Ryuk Ransomware Attack: Rush to Attribution Misses the Point

securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/

January 9, 2019

Senior analyst Ryan Sherstobitoff contributed to this report.

During the past week, an outbreak of Ryuk ransomware that impeded newspaper printing services in the United States has garnered a lot of attention. To determine who was behind the attack many have cited past research that compares code from Ryuk with the older ransomware Hermes to link the attack to North Korea. Determining attribution was largely based on the fact that the Hermes ransomware has been used in the past by North Korean actors, and code blocks in Ryuk are similar to those in Hermes.

The McAfee Advanced Threat Research team has investigated this incident and determined how the malware works, how the attackers operate, and how to detect it. Based on the technical indicators, known cybercriminal characteristics, and evidence discovered on the dark web, our hypothesis is that the Ryuk attacks may not necessarily be backed by a nation-state, but rather share the hallmarks of a cybercrime operation.

How McAfee approaches attribution

Attribution is a critical part of any cybercrime investigation. However, technical evidence is often not enough to positively identify who is behind an attack because it does not provide all the pieces of the puzzle. Artifacts do not all appear at once; a new piece of evidence unearthed years after an attack can shine a different light on an investigation and introduce new challenges to current assumptions.

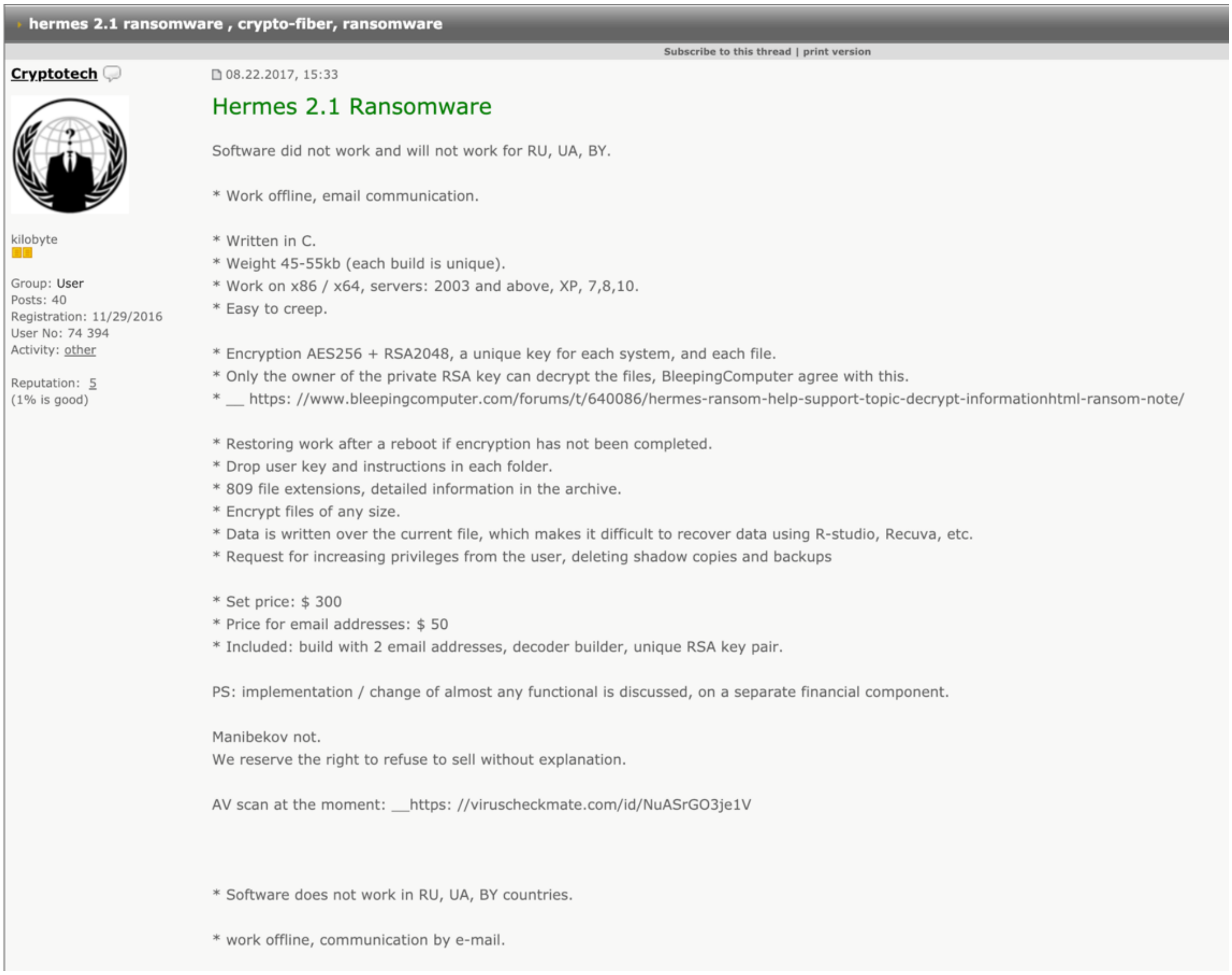
Ryuk attack: putting the pieces together

In October 2017, we investigated an attack on a Taiwanese bank. We discovered the actors used a clever tactic to distract the IT staff: a ransomware outbreak timed for the same moment that the thieves were stealing money. We used the term *pseudo-ransomware* to describe this attack. The malware was Hermes version 2.1.

One of the functions we often see in ransomware samples is that they will not execute if the victim’s system language is one of the following:

- 419 (Russian)
- 422 (Ukrainian)
- 423 (Belarusian)

That was October 2017. Searching earlier events, we noticed a posting from August 2017 in an underground forum in which a Russian-speaking actor offered the malware kit Hermes 2.1 ransomware:



hermes 2.1 ransomware , crypto-fiber, ransomware

Subscribe to this thread | print version

Cryptotech

kilobyte

Group: User
Posts: 40
Registration: 11/29/2016
User No: 74 394
Activity: other

Reputation: 5
(1% is good)

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/

* 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.

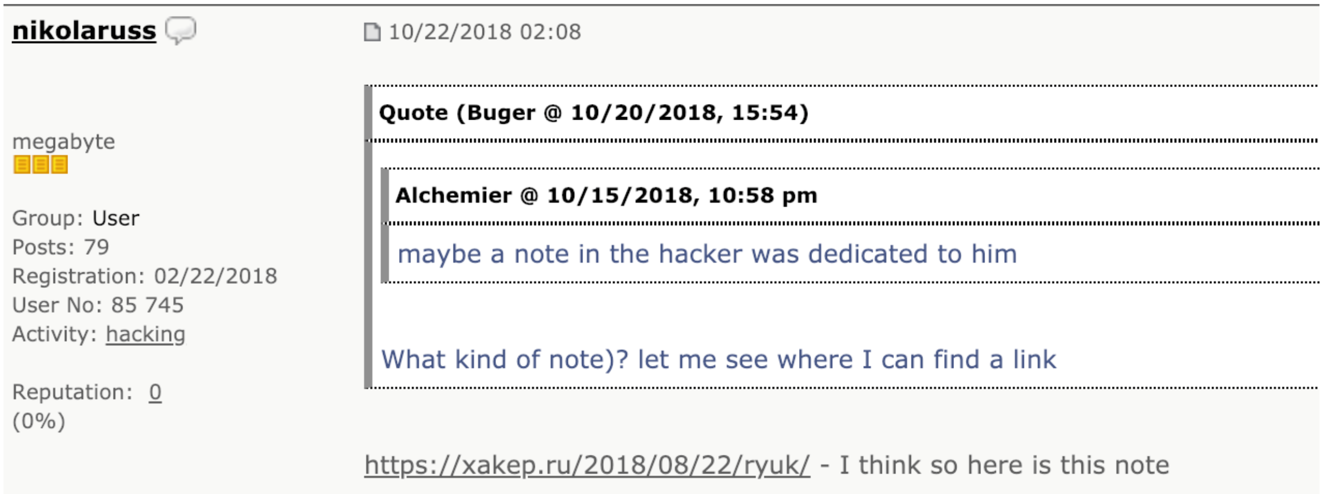
AV scan at the moment: __https: //viruscheckmate.com/id/NuASrGO3je1V

* Software does not work in RU, UA, BY countries.

* work offline, communication by e-mail.

What if the actor who attacked the Taiwanese bank simply bought a copy of Hermes and added it to the campaign to cause the distraction? Why go to the trouble to build something, when the actor can just buy the perfect distraction in an underground forum?

In the same underground forum thread we found a post from October 22, 2018, mentioning Ryuk.



nikolaruss

megabyte

Group: User
Posts: 79
Registration: 02/22/2018
User No: 85 745
Activity: hacking

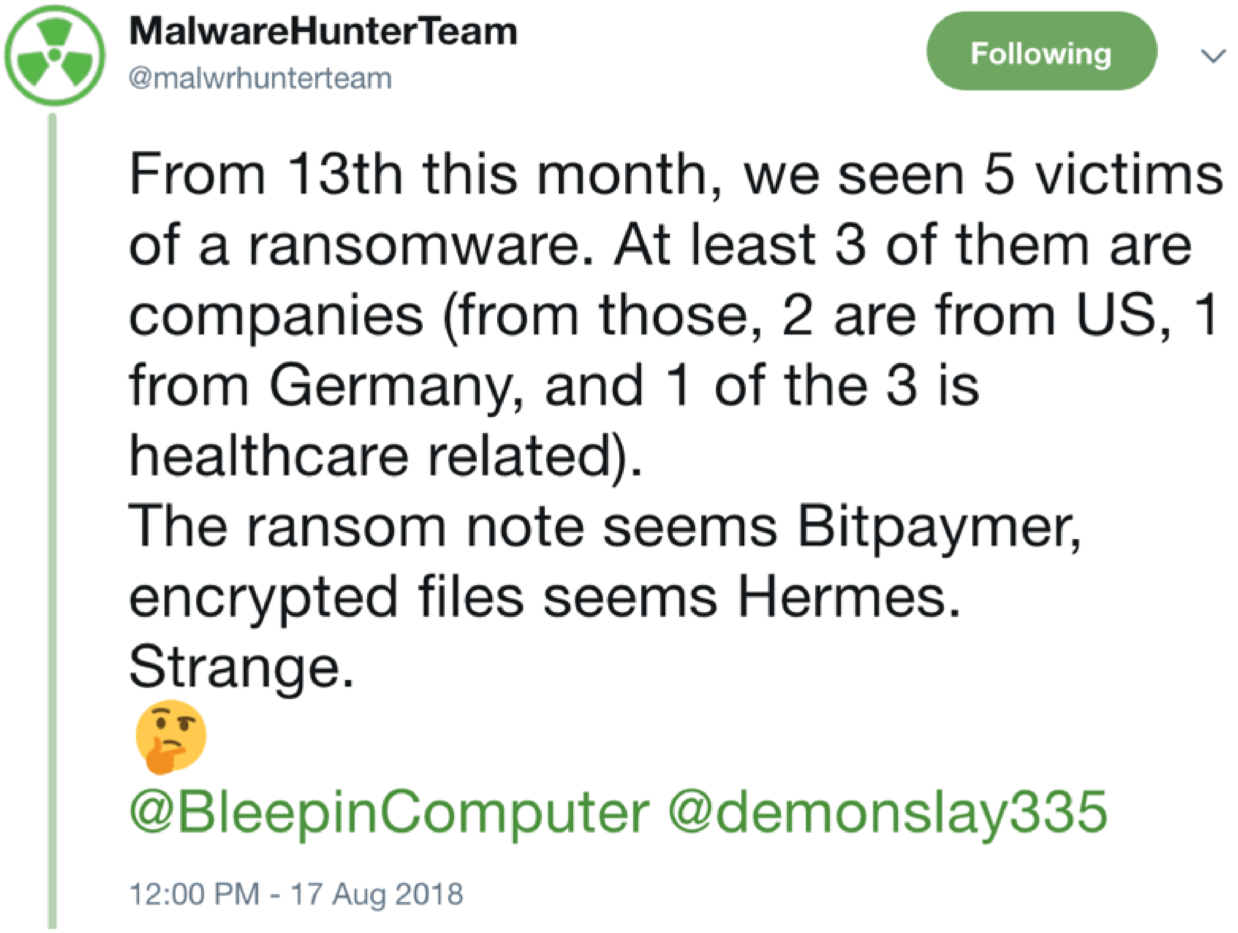
Reputation: 0
(0%)

10/22/2018 02:08

> **Quote (Buger @ 10/20/2018, 15:54)**
>
> > **Alchemier @ 10/15/2018, 10:58 pm**
> >
> > maybe a note in the hacker was dedicated to him
>
> What kind of note)? let me see where I can find a link

https://xakep.ru/2018/08/22/ryuk/ - I think so here is this note

This post contains a link to an article in the Russian security magazine Xakep.ru ("Hacker") discussing the emergence of Ryuk and how it was first discovered by MalwareHunterTeam in August 2018. This first appearance came well before last week's attack on newspaper printing services.



MalwareHunterTeam
@malwrhunterteam

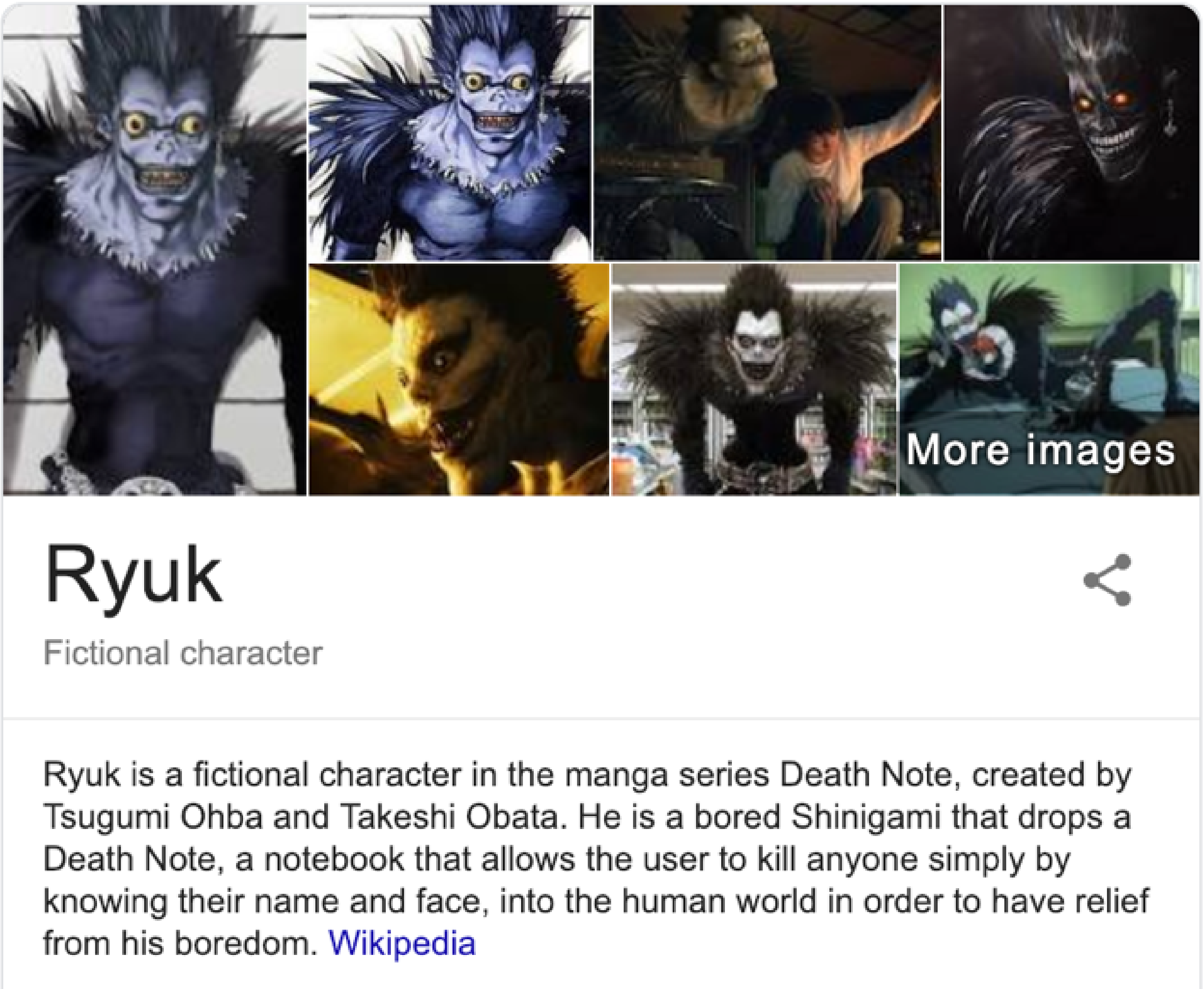
From 13th this month, we seen 5 victims of a ransomware. At least 3 of them are companies (from those, 2 are from US, 1 from Germany, and 1 of the 3 is healthcare related).
The ransom note seems Bitpaymer, encrypted files seems Hermes.
Strange.
🤔
@BleepinComputer @demonslay335

12:00 PM - 17 Aug 2018

Manga connection

Ryuk, according to Wikipedia, refers to a Japanese manga character from the series "Death Note." Ryuk apparently drops a death note, a fitting name for ransomware that drops ransom notes.

Ransomware is typically named by its cybercriminal developer, as opposed to the naming of state-sponsored malware, which is mostly is done by the security industry. It seems the criminals behind Ryuk are into manga.



Ryuk

Fictional character

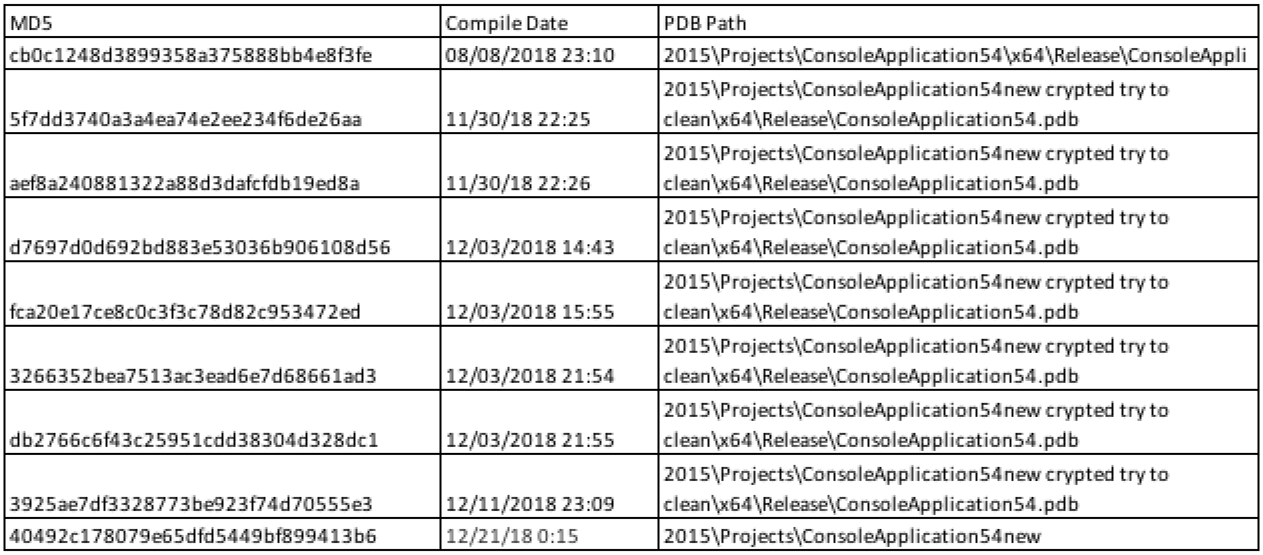
Ryuk is a fictional character in the manga series Death Note, created by Tsugumi Ohba and Takeshi Obata. He is a bored Shinigami that drops a Death Note, a notebook that allows the user to kill anyone simply by knowing their name and face, into the human world in order to have relief from his boredom. Wikipedia

The use of manga character names and references is common in the cybercriminal scene. We often come across manga-inspired nicknames and avatars in underground forums.

Technical indicators

Looking at research from our industry peers comparing Ryuk and Hermes, we notice that the functionalities are generally equal. We agree that the actors behind Ryuk have access to the Hermes source code.

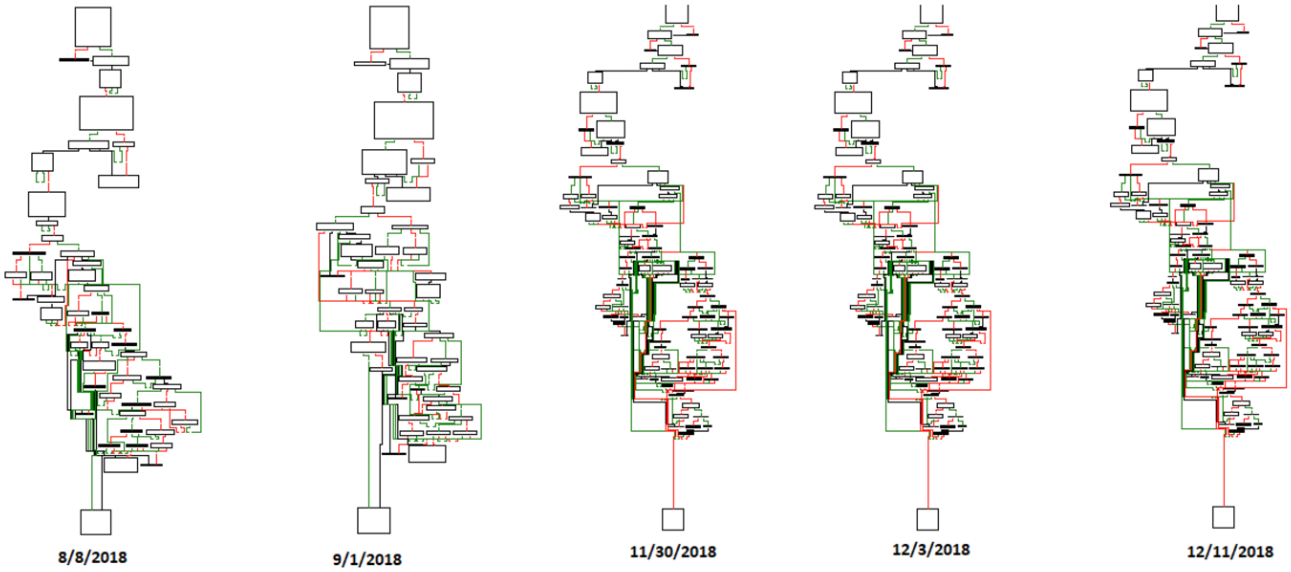
Let’s dive a bit deeper into Ryuk and compare samples over the last couple of months regarding compilation times and the presence of program database (PDB) paths:



MD5	Compile Date	PDB Path
cb0c1248d3899358a375888bb4e8f3fe	08/08/2018 23:10	2015\Projects\ConsoleApplication54\x64\Release\ConsoleAppli
5f7dd3740a3a4ea74e2ee234f6de26aa	11/30/18 22:25	2015\Projects\ConsoleApplication54new crypted try to clean\x64\Release\ConsoleApplication54.pdb
aef8a240881322a88d3dafcfdb19ed8a	11/30/18 22:26	2015\Projects\ConsoleApplication54new crypted try to clean\x64\Release\ConsoleApplication54.pdb
d7697d0d692bd883e53036b906108d56	12/03/2018 14:43	2015\Projects\ConsoleApplication54new crypted try to clean\x64\Release\ConsoleApplication54.pdb
fca20e17ce8c0c3f3c78d82c953472ed	12/03/2018 15:55	2015\Projects\ConsoleApplication54new crypted try to clean\x64\Release\ConsoleApplication54.pdb
3266352bea7513ac3ead6e7d68661ad3	12/03/2018 21:54	2015\Projects\ConsoleApplication54new crypted try to clean\x64\Release\ConsoleApplication54.pdb
db2766c6f43c25951cdd38304d328dc1	12/03/2018 21:55	2015\Projects\ConsoleApplication54new crypted try to clean\x64\Release\ConsoleApplication54.pdb
3925ae7df3328773be923f74d70555e3	12/11/2018 23:09	2015\Projects\ConsoleApplication54new crypted try to clean\x64\Release\ConsoleApplication54.pdb
40492c178079e65dfd5449bf899413b6	12/21/18 0:15	2015\Projects\ConsoleApplication54new

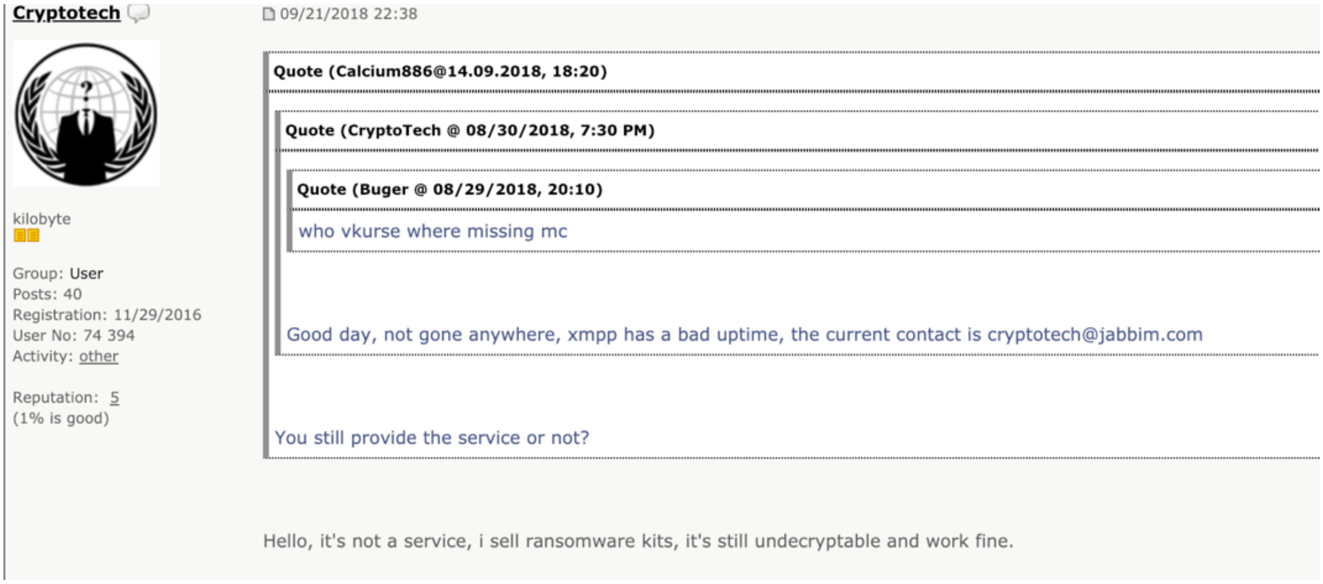
We can see the PDB paths are almost identical. When we compare samples from August and December 2018 and focus on the checksum values of the executables' rich headers, they are also identical.

From a call-flow perspective, we notice the similarities and evolution of the code:



The Hermes 2.1 ransomware kit, renamed and redistributed as Ryuk.

The author and seller of Hermes 2.1 emphasizes that he is selling is a kit and not a service. This suggests that a buyer of the kit must do some fine tuning by setting up a distribution method (spam, exploit kit, or RDP, for example) and infrastructure to make Hermes work effectively. If changing a name and ransom note are part of these tuning options, then it is likely that Ryuk is an altered version Hermes 2.1.



Cryptotech

09/21/2018 22:38

kilobyte

Group: User
Posts: 40
Registration: 11/29/2016
User No: 74 394
Activity: other

Reputation: 5
(1% is good)

> **Quote (Calcium886@14.09.2018, 18:20)**
>
> > **Quote (CryptoTech @ 08/30/2018, 7:30 PM)**
> >
> > > **Quote (Buger @ 08/29/2018, 20:10)**
> > >
> > > who vkurse where missing mc
> >
> > Good day, not gone anywhere, xmpp has a bad uptime, the current contact is cryptotech@jabbim.com
>
> You still provide the service or not?

Hello, it's not a service, i sell ransomware kits, it's still undecryptable and work fine.

Attribution: analyzing competing hypotheses

In the race to determine who is behind an attack, research facts (the What and How questions) are often put aside to focus on attribution (the Who question). Who did it? This pursuit is understandable yet fundamentally flawed. Attribution is crucial, but there will always be unanswered questions. Our approach focuses on answering the What and How questions by analyzing the malware, the infrastructure involved, and the incident response performed at the victim's site.

Our approach is always to analyze competing hypotheses. When investigating an incident, we form several views and compare all the artifacts to support these hypotheses. We try not only to seek verifying evidence but also actively try to find evidence that falsifies a hypothesis. Keeping our eyes open for falsifying facts and constantly questioning our results are essential steps to avoid conformation bias. By following this method, we find the strongest hypothesis is not the one with the most verifying evidence, but the one with the least falsifying evidence.

Examining competing hypotheses is a scientific approach to investigating cyber incidents. It may not help with the race to attribution, but it ensures the output is based on available evidence.

The most *likely* hypothesis in the Ryuk case is that of a cybercrime operation developed from a tool kit offered by a Russian-speaking actor. From the evidence, we see sample similarities over the past several months that indicate a tool kit is being used. The actors have targeted several sectors and have asked a high ransom, 500 Bitcoin. Who is responsible? We do not know. But we do know how the malware works, how the attackers operate, and how to detect the threat. That analysis is essential because it allows us to serve our customers.

John Fokker

John Fokker is a Principal Engineer and Head of Cyber Investigations for the Advanced Threat Research. Prior to joining the team, he worked at the National High Tech Crime Unit...