTeam. Twitter. 17 August 2018. https://twitter.com/malwrhunterteam/status/1030529747174998016.

[4] Cimpanu, C. Canadian restaurant chain suffers country-wide outage after malware outbreak. ZDNet. 2 October 2018. https://www.zdnet.com/article/restaurant-chain-suffers-canada-wide-outage-after-malware-outbreak/.

[5] Malwarebytes. Let's talk Emotet malware. https://www.malwarebytes.com/emotet/.

[6] Onwasa. Cyber-Criminals target critical utility in Hurricane-ravaged area. 15 October 2018. https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A.

[7] Ilascu, I. Ryuk Ransomware Involved in Cyberattack Stopping Newspaper Distribution. Bleeping Computer. 31 December 2018. https://www.bleepingcomputer.com/news/security/ryuk-ransomware-involved-in-cyberattack-stopping-newspaper-distribution/.

[8] Office of the CIO. HC3 Threat Intelligence Briefing Ryuk Ransomware. US Department of Health and Human Services. 30 August 2018. https://assets.documentcloud.org/documents/4829428/TLPWhite-20180830-Ryuk-Hermes-Ransomware.pdf.

[9] Fokker, J.; Beek, C. Ryuk Ransomware Attack: Rush to Attribution Misses the Point. McAfee. 9 January 2019. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/.

[10] Hanel, A. Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware. CrowdStrike. 10 January 2019. https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.

[11] Buchanan, C. Ransomware attack targets rural Georgia county. 11Alive. 6 March 2019. https://www.11alive.com/article/tech/ransomware-attack-targets-rural-georgia-county/85-2d6459e7-bd16-4cf9-b9fb-b03108a25144.

[12] Cybereason. A one-two punch of Emotet, Trickbot, & Ryuk stealing & ransoming data. 2 April 2019. https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data.

[13] Abrams, L. Ryuk Ransomware Adds IP and Computer Name Blacklisting. BleepingComputer. 10 June 2019. https://www.bleepingcomputer.com/news/security/ryuk-ransomware-adds-ip-and-computer-name-blacklisting/.

[14] Kivu Consulting. Kivu Myth Busters: Ryuk vs. North Korea. 1 February 2019. https://kivuconsulting.com/wp-content/uploads/2019/03/Kivu-Threat-Intelligence-2.1.19-2.pdf.

[15] Ng, A. Another Florida city pays hackers over ransomware attack. CNET. 26 June 2019. https://www.cnet.com/news/another-florida-city-pays-hackers-over-ransomware-attack/.

[16] Tidy, J. How a ransomware attack cost one firm £45m. BBC. 25 June 2019. https://www.bbc.com/news/business-48661152.

[17] Panettieri, J. Ransomware: MSP Pays Hackers $150,000 to Unlock Data. MSSP Alert. 25 June 2019. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/msp-pays-150000-to-recover-data/.

[18] Goodin, D. New ransomware rakes in $4 million by adopting a ‘big game hunting’ strategy. Arstechnica. 1 December 2019. https://arstechnica.com/information-technology/2019/01/new-ransomware-rakes-in-4-million-by-adopting-a-big-game-hunting-strategy/.

[19] CBS Baltimore. Baltimore Ransomware Attack | City Proposes Using $10M In Excess Revenues To Pay For Recovery From Hack. 25 June 2019. https://baltimore.cbslocal.com/2019/06/25/baltimore-ransomware-attack-excess-revenues-cover-costs-to-recover-from-hack/.