An Overhead View of the Royal Road

nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html

2020-01-29

Abstract

Several targeted attack groups share the tools used in the attack and are reported to be doing similar attacks. Attack tools are also shared in attacks targeting Japanese organizations, for example, Tick. Tick may use a tool called Royal Road RTF Weaponizer.

And Royal Road is used by targeted attack groups such as Goblin Panda and Temp.Trident that is suspected of being involved in China.

In this blog, we will focus on the Royal Road, and introduce the features of the tool, such as the outline of the tool, its behavior, and the exploited vulnerability. Next, the targeted attack groups that use the Royal Road are listed, and each attack case is shown in detail. We have collected over 100 malicious documents from 2018 and investigated malware that is deployed and downloaded from there. Even in groups using the same Royal Road, we attributed them based on the target country/organization, the technique used for the attack, the malware executed, etc.

There are a wide variety of countries/organizations targeted for attack, mainly in Asia. Such information has been published by researchers all over the world, but it's not widely known that Royal Road is used in Tick attacks targeting Japanese organizations. Attacks using Royal Road are still active in 2019. Share analysis results of malicious documents and malware based on the cases we observed. Other targeted attack groups may be related to Royal Road. We introduce the attack cases of these attack groups and show their relevance.

Finally, we show the hunting technique using the characteristics of RTF files using Royal Road and the techniques that are preferred by targeted attack groups that use them. This blog will help researchers who are researching and analyzing targeted attacks and CSIRT/SOC members to understand the attacks and take countermeasures.

Summary

Royal Road

Royal Road is RTF weaponizer that named by Anomali. Sometimes called “8.t RTF exploit builder”. This tool is not OSS, However it's shared between multiple actors.

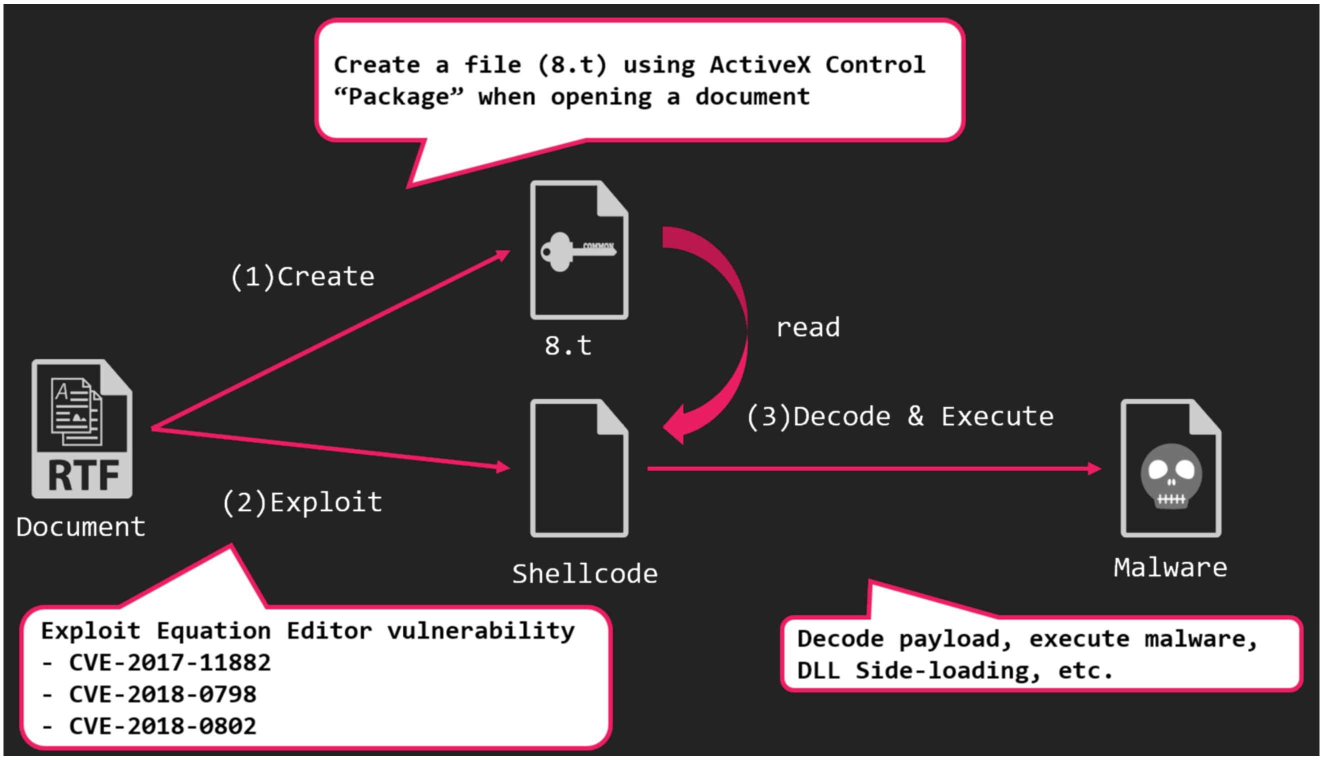
We define the RTFs generated by RoyalRoad is supposed to satisfy the following two conditions:

1. Exploit the vulnerability in the Equation Editor
2. Have an object named 8.t in the RTF

Royal Road behaves as follows.

1. RTF create a file (8.t) using ActiveX Control “Package” when opening a document

2. All Vulnerabilities used by exploit coed are based on Equation Editor.
    - CVE-2017-11882
    - CVE-2018-0798
    - CVE-2018-0802
3. It decode 8.t, execute malware, dll-sideloading, etc



Create a file (8.t) using ActiveX Control "Package" when opening a document

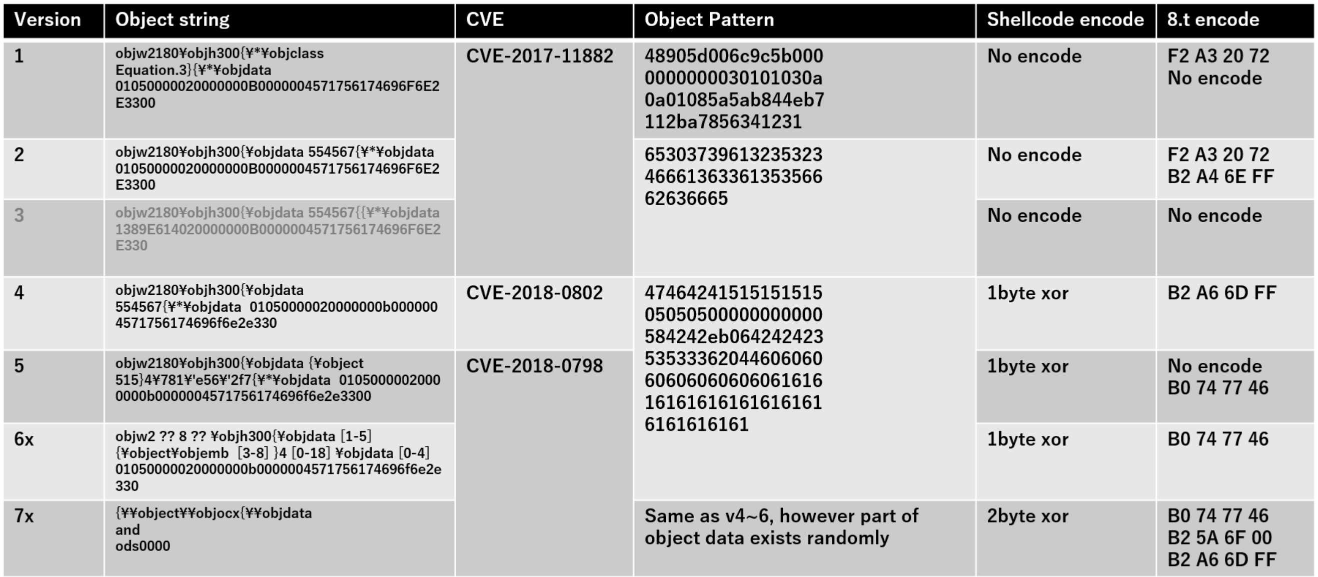
Exploit Equation Editor vulnerability
- CVE-2017-11882
- CVE-2018-0798
- CVE-2018-0802

Decode payload, execute malware, DLL Side-loading, etc.

Classification v1-v5 defined by Proofpoint and Anomali published at VB2019. We are doing more research about RTF Object. RTF analysis showed that there was a special byte sequence immediately before the shellcode. We called that an object pattern. 8.t encoding is not distinguished by version. It's considered an actor distinction rather than a tool distinction.

About v3, RTF including 8.t could not be found in our survey, so we define this as RoyalRoad-related, not RoyalRoad.

New version definitions for v6 and later. The object string has changed a little since v5, but it is basically the same. v7 has a very different object string. v7 object pattern is same as v4-v6, but part ofobject data exists randomly.



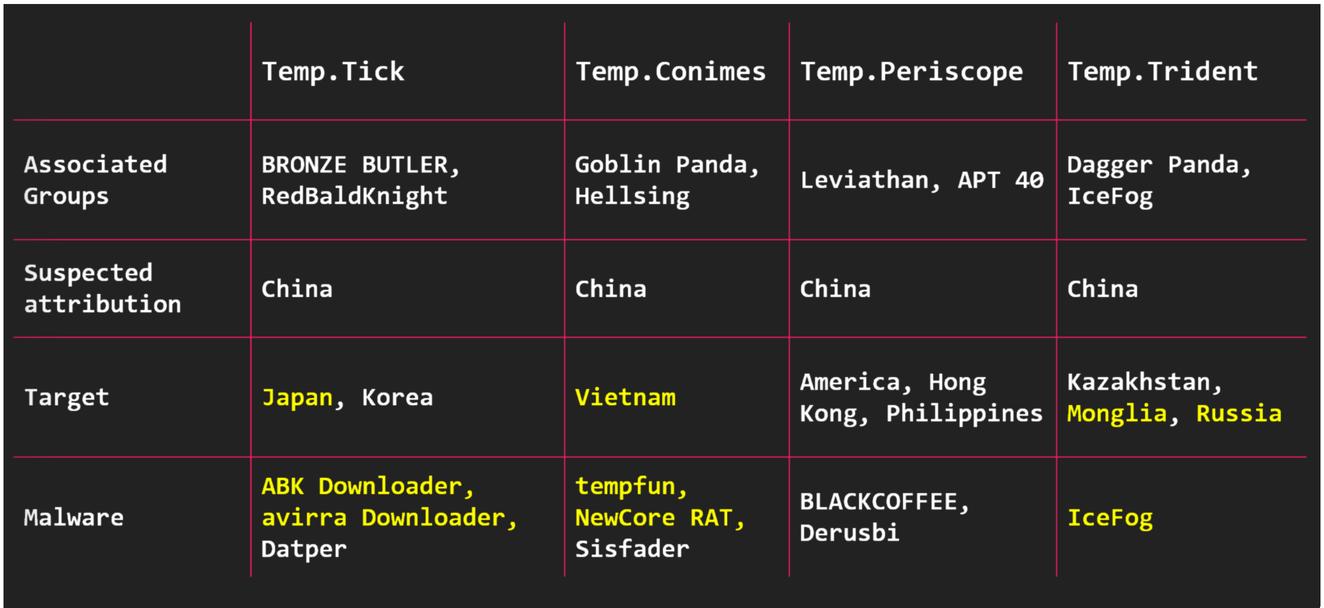
Version	Object string	CVE	Object Pattern	Shellcode encode	8.t encode
1	objw2180¥objh300{¥*¥objclass Equation.3}{¥*¥objdata 01050000020000000B0000004571756174696F6E2E3300	CVE-2017-11882	48905d006c9c5b000 0000000030101030a 0a01085a5ab844eb7 112ba7856341231	No encode	F2 A3 20 72 No encode
2	objw2180¥objh300{¥objdata 554567{¥*¥objdata 01050000020000000B0000004571756174696F6E2E3300		65303739613235323 46661363361353566 62636665	No encode	F2 A3 20 72 B2 A4 6E FF
3	objw2180¥objh300{¥objdata 554567{{¥*¥objdata 1389E614020000000B0000004571756174696F6E2E330			No encode	No encode
4	objw2180¥objh300{¥objdata 554567{¥*¥objdata 01050000020000000b0000004571756174696f6e2e330	CVE-2018-0802	47464241515151515 05050500000000000 584242eb064242423 53533362044606060 60606060606061616 16161616161616161 6161616161	1byte xor	B2 A6 6D FF
5	objw2180¥objh300{¥objdata {¥object 515}4¥781¥'e56¥'2f7{¥*¥objdata 01050000020000000b0000004571756174696f6e2e3300	CVE-2018-0798		1byte xor	No encode B0 74 77 46
6x	objw2 ?? 8 ?? ¥objh300{¥objdata [1-5] {¥object¥objemb [3-8] }4 [0-18] ¥objdata [0-4] 01050000020000000b0000004571756174696f6e2e330			1byte xor	B0 74 77 46
7x	{¥¥object¥¥objocx{¥¥objdata and ods0000		Same as v4~6, however part of object data exists randomly	2byte xor	B0 74 77 46 B2 5A 6F 00 B2 A6 6D FF

For attribution

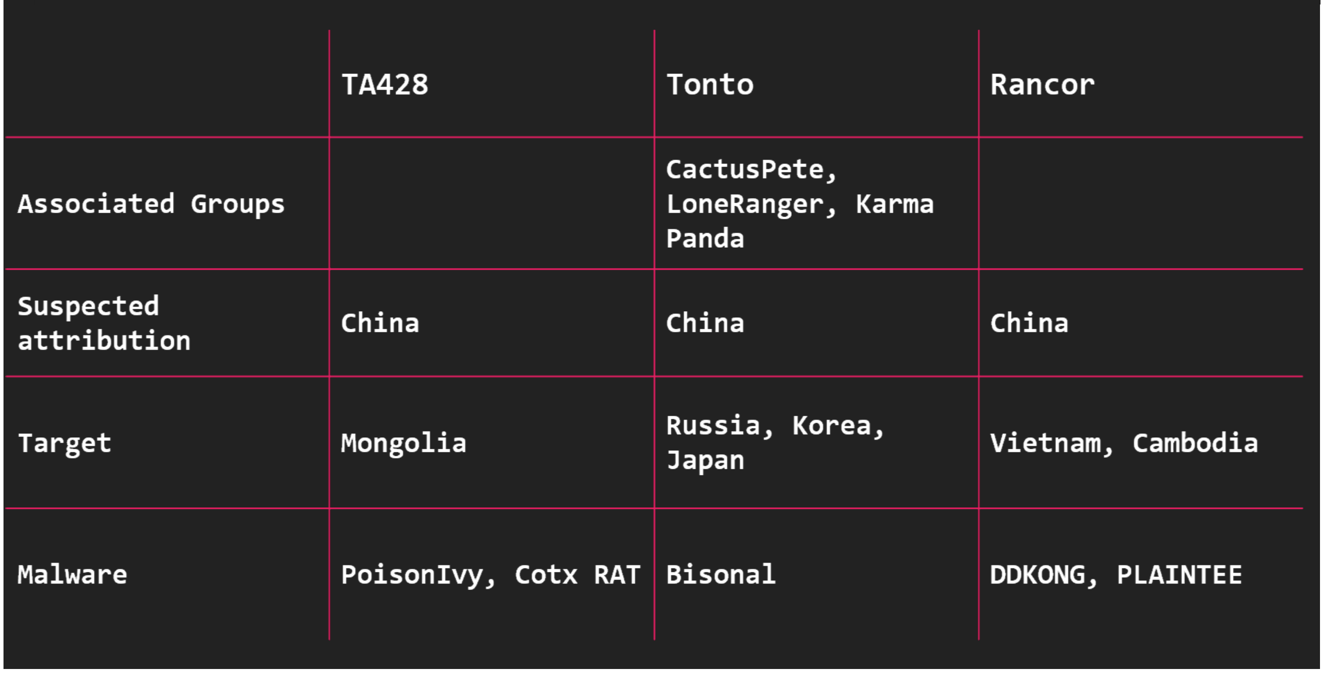
- Time
  - submission to public service
  - RTF creation
- Target country
  - decoy file language
- RTF characteristics
  - Object strings
  - Object patterns
  - Package patterns
  - Object name, Path
- Payload encoding patterns
- Dropped file name
- Malware execution techniques
  - T1137 (Office Application Startup)
  - T1073 (DLL Side-Loading)
- Final payload (malware family)

Actors

Here are the actors that have been confirmed to use RoyalRoad. It is considered that China’s involvement is suspected.

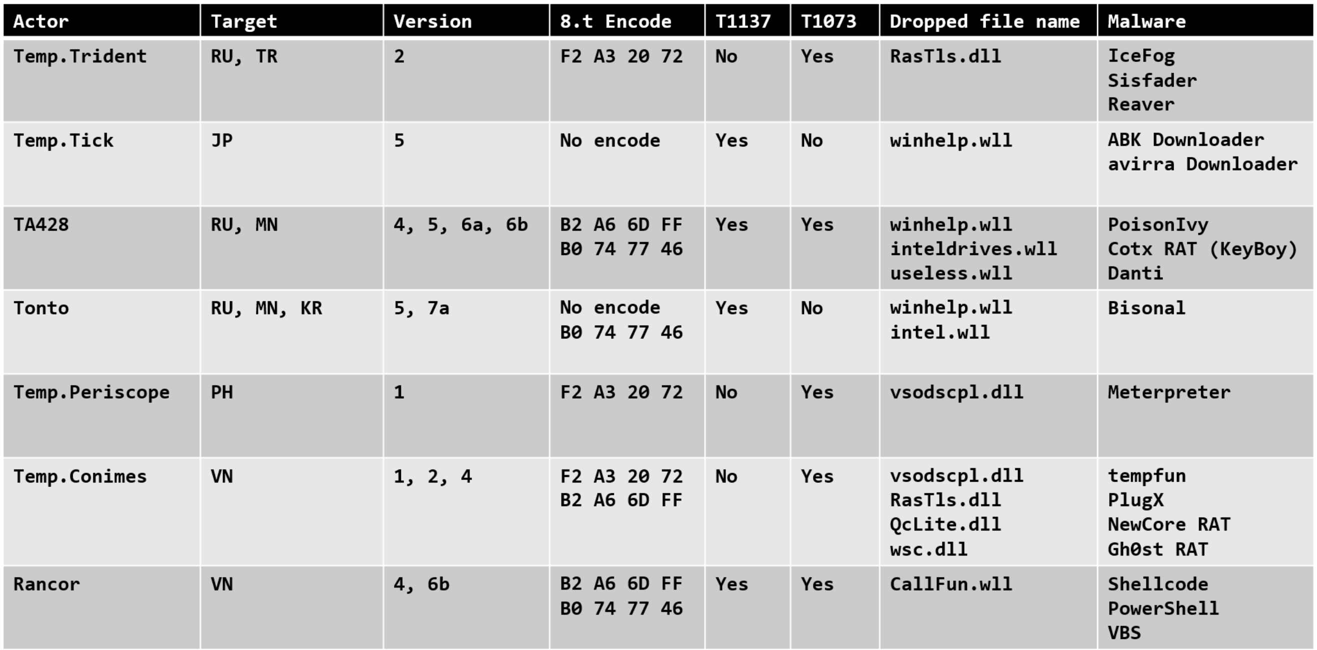


	Temp.Tick	Temp.Conimes	Temp.Periscope	Temp.Trident
Associated Groups	BRONZE BUTLER, RedBaldKnight	Goblin Panda, Hellsing	Leviathan, APT 40	Dagger Panda, IceFog
Suspected attribution	China	China	China	China
Target	Japan, Korea	Vietnam	America, Hong Kong, Philippines	Kazakhstan, Monglia, Russia
Malware	ABK Downloader, avirra Downloader, Datper	tempfun, NewCore RAT, Sisfader	BLACKCOFFEE, Derusbi	IceFog



	TA428	Tonto	Rancor
Associated Groups		CactusPete, LoneRanger, Karma Panda	
Suspected attribution	China	China	China
Target	Mongolia	Russia, Korea, Japan	Vietnam, Cambodia
Malware	PoisonIvy, Cotx RAT	Bisonal	DDKONG, PLAINTEE

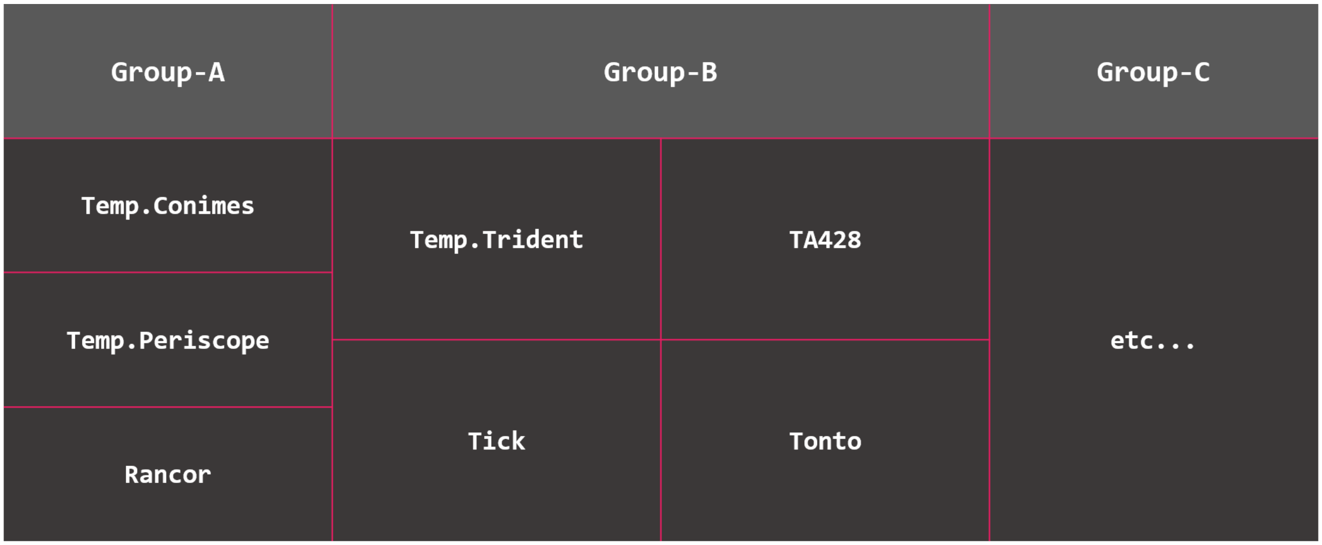
These are tables summarizing each actor's characteristics. We categorize these actors into three groups.



Actor	Target	Version	8.t Encode	T1137	T1073	Dropped file name	Malware
Temp.Trident	RU, TR	2	F2 A3 20 72	No	Yes	RasTls.dll	IceFog Sisfader Reaver
Temp.Tick	JP	5	No encode	Yes	No	winhelp.wll	ABK Downloader avirra Downloader
TA428	RU, MN	4, 5, 6a, 6b	B2 A6 6D FF B0 74 77 46	Yes	Yes	winhelp.wll inteldrives.wll useless.wll	PoisonIvy Cotx RAT (KeyBoy) Danti
Tonto	RU, MN, KR	5, 7a	No encode B0 74 77 46	Yes	No	winhelp.wll intel.wll	Bisonal
Temp.Periscope	PH	1	F2 A3 20 72	No	Yes	vsodscpl.dll	Meterpreter
Temp.Conimes	VN	1, 2, 4	F2 A3 20 72 B2 A6 6D FF	No	Yes	vsodscpl.dll RasTls.dll QcLite.dll wsc.dll	tempfun PlugX NewCore RAT Gh0st RAT
Rancor	VN	4, 6b	B2 A6 6D FF B0 74 77 46	Yes	Yes	CallFun.wll	Shellcode PowerShell VBS

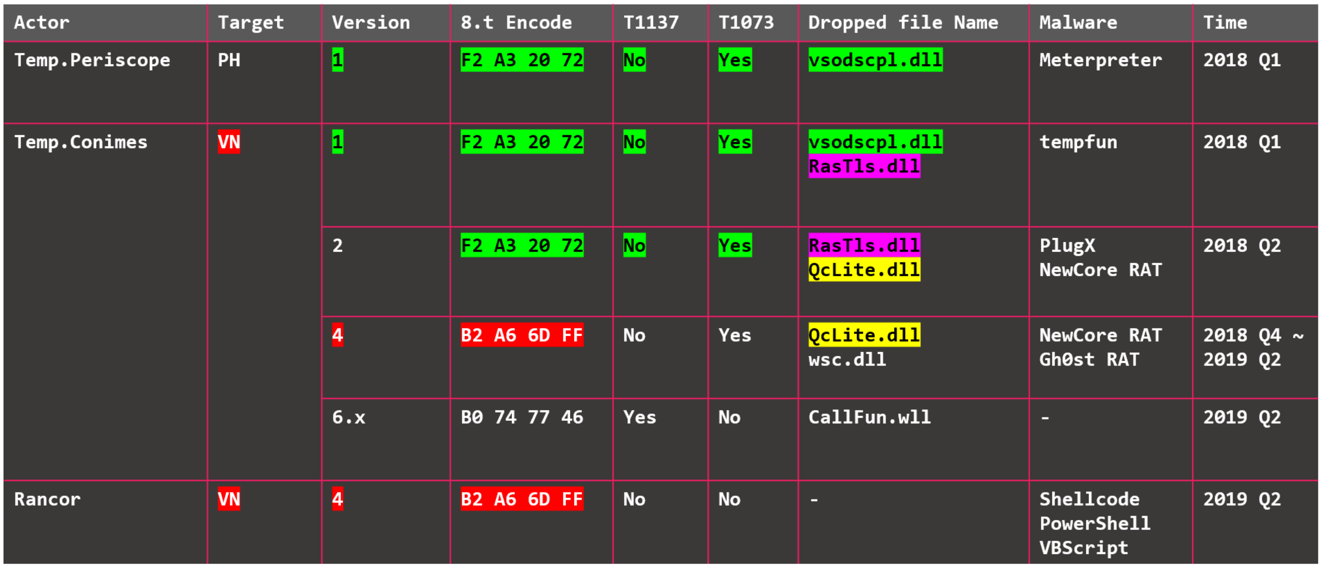
Group

- Group-A is Conimes, Periscope and Rancor.
- Group-B is Trident, Tick, TA428 and Tonto.
- Group-C is something else we don’t know.



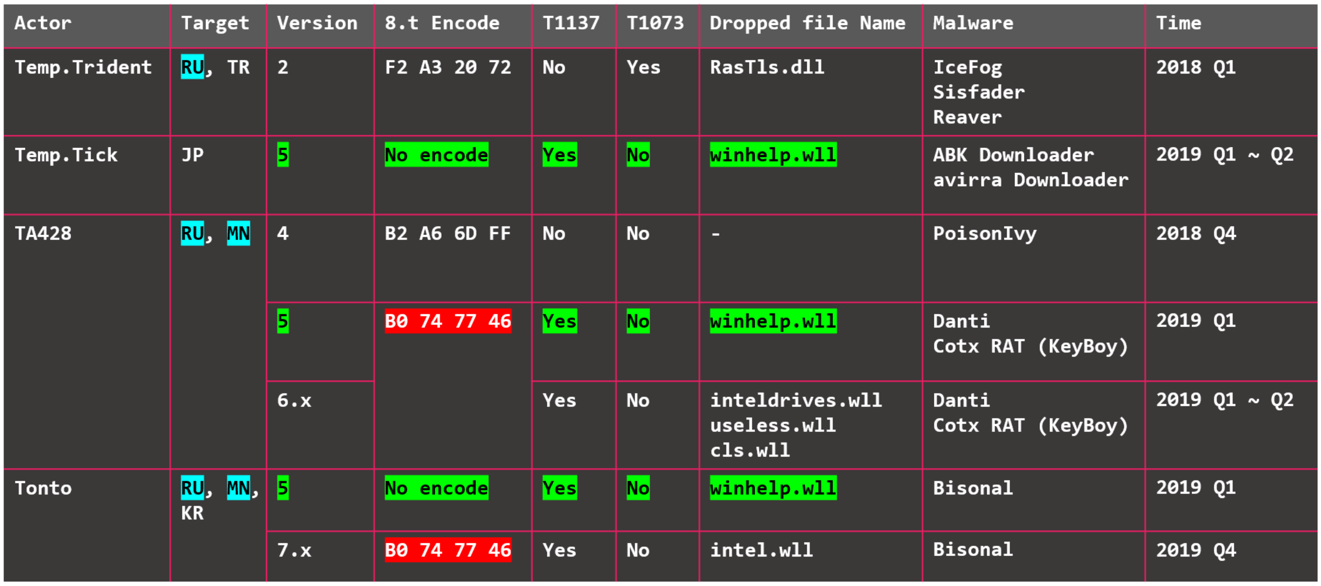
Group-A	Group-B		Group-C
Temp.Conimes	Temp.Trident	TA428	etc...
Temp.Periscope			
Rancor	Tick	Tonto	

Group-A is targeting Southeast Asia. Periscope and Conimes ware active at the same time and share the same techniques. Conimes and Rancor ware also active at the same time and share some techniques. We believe these groups are close and may share tools and insights.



Actor	Target	Version	8.t Encode	T1137	T1073	Dropped file Name	Malware	Time
Temp.Periscope	PH	1	F2 A3 20 72	No	Yes	vsodscpl.dll	Meterpreter	2018 Q1
Temp.Conimes	VN	1	F2 A3 20 72	No	Yes	vsodscpl.dll RasTls.dll	tempfun	2018 Q1
		2	F2 A3 20 72	No	Yes	RasTls.dll QcLite.dll	PlugX NewCore RAT	2018 Q2
		4	B2 A6 6D FF	No	Yes	QcLite.dll wsc.dll	NewCore RAT Gh0st RAT	2018 Q4 ~ 2019 Q2
		6.x	B0 74 77 46	Yes	No	CallFun.wll	-	2019 Q2
Rancor	VN	4	B2 A6 6D FF	No	No	-	Shellcode PowerShell VBScript	2019 Q2

Group-B is including Trident, Tick, TA428 and Tonto. These are actors targeting East Asia, especially Russia, Korea and Japan. Tick, TA428 and Tonto may use the same technique. Especially Tick and Tonto are very similar. We believe that Group-B actors are very close and share techniques and insights.



Actor	Target	Version	8.t Encode	T1137	T1073	Dropped file Name	Malware	Time
Temp.Trident	RU, TR	2	F2 A3 20 72	No	Yes	RasTls.dll	IceFog Sisfader Reaver	2018 Q1
Temp.Tick	JP	5	No encode	Yes	No	winhelp.wll	ABK Downloader avirra Downloader	2019 Q1 ~ Q2
TA428	RU, MN	4	B2 A6 6D FF	No	No	-	PoisonIvy	2018 Q4
		5	B0 74 77 46	Yes	No	winhelp.wll	Danti Cotx RAT (KeyBoy)	2019 Q1
		6.x		Yes	No	inteldrives.wll useless.wll cls.wll	Danti Cotx RAT (KeyBoy)	2019 Q1 ~ Q2
Tonto	RU, MN, KR	5	No encode	Yes	No	winhelp.wll	Bisonal	2019 Q1
		7.x	B0 74 77 46	Yes	No	intel.wll	Bisonal	2019 Q4

Wrap-up

The RTF file created using the Royal Road exploits a vulnerability in the equation editor. The RTF file has a various of characteristics that help with attribution. There are many actors who use Royal Road. We can divide them into three groups and suppose connections between actors.

Appendix

Appendix-1: IOC

https://nao-sec.org/jsac2020_ioc.html

Appendix-2: Tool

- rr_decoder
- Yara Rules

Full report is here: [PDF (EN)]