



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

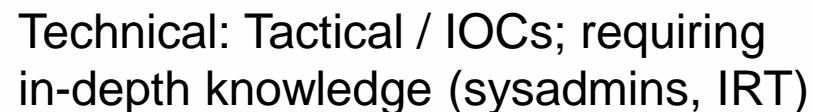
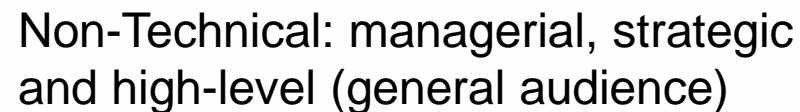
HC3 Threat Intelligence Briefing Ryuk Ransomware

OVERALL CLASSIFICATION IS**UNCLASSIFIED****TLP:WHITE****8/30/2018**

- ▶ Intro
- ▶ Overview
- ▶ Ryuk Profile
- ▶ Ransom Note
- ▶ Lazarus Group
- ▶ Hermes
- ▶ Similarity Examples
- ▶ Indicators of Compromise
- ▶ Protections and Mitigations
- ▶ Conclusion



Slides Key:





Overview

Threat: *Ryuk Ransomware* ([Check Point](#))

- >**ACTIVE SINCE:** 13 August 2018
- >Highly Targeted, well-resourced and planned
- >**Ransom is comparatively HIGH**
 - >15 BTC – 50 BTC
 - >Attackers reportedly netted ~\$640,000

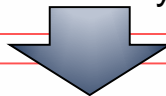
Notables ([id-ransomware](#)):

- >Attempts to encrypt network resources



- >At the end of encryption, Ryuk destroys its encryption key and launches a BAT file that will remove shadow copies and various backup files from the disk.

>The structure of the encrypted file is identical to the structure used in Hermes Ransomware, including the HERMES distinctive token that this malware uses to identify the files that it has already encrypted.



- > Ryuk may either be the work of the HERMES operators, the allegedly North Korean group, or the work of an actor who has obtained the HERMES source code.





Ryuk Profile

Ryuk Ransomware ([Check Point](#))

NOT LIKE COMMON RANSOMWARE

- Systematically distributed via malicious spam (MALSPAM) campaigns
- Exploit kits

SIMILAR TO SAMSAM CAMPAIGNS

- Tailored to each victim (deliberate targeting)
- Encryption scheme is intentionally built for small-scale operations
- Only crucial assets and resources are infected in each targeted network
- Infection and distribution carried out manually by the attackers



What This Means...

- **Attackers are required to complete** extensive network mapping, lateral movement and credential collection prior to each operation.



Ransom Note

```

RyukReadMe.txt - Notepad
File Edit Format View Help
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
eliasmarco@tutanota.com
or
Camdenscott@protonmail.com

BTC wallet:
15RLwdVny5n1n7mTvu1zjg6wt86dhYqnj

Ryuk
No system is safe

```

Two different versions of ransom notes have been seen sent to different victims ([Checkpoint](#))

```

RyukReadMe.txt - Notepad
File Edit Format View Help
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
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:
1LKULheYnNTJXgQNM024MeLrBBCouECH7

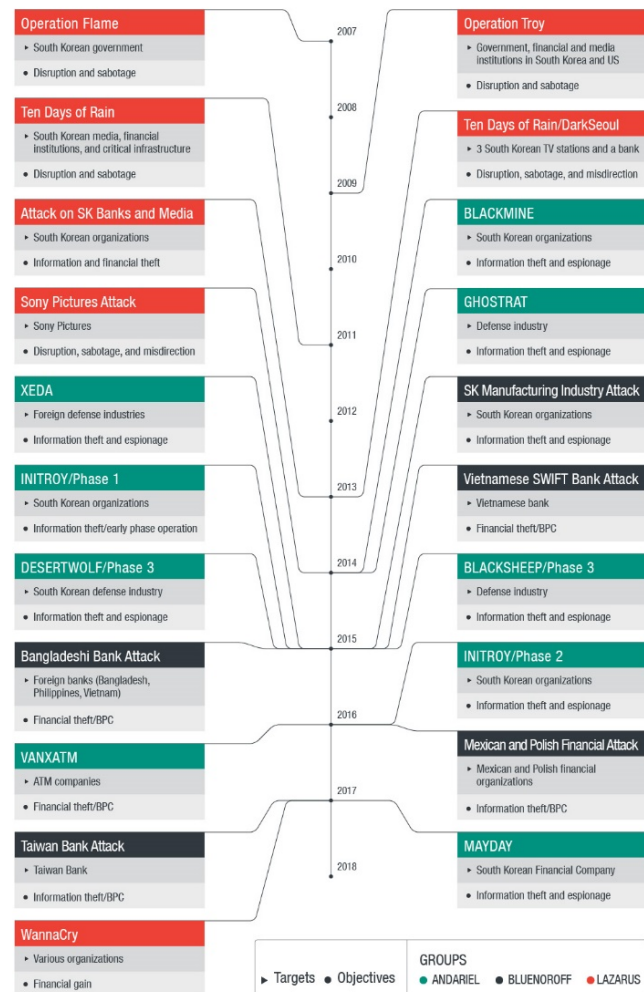
Ryuk
No system is safe

```


Lazarus Group

Threat group that has been attributed to the North Korean government ([Kaspersky](#))

- Focus on espionage, data theft, and financial attacks
- Massive scale and growth
- Two related “spinoff” groups: Bluenoroff and Andariel
- Masquerades as Russian attackers
- Notable Attacks:
 - Operation Troy, 2013
 - Operation DarkSeoul, 2013
 - Sony Pictures Entertainment, 2014
 - Bangladesh Central Bank, 2016



Source: [Trend Micro](#)



Threat: HERMES Ransomware ([Check Point](#))

>ACTIVE SINCE: October 2017

Notably targeted Far Eastern International Bank in Taiwan

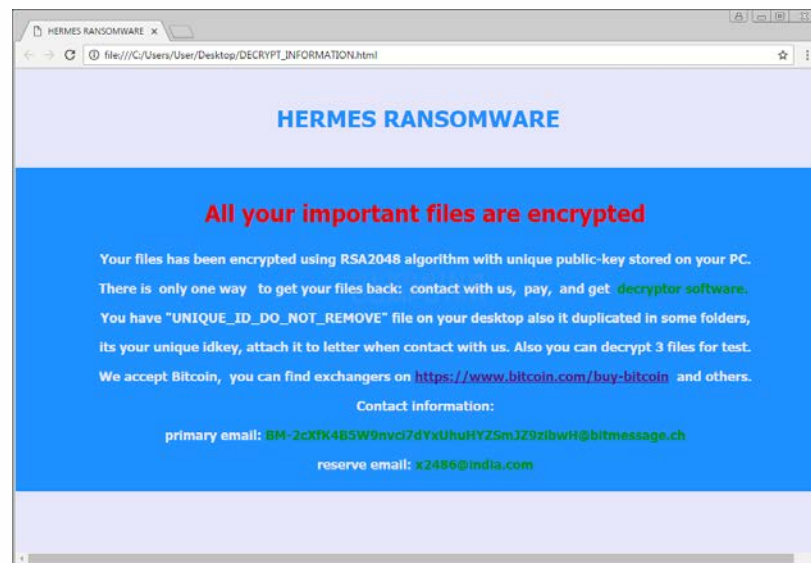
- Fraudulent attempts to wire as much as \$60 million.
- Stolen credentials were used to access the bank's SWIFT accounts



The Hermes Ransomware is installed on victims' computers after they open an unsolicited email attachment
Ransomware will drop an HTML file named 'DECRYPT_INFORMATION.html'

Comparison between Ryuk and Hermes

- Researchers believe targeted Ryuk attacks were the work of HERMES operators (Lazarus) or an actor that has obtained the HERMES source code
- Both the nature of the attack and the malware's own inner workings tie Ryuk to the HERMES ransomware
- Similar encryption logic





Similarity Examples

Hermes

```
*(_DWORD *)s_HERMES = 'MRLH';
*(WORD *)&s_HERMES[4] = 'SE';
s_HERMES[6] = 0;
if ( v42.QuadPart > 0x4C4B40ui64 )
{
    SetFilePointerEx(v4, 0i64, 0, 2u);
    uid = 0;
    v28 = 0;
    v27 = 0i64;
    ml_num_to_uid_ex(num, &uid, 10);
    ml_strcat_a(&marker, L"|");
    ml_strcat_a(&marker, &uid);
    ml_strcat_a(&marker, L"|");
    ml_strcat_a(&marker, s_HERMES);
}
else
{
    ml_w_memmove(&marker, s_HERMES);
}
```

Ryuk 32-bit

```
strcpy(s_HERMES, "HERMES");
if ( *(_QWORD *)v25 > 0x4C4B40ui64 )
{
    SetFilePointerEx_0(hFile, 0, 0, 2);
    v41 = 0;
    *(_QWORD *)uid = 0i64;
    ml_num_to_uid(num, uid);
    ml_strcat_a(marker, "|");
    ml_strcat_a(marker, uid);
    ml_strcat_a(marker, "|");
    ml_strcat_a(marker, s_HERMES);
}
else
{
    ml_w_memmove(marker, s_HERMES);
}
```

Marker generation in Ryuk and Hermes.

Hermes

```
do
{
    if ( *((_BYTE *)&v23 + v12) == 'H'
        && *((_BYTE *)&v23 + v12 + 1) == 'E'
        && *((_BYTE *)&v23 + v12 + 2) == 'R'
        && *((_BYTE *)&v23 + v12 + 3) == 'M'
        && *((&v24 + v12) == 'E'
        && v25[v12] == 'S' )
    {
        CloseHandle(v4);
        return 5;
    }
    ++v12;
}
while ( v12 < 0x14 );
```

Ryuk 32-bit

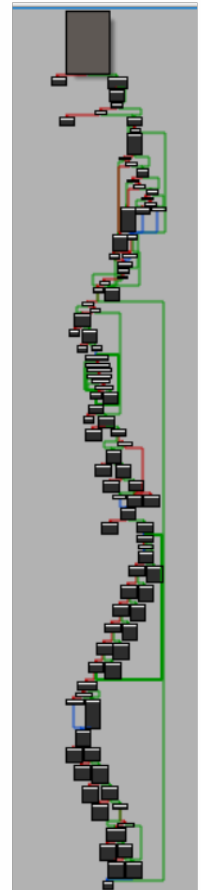
```
do
{
    if ( *((_BYTE *)&v42 + v12) == 'H'
        && *((_BYTE *)&v42 + v12 + 1) == 'E'
        && *((_BYTE *)&v42 + v12 + 2) == 'R'
        && *((_BYTE *)&v42 + v12 + 3) == 'M'
        && *((&v43 + v12) == 'E'
        && v44[v12] == 'S' )
    {
        CloseHandle_0(hFile);
        return 5;
    }
    ++v12;
}
while ( v12 < 0x14 );
```

Marker check in Ryuk and Hermes

Hermes



Ryuk 32-bit



Call flow graphs of the encryption functions in Ryuk and Hermes.

Source: [Checkpoint](#)





Indicators of Compromise

Ryuk Ransomware hashes (MD5):

- ▶ c0202cf6aeab8437c638533d14563d35
- ▶ d348f536e214a47655af387408b4fca5
- ▶ 958c594909933d4c82e93c22850194aa
- ▶ 86c314bc2dc37ba84f7364acd5108c2b
- ▶ 29340643ca2e6677c19e1d3bf351d654
- ▶ cb0c1248d3899358a375888bb4e8f3fe
- ▶ 1354ac0d5be0c8d03f4e3aba78d2223e

Malware Dropper hashes (MD5):

- ▶ 5ac0f050f93f86e69026faea1fbb4450





Protection & Mitigations

Recommended Practices for Hermes (Researchers continue to analyze Ryuk) ([BAE Systems](#))

- Firewall off SMB (445) for internal computers. If access to this service is required, it should be permitted only for those IP's that require access. i.e. 445 is required for SCOM to push an agent install, therefore 445 should only be allowed from that source server;
- Application blacklisting should be implemented to prevent the use of tools such as vssadmin.exe, cmd.exe, powershell.exe and similar;
- File Integrity Monitoring should be considered and configured to monitor file creations in “trusted” locations such as the System32 directory. This can also be used to monitor deletes, with an alert configured to fire on excessive deletes in a row;
- Windows Security Event logs should be monitored to capture Scheduled Task creation events – Event ID 4698;
- Registry Auditing should be enabled and monitored to capture any additions to HKLM\Software\Microsoft\Windows\CurrentVersion\Run;
- Excessive use of known administrative privilege accounts should be alerted on – specifically in a “one to many” behavioral configuration. i.e. is one specific IP connecting to a large number of devices using the same credentials in a short period of time;
- Ensure privileged accounts have a complex password that does not include any part of the username, or application it relates to.

Additional longer term recommendations for financial institutions:

- Practice incident response scenarios which include complex attacks combining covert payment fraud and overt network disruption through ransomware, DDoS, network downtime, etc.
- Ensure that you are progressing towards being able to attest against the SWIFT 27 controls.



Conclusion

Upcoming Briefs

- ▶ Chain Supply Threats
- ▶ Trends in Malicious Macro Usage
- ▶ Cryptomining Landscape
- ▶ Various APT/FIN Groups

Analyst-to-analyst webinars are available

Questions / Comments / Concerns?

HHS HC3 Email Address: HC3@hhs.gov

