

Shinigami's revenge: the long tail of Ryuk malware

Deloitte.



GABRIELA NICOLAO
LUCIANO MARTINS



@rove4ever



@clucianomartins

virus
BULLETIN

ABOUT US

Cyber Threat Intelligence at Deloitte

- ✓ Argentina Team
- ✓ Conference Speakers
- ✓ Malware Analysis
- ✓ APT Hunting



GABRIELA NICOLAO



LUCIANO MARTINS



ABOUT RANSOMWARE

YOU ARE HACKED

PERSONAL FILES HAVE BEEN ENCRYPTED!

TO RESTORE YOUR DATA YOU HAVE TO PAY!

ransomsupport@gmail.com

**YOU CAN'T RESTORE YOUR DATA
DECRYPTOR!!!!!!!!!!!!!!!!!!!!**

I want to play a game with you. Let me explain the rule
Your personal files and folders deleted. You're trapped. If
you don't comply I'll delete every thing on your drive. I can
recover. I've already encrypted your personal files. So
every time I select some of them to delete you.



TARGETED RANSOMWARE

- ✓ Samsam
- ✓ MegaCortex
- ✓ Lockergoga
- ✓ Bit Paymer
- ✓ Ryuk
- ✓ Sodinokibi (REvil)

Gentlemen,
Your business is a serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network, a
you should thank the Lord for being hacked by serious people not some stupid schoolboy.
They can damage all your important data just for fun.
Now your files are encrypted with the strongest military algorithms RSA4096 and AES-256
No one can help you to restore your files without our special decoder.
Photorec, RannohDecryptor etc. recovery tools
are useless and can destroy your files irreversibly.
If you want to restore your files write us emails (contacts are at the bottom of the s
and attach 2-3 encrypted files. Archived and your files should not contain valuable informat
(Less than 5 Mb each, not excel sheets, etc.)
(Databases, backups, excel sheets, etc.)
You will receive decrypted samples and our instructions 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 files 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
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com
BTC wallet:
15RLwDvny5n1n7mTvU1zjg67wt86dhvqNj
Ryuk
No system is safe

...een found wanting.
...rypted your files.
...software.
...y they are useless.
...er back on.
...file('s)
...s.
...s.

README-NOW.txt - Notepad
File Edit Format View Help
There was a significant flaw in the security system of your company. You should be thankful that the flaw was exploited by us. They would have damaged all of your data by mistake.
Your files are encrypted with the strongest military algorithms. Without our special decoder it is impossible to restore your files. Attempts to restore your data with third party software will lead to irreversible destruction of your data.
To confirm our honest intentions. Send us 2-3 different random files and you will get 2-3 files back. It can be from different computers in your network. Sample files we unlock for free. Files should not contain valuable information.
We exclusively have decryption software for your files. DO NOT RESET OR SHUTDOWN your computer. 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 your files.
To get information on the price of the decoder contact us at CottleZehyco1994@o2.pl. The payment has to be in Bitcoins. The final price depends on how fast you contact us. AS soon as we get bitcoins you will get all your decrypted files back. Moreover you will get instructions how to close the hole in your systems security and how to avoid such problems in the future.

ABOUT RYUK

- August 2018.
- Targeted campaigns: Newspapers, restaurant, public institutions, cloud service provider, public institutions.
- Used along with other threats.
- Attributed to different threat actors.
- Sold in underground forums as a toolkit.



ABOUT RYUK



National Cyber
Security Centre
a part of GCHQ

Advisory: Ryuk ransomware targeting organisations globally

Source: <https://s3.eu-west-1.amazonaws.com/ncsc-content/files/RYUK%20Advisory%20draft%20CP%20June%202019.pdf>

TECHNICAL ASPECTS

1

Remove shadow copies and backups (T1490)

2

Some variants modify Run registry key (T1060).

3

Some variants encrypt the boot manager. (T1486)

4

Some variants claim to encrypt files using RSA4096+AES256 (T1486)

5

All variants added string HERMES to encrypted files.

6

Ransom notes contain two emails to contact Threat actors.

7

Some variants append RYK to encrypted files. Some don't append any extension (T1042)

8

Contain a list of services and processes to stop/kill (T1489)

9

Avoids to infect systems in Russian, Ukrainian and Belarusian languages.

RUYK CHRONOLOGY

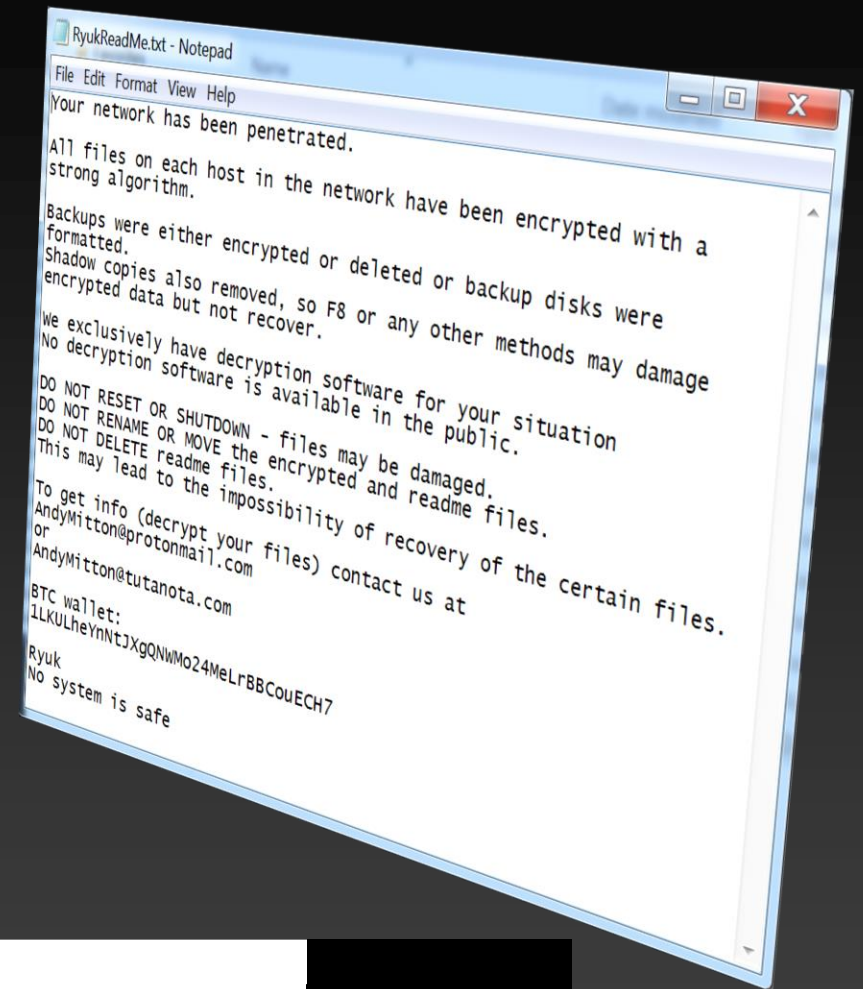
2018



DISCOVERY

On August 17, 2018, Ryuk was mentioned in a tweet..

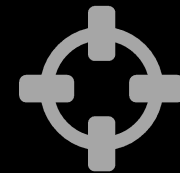
August

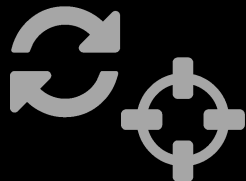


October

TARGETS

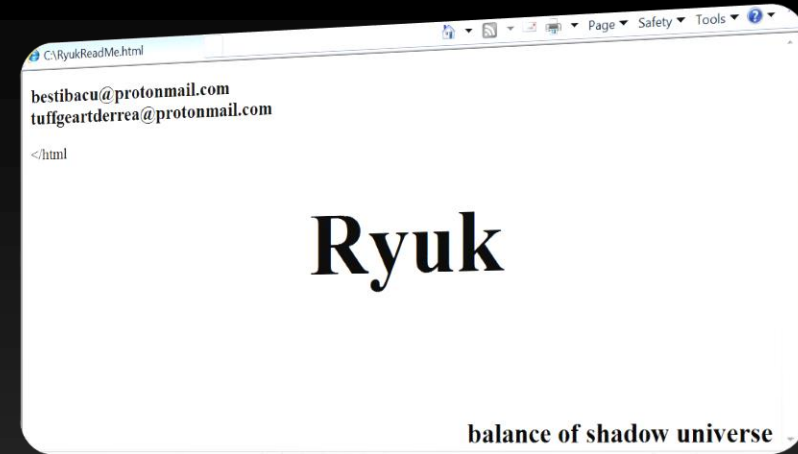
Ryuk infected a Canadian restaurant chain and a water and sewer authority in US





UPDATE & TARGET
Removed BTC wallet.
Tribune Publishing group and
Cloud hosting provider in the US.

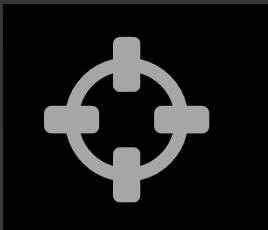
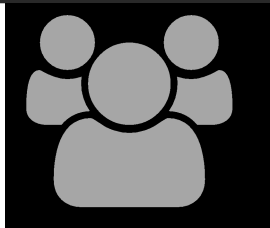
December



2019

January

ATTRIBUTION
From North Korea to GRIM
SPIDER.



TARGET
Jackson County email system
compromised

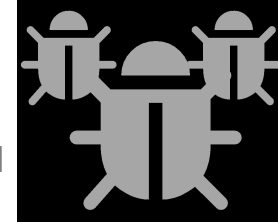
March

**4 MILLION
USD**

April

TRIPLE THREAT

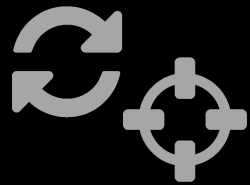
EMOTET+TRICKBOT+RYUK.
FIN6 delivered LockerGoga and
Ryuk



June

UPDATE & TARGET

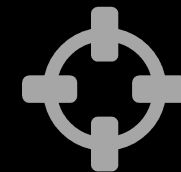
IP Blacklist feature
Bonfiglioli Riduttori italian
Company compromised



July


TARGET

LaPorte County pays \$130,000
to recover from Ryuk attack



2020

RANSON BARGAIN

 **[REDACTED]** 2
manwindhatti <manwindhatti@protonmail.com>

To: **[REDACTED]**

To unlock files, you need to pay 1500 btc.

To confirm our honest intentions, we will unlock two files for free.
Send us 2 different random files and you will get it back already decrypted.
You can choose files from different computers on your network - so you will be sure that one key decrypts everything.
Files size should not exceed 5Mb.

Waiting for 1500 btc to close the problem. Then you will receive decryption software that would completely recover all your files.
It's simple windows executable that needs Administrator privileges to be used. The cure procedure contains next steps:

- 1) Turn off any AV running;
- 2) Turn off internet connection (it will help to avoid any improper decryption - question of your safety);
- 3) Start that exe on each workstation or server; wait for it's prompt that "operation complete" (it takes time depending on amount of data on current system)
- 4) Check that all is fine and get back to normal work.

 **[REDACTED]** 2
manwindhatti <manwindhatti@protonmail.com>

To: **[REDACTED]**

1320 btc 1500+ network server

 **[REDACTED]** 2
manwindhatti <manwindhatti@protonmail.com>

To: **[REDACTED]**

1320 btc

RANSOM BARGAIN

Ransomware gang wanted \$5.3 million from US city, but they only offered \$400,000

New Bedford officials decide to restore from backups after negotiations fail.



By [Catalin Cimpanu](#) for [Zero Day](#) | September 4, 2019 -- 23:58 GMT (00:58 BST) | Topic: [Security](#)

Source: <https://www.zdnet.com/article/ransomware-gang-wanted-5-3-million-from-us-city-but-they-only-offered-400000/>

RYUK
AVERAGE
PRICE

82 BTC
674,039 USD

ONE WALLET MULTIPLE CAMPAIGNS

2019

March

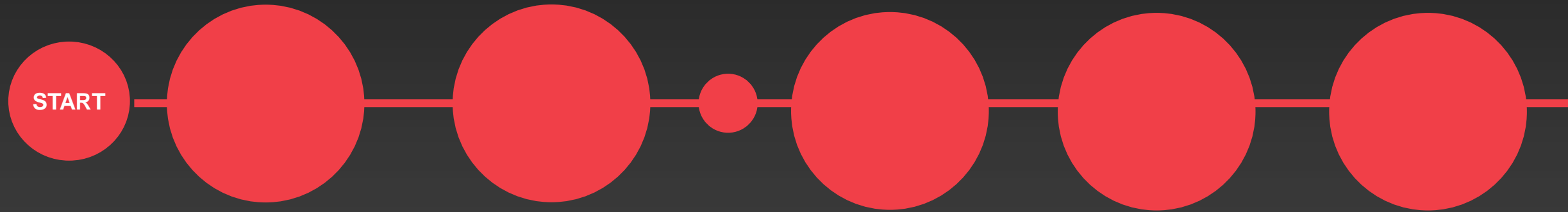
April

May

June

July

August



START

Giernothcarvell91@protonmail.com
amoreeTapaoan94@protonmail.com

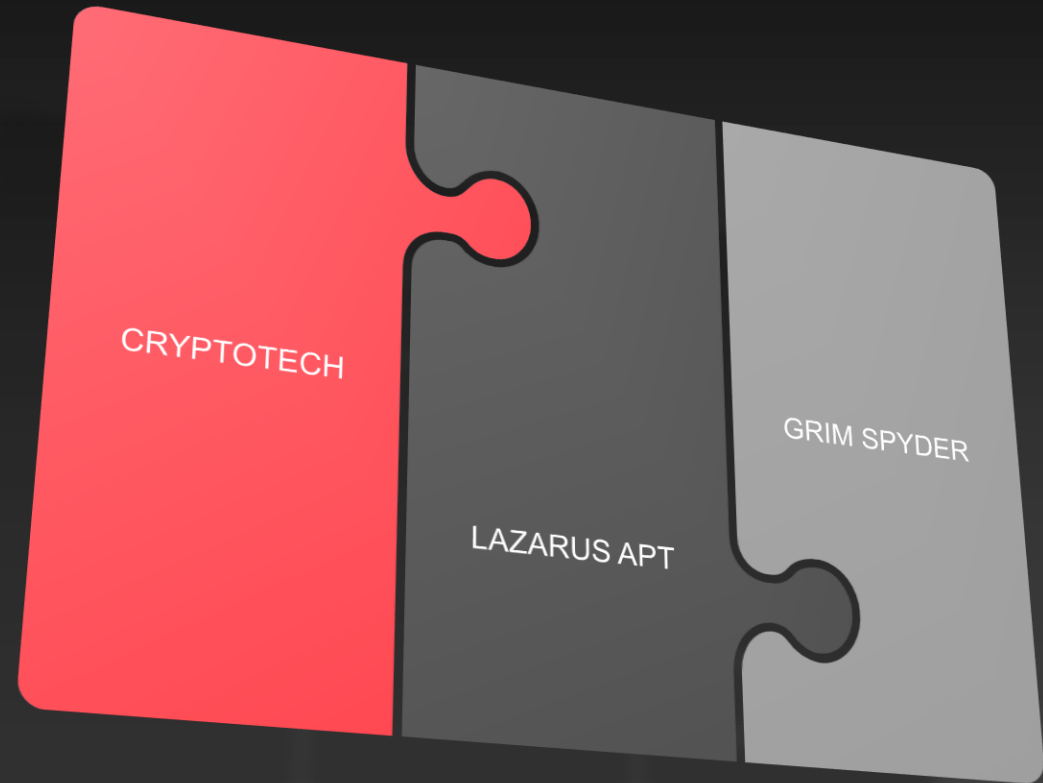
SolayaMatheny96@protonmail.com
TaralynKeels@protonmail.com

disdystkotmo@protonmail.com
ReisertEleonore@protonmail.com
anstandestbrem@protonmail.com

MaddouxKomara@protonmail.com
sledsivodetr1977@protonmail.com
necnuachaba1976@protonmail.com

stalsurniagwar1970@protonmail.com

WHO IS BEHIND RYUK?



WHO IS BEHIND 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



килобайт
■■■

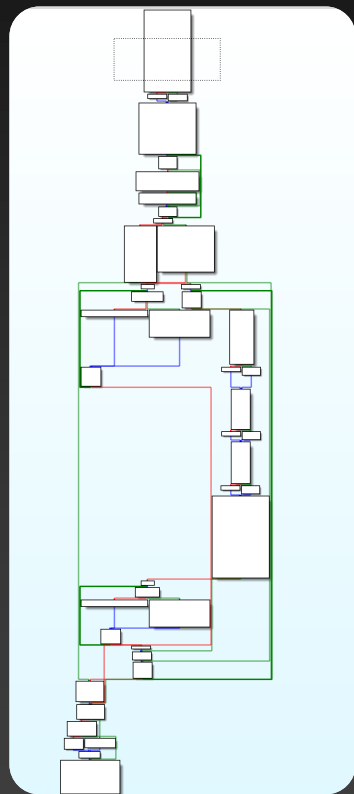
Добрый день, если есть сомнения по поводу авторства велком в жабу, но предлагаю вам не верить мне на слово а публично создать блек, забегая наперед даю вам 100% что он окончится не в вашу пользу. Продукт с нуля и по сей дей разрабатывается нами.

Готовится к выходу апдейт!

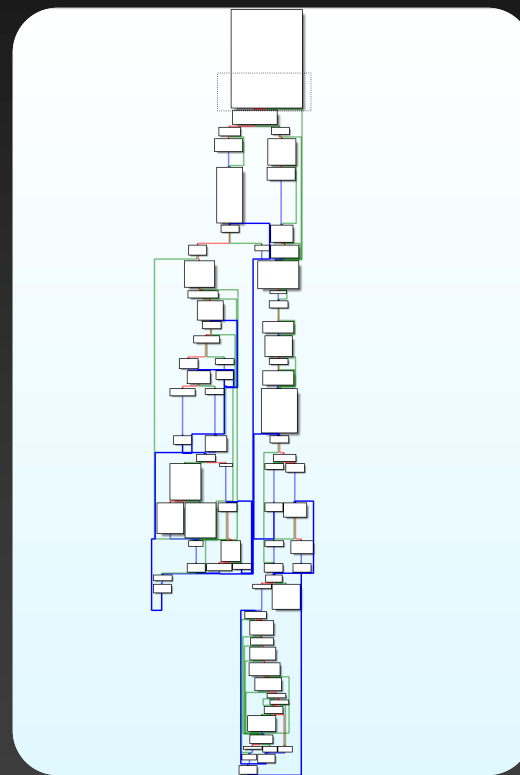
Key Point: Willingness to go through exploit[.]in forum's arbitration process, along with a demonstration of inside knowledge on the upcoming release, further lends weight to CryptoTech team's sole involvement in the Hermes/Ryuk ransomware development and maintenance.

Source: <https://kivuconsulting.com/wp-content/uploads/2019/03/Kivu-Threat-Intelligence-2.1.19-2.pdf>

WHO IS BEHIND RYUK?



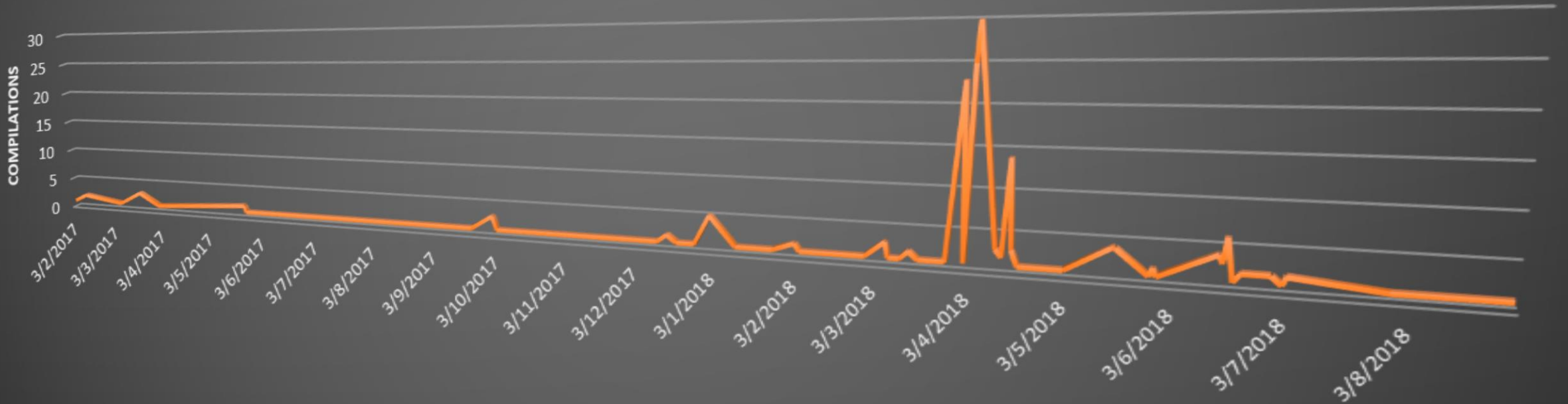
HERMES



RYUK

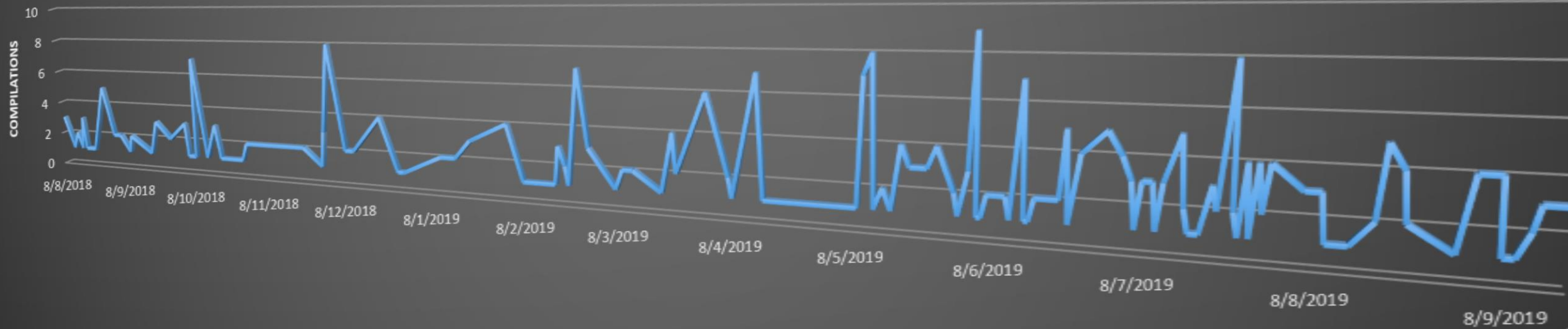
HERMES TIMELINE

Hermes

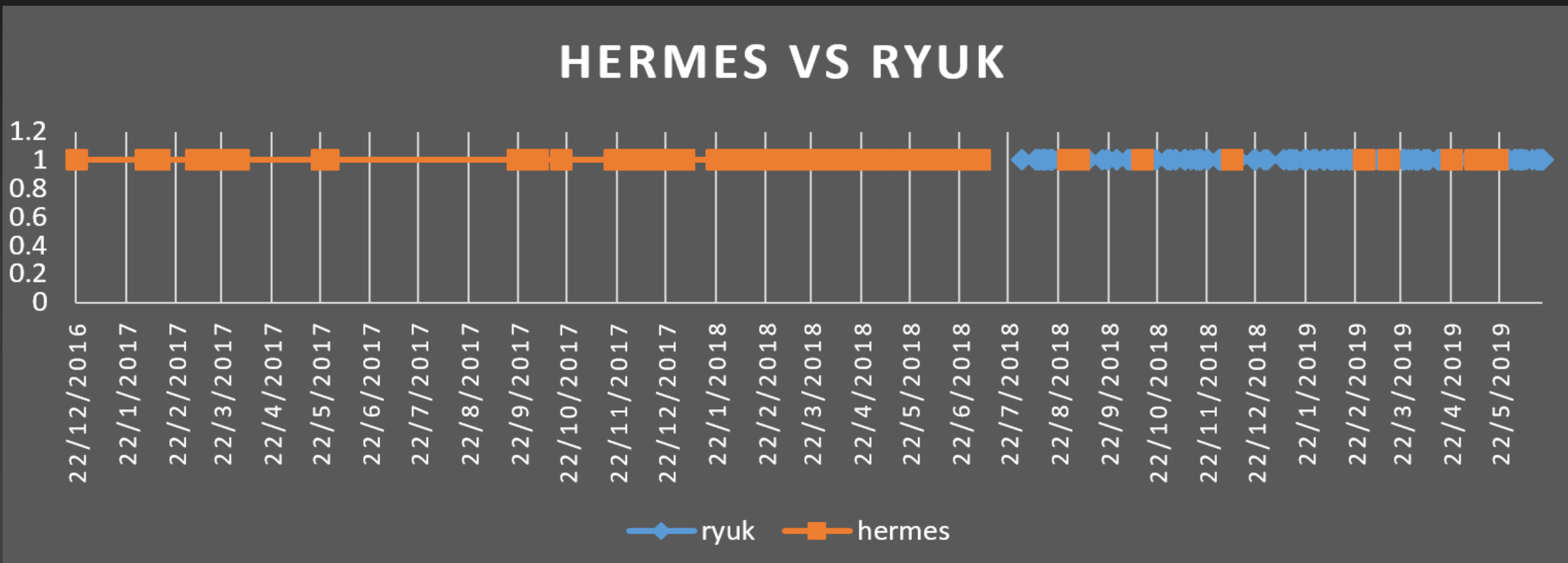


RYUK TIMELINE

Ryuk



HERMES AND RYUK TIMELINE



CONCLUSIONS

- Ryuk continues to be an active threat as threat actors using Ryuk are releasing newer versions of this family. The newer version of Ryuk released in June 2019 does not have any significant changes in terms of ransomware infection code or file encryption compared to the previous one. The core functionality remains unchanged while adding features to avoid detections
- The more you pay, the more attacks they will be:
 - Ryuk ransomware infected machines of Rural Jackson County, Georgia, in March 2019. It was stated that the county paid \$400,000.
 - In June, 2019, Ryuk obtained more than \$1 million dollars from Florida.
 - These type of high payouts will probably encourage threat actors to perform more campaigns delivering Ryuk and other targeted ransomware

RECOMMENDATIONS

01

DON'T PAY!

Threat actor(s) may be unwilling or unable to decrypt them after they receive payment.

02

IMPLEMENT CONTROLS

Implement AC and IAM to limit network privileges
Grant minimum local privileges

03

CATEGORIZE DATA

Sensitive research or business data should not reside in the same server

04

BACKUPS

Use frequent, tested, segmented and redundant backups. Perform remote and local offline backups

**THANKS FOR
WATCHING**

QUESTIONS?

