vb 2019 LONDON 2 – 4 October 2019

ATTRIBUTION IS IN THE OBJECT: USING RTF OBJECT DIMENSIONS TO TRACK APT PHISHING WEAPONIZERS

Ghareeb Saad
Anomali, UK

Michael A. Raggi
Proofpoint, USA

gsaad@anomali.com; mraggi@proofpoint.com

ABSTRACT

Typographers and font designers sometimes quip that the divine fingerprint of the artist exists in the spaces between the letters ('God is in the Kerning' – Matteo Bologna). They have also said 'Nothing made by a human can avoid personal expression' (Hrant Papazian). *Anomali Labs* has conducted an in-depth study of the unique object dimensions present in weaponized RTF exploits used in phishing attacks. Through this research we have found that, like typographers, the developers of malicious RTF weaponizers leave behind a unique fingerprint on the malicious phishing attachments they create. This fingerprint can be found in the unique height and width of the malicious objects present in a phishing attachment. So, if God can be found in the kerning, we, as threat researchers, believe that attribution is in the object.

RTF files are among the most popular file formats used in phishing attacks today. *Anomali Labs* has tracked the unique object dimensions present in 22 RTF exploits for CVE-2018-8570, CVE-2018-0802, CVE-2017-11882, CVE-2017-0199, CVE-2014-1761 and CVE-2012-0158 to gain insight into the adversary's weaponization process. By identifying the height and width of malicious RTF objects and creating YARA signatures to track them, analysts have identified APT campaigns related to three distinct Chinese APT groups (Temp.Periscope, Temp.Trident and Goblin Panda), one South Asian APT (Sidewinder), and the cybercriminal campaigns of a known Pakistani APT group (Gorgon Group/Subaat). This paper will cover basic RTF object metadata structure, how this data, when unique, can be used to track threat actors, and an in-depth case study of Chinese and Indian APTs utilizing a shared RTF phishing weaponizer to carry out diverse espionage campaigns across Asia and Central Europe.

EXPLOIT SUPPLY CHAIN & THE NEED FOR WEAPONIZER ATTRIBUTION

The use of weaponized exploits in targeted phishing attacks continues to be among the most popular and effective techniques observed by cybersecurity researchers today. The 2019 *Verizon* DBIR report cites 'Email Attachment' as the top malware infection vector in incidents and reports that *Office* documents and *Windows* applications are the most common infection vectors [1]. Among the *Office* documents utilized in cyber attacks, RTF file format is often used for phishing attachments and is regularly observed in espionage campaigns linked to prominent Advanced Persistent Threat (APT) adversaries. Rich Text Format (RTF) is a proprietary document file format created by *Microsoft* which has found popularity since its creation in 1987. The ubiquity of RTF attachments in APT

attacks has led researchers to conduct an in-depth analysis of hundreds of weaponized RTF exploit files. This analysis has resulted in the development of a repeatable process for tracking the malicious files created by RTF phishing weaponizers and has introduced visibility into the threat actors' supply chain for these weaponizer tools. Often, scripted phishing weaponizers will create malicious documents with predictable object dimensions for certain Common Vulnerability Exposures (CVEs). Based on these artifacts, it is possible to develop YARA detection signatures to allow analysts to study the spread and dissemination of phishing weaponizers across the threat landscape. With this visibility into the weaponization phase of the cyber kill chain, researchers can understand the origination point of weaponizers, which is invaluable for threat actor attribution. Additionally, the ability to detect and track these RTFs is highly advantageous to infosec organizations as it provides attack visibility during the delivery phase of a potential intrusion.

This paper presents a new technique for attributing RTF weaponizers using object dimensions. Researchers have studied more than 6,000 malicious RTF samples and have been able to group and attribute more than 27 different RTF weaponizers using object dimensions. An RTF weaponizer for CVE-2017-11882, CVE-2018-0802 and CVE-2018-0798, dubbed 'Royal Road', was discovered being used in espionage campaigns, and ultimately released into the commodity threat landscape. Royal Road is believed to have originated amongst a group of Chinese APTs conducting espionage campaigns from 2017 to 2019. In 2018, it was observed being used by the Indian APT actor Sidewinder, and in 2019 it was seen being adopted by cybercriminal actors. The diffusion of custom weaponizers like Royal Road, from exclusive usage by its developers or purchasers through to its ultimate emergence as a commodity tool, will be explored as a recurring pattern which we refer to as the 'Weaponizer Life Cycle'.

RTF EXPLOITATION

Rich Text Format was developed by *Microsoft* from 1987 until 2008, and remains supported by *Windows*, *Mac* and *Linux* operating systems. The RTF format was created to enable cross-platform document interchange. This file format has, for years, been a popular target for vulnerability researchers and exploit developers because it can host different object types. The object types include: annotations, fonts, pictures, OLE and SWF. This allows adversaries to deliver exploits from different object types, often by attaching RTF files to phishing emails. The versatility of the RTF format for exploit delivery from different object types has given rise to the following popular CVEs:

- CVE-2014-1761
- CVE-2015-7645
- CVE-2016-4117
- CVE-2016-1019
- CVE-2017-0199
- CVE-2017-8570
- CVE-2017-11882
- CVE-2018-0802
- CVE-2018-0798

RTF TRACKING AND ATTRIBUTION TECHNIQUES

There are many aspects of RTF files that can be used to conduct analysis or track weaponized exploits for attribution purposes. In this paper we will focus on four specific techniques that can provide insight into both adversary operators and adversary supply chains. These four techniques include the tracking of RTF metadata, shellcode, obfuscation, encoding artifacts and object dimensions.

Metadata & author name

In addition to accommodating objects, RTF files can include metadata 'Tag ID' values that can be used to support threat actor attribution. Specifically, analysis of the metadata tag IDs for 'author', 'company', 'operator (last modified by)', 'title' and 'vern' (internal version number) associated with RTF phishing attachments can provide string values that can be leveraged as indicators of compromise. These metadata tag IDs should be recorded and attributed to a threat actor if observed in multiple campaigns over time, alongside additional overlapping IoCs or tactics techniques and procedures (TTPs). Metadata tag ID values can be observed in the strings of the RTF as well as through proprietary analysis tools such as *VirusTotal Enterprise* in the description section of an uploaded malware binary. The tag values for author and operator fields are derived from the machine used to create the RTF phishing attachment. In some instances, if the operator is using an application like *Microsoft Office* to create a weaponized phishing attachment, file compilation will apply the author value associated with the operator's application to the created malicious file. Additionally, a unique value for the 'vern' or internal version number will be applied to all malicious phishing attachments created by that code base. The example shown in Figure 1 from the *VirusTotal* interface demonstrates a recurring metadata author value that was used by a CVE-2012-0158 phishing weaponizer attributed to the Chinese Goblin Panda APT, also known as Conimes. This technique has been explored at length in a SANS CTI Summit presentation on the topic [2].

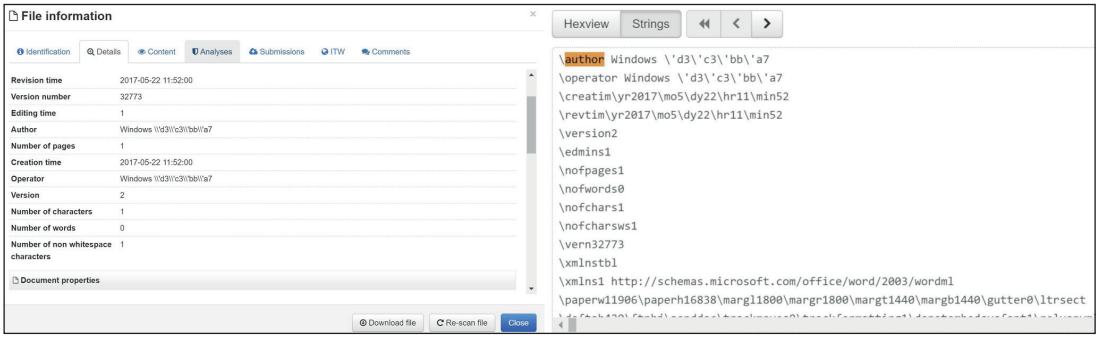

Figure 1: VirusTotal user interface showing RTF metadata author 'Tag ID' and strings.

Although RTF metadata tag ID tracking is a useful method, over time, to develop attribution based on RTF attachments in targeted campaigns, there are limitations to this technique. In many cases RTF metadata is fleeting and trivial to alter from campaign to campaign. Often these values are updated to mimic regionally specific personnel at targeted organizations and changed to the native languages spoken by the targets. Additionally, RTF metadata tags are not mandatory values that must be included upon the compilation of an RTF file. In some cases adversaries have removed RTF metadata tag IDs from weaponized RTF attachments upon updating a phishing weaponizer. Based on the

inconsistent and non-essential nature of RTF metadata as a social engineering mechanism in weaponized RTFs, this tracking method provides the best visibility, over multiple campaigns, of the operator's personas and possible targeting intention, while being a fleeting indicator of compromise.

Shellcode

Certain characteristics of the shellcode used to exploit a vulnerability targeted by a malicious RTF can be used to track certain RTF weaponizers. The most common characteristic of shellcode would be certain Return Oriented Programming (ROP) gadgets being used by the exploit or the technique used to drop and execute the payload. While these characteristics are usually permanent and rarely changed, it is usually difficult to develop YARA rules to automatically track them.

Obfuscation artifacts

The *Office* RTF parser and RTF file specification is very flexible from a development standpoint. One of the most flexible features of an RTF file is the allowance of cascading objects, which can represent data in different formats and escape characters. Exploit developers make use of this functionality to build obfuscated payloads that are still valid when rendered in *Office*, but which can evade AV engines by representing malicious internal content in formats other than what is most commonly used in AV static signature detection. This has the beneficial secondary outcome of making it harder for analysts to extract or analyse the malicious payload.

Actors often deploy scripts to insert custom obfuscation gadgets into their malicious RTFs. Using these gadgets as strings in YARA signatures is a very useful method for tracking RTFs created for certain campaigns or actors. There are multiple articles and papers discussing RTF obfuscation in detail [3, 4]. Figures 2 to 4 show some examples of RTF obfuscation gadgets that can be used to track malicious RTFs.

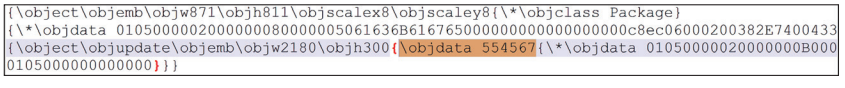

Figure 2: Obfuscation gadget present in Royal Road weaponizer version 2.

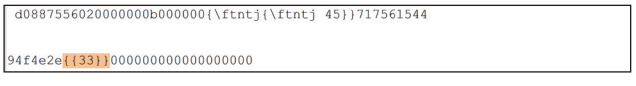

Figure 3: Example of obfuscation gadget used in malicious RTFs.

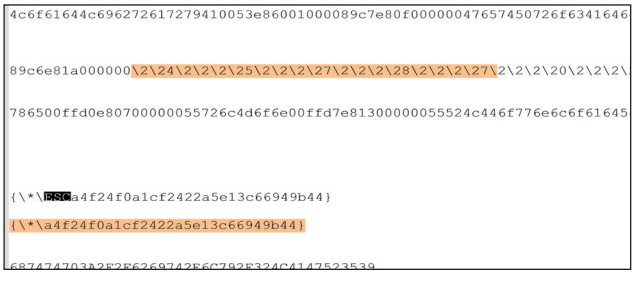

Figure 4: Example of obfuscation gadget used in malicious RTFs.

Object dimensions and phishing weaponizers

CVEs and exploits are often purchased from digital black markets as Python scripts that can be used to weaponize a lure document. Alternatively, weaponizers have been known to be developed as internal tools for APT organizations. Based on the popularity of *Word* for rendering email attachments, threat actors usually build their lure '.doc' using a normal *Office* application and then use the acquired script to inject the malicious RTF object into the lure document once it has been created.

Based on RTF specifications, any object that has a graphical representation (which will most commonly be rendered in *Word*) needs to specify the object dimension as part of the RTF object header. This is to say that the object height and width for graphic representation are included in the strings of the compiled RTF file to ensure that an error will not occur when attempting to load the object. Table 1 includes a list of the object dimensions and attributes that can be included in an RTF object header at the time of compilation.

Object size, position, cropping and scaling	
\objh*N*	***N*** is the original object height in twips, assuming the object has a graphical representation.
\objw*N*	***N*** is the original object width in twips, assuming the object has a graphical representation.
\objsetsize	Forces the object server to set the object's dimensions to those specified by the client.
\objalign*N*	***N*** is the distance in twips from the left edge of the objects that should be aligned on a tab stop. This is needed to place *Equation Editor* equations correctly in line.
\objtransy*N*	***N*** is the distance in twips the objects should be moved vertically with respect to the baseline. This is needed to place *MathType* equations correctly in line.
\objcropt*N*	***N*** is the top cropping distance in twips.
\objcropb*N*	***N*** is the bottom cropping distance in twips.
\objcropl*N*	***N*** is the left cropping distance in twips.
\objcropr*N*	***N*** is the right cropping distance in twips.
\objscalex*N*	***N*** is the horizontal scaling percentage.
\objscaley*N*	***N*** is the vertical scaling percentage.

Table 1: Object dimensions and attributes that may be present in RTF header.

If the malicious RTF exploit object has a graphical representation (most phishing attachments do), the object dimensions are crafted inside the weaponizer script and included in the strings of the malicious RTF exploit. An extended study of multiple RTF weaponizers and malicious RTF files targeting numerous vulnerabilities proved that the object dimension are very often unique numbers.

Specifically, the object height and width were frequently found to be unique and it was observed that they never changed across the usage of certain weaponizers, even in instances when the weaponizer was being utilized by multiple actors deploying diverse shellcode. Whereas the RTF obfuscation and final delivered payload may change, the RTF object dimensions were found to remain constant.

Interestingly, RTF object dimensions are rarely used by anti-virus (AV) engines to detect malicious RTF files. This current lack of object dimension-based detection may be why developers do not need to change object dimension to bypass AV engines. On the other hand, metadata, obfuscation and shellcode (all used in other attribution techniques) tend to be changed regularly by actors attempting to bypass AV detection. We noticed in multiple cases that, even when the actors were very successful in updating their weaponizer to provide better AV detection evasion, a simple YARA rule tracking the object dimension was able to find the malicious RTF created by a new version of the weaponizer. Figure 5, is the strings section from a malicious RTF sample created by the Royal Road RTF weaponizer. We successfully tracked samples created by this weaponizer via a YARA rule to detect the unique object dimensions. The static AV detections in *VirusTotal*, which are shown in Figure 6, failed to detect many of these samples with accuracy. Specifically, in the sample included in Figure 6, only one AV engine identified the sample as an exploit for CVE-2017-11882. Adversaries were likely able to evade AV detection by manipulating the shellcode and employing updated obfuscation techniques. The use of YARA signatures to detect object dimensions for phishing weaponizers provides researchers with a way to identify malicious RTFs that is independent of adversary obfuscation attempts.

```
ASCII Strings:
======================
\object\objupdate\objemb\objw2180\objh300
\objdata 554567
\objdata 1389E61402000000B0000004571756174696F6E2E330000000000000000000260000D
01\'cdCF11E0A1B11AE1000000000000000000000000000000000003E000300FEFF090006000000000000000000000001000000010000000000000000
\0
0000000000048905D006C9C5B000000000066FE01DABC0A01112
\yxe15478  \32
\object
2\'cd\'cd3
\pnaiud 7f8a
80000B9346F1D8AB808D2588A31C18B098B491483C140FFE13765303739613235323466613633613535666263666659B1545000000E97408000055
```

Figure 5: Object dimension strings from a Royal Road version 2 sample.

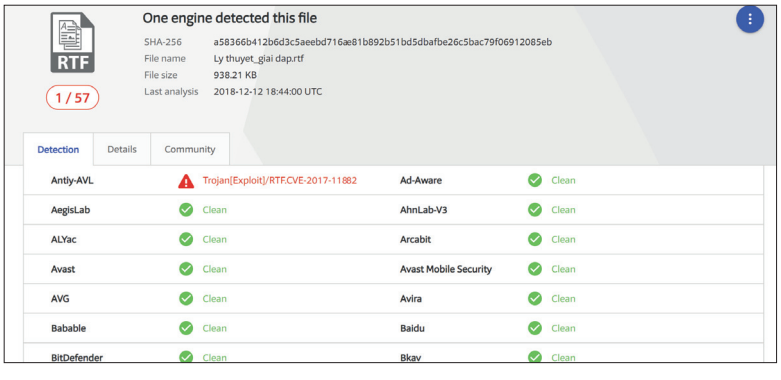

Figure 6: VirusTotal AV detection for Conimes / Goblin Panda RTF sample identified via YARA signature for RTF object dimensions 'objh2180/objw300'.

The tracking of RTF object dimensions has led researchers to identify 27 unique weaponizers that include APT, cybercriminal and public tools. Of the over 6,000 malicious RTF files analysed, 4,445 contained unique object dimensions. This demonstrates how distinct object dimensions are per weaponized RTF sample and reinforces that a cluster of shared object dimensions between samples is an indication that they were likely created by the same weaponizer.

Comparing RTF attribution techniques: pros and cons

Technique	Pros	Cons
Metadata and author name (fleeting & operator-centric)	Operator-centric Provides context via social engineering content and language of targets ('human fingerprint') Can be used to track specific campaigns Actor-specific Easy to track	Trivial to change Not required in all weaponized files Regularly evolving
RTF obfuscation artifacts (evolving & supply-chain-centric)	Unique to shellcode developer Supply-chain-centric Can facilitate attribution and correlations between threat actors Easy to track using YARA rules	Regularly evolving with high turnover so threat actors can bypass AV detection
Shellcode (permanent & operator-centric)	A more permanent actor artifact to track Usually specific to a single actor Difficult for actors to change entirely	Complex to create a signature, specifically utilizing YARA rules to track shellcode
Object dimensions (permanent & supply-chain-centric)	Very specific to weaponizer developer & exploit supplier Does not change regularly Allows attribution of a shared exploit supply chain Maps relations between different connected groups	Does not provide operator visibility If multiple actors are using the weaponizer it does not provide deeper attribution to a specific group

Table 2: Comparison of RTF attribution techniques.

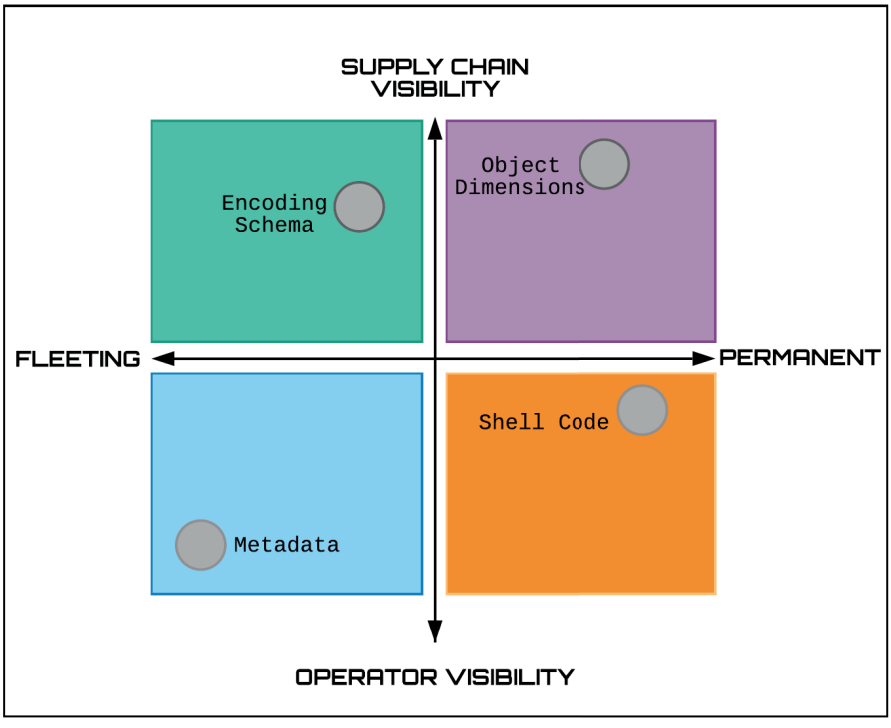

Figure 7: Quadrant view of permanence versus operational visibility in RTF attribution techniques.

THE ROYAL ROAD WEAPONIZER

Researchers have identified a unique phishing weaponizer that, to date, has been utilized in Chinese and South Asian APT targeted attacks, as well as in cybercriminal campaigns. The weaponizer, which has been dubbed 'Royal Road', is believed to be a code base capable of creating weaponized RTF exploits complete with believable lure content for CVE-2017-11882, CVE-2018-0802 and CVE-2018-0798. This weaponizer has primarily been used by Chinese APT actors in espionage campaigns supporting intelligence requirements for the Belt and Road Initiative in Central Asia, Russia, Vietnam and Mongolia, but also with the targeting of US maritime, academic and defence sectors. Specifically, the weaponizer can be identified by the unique object dimensions `objh2180/objw300` appearing in the malicious RTF's strings. Further variations of this weaponizer can be identified by the object data which follows the object dimensions, the metadata associated with the RTF files, and an examination of post-exploitation infection techniques utilized by disparate threat actors.

Versions of the Royal Road tool weaponize RTF files to exploit CVE-2017-11882, CVE-2018-0802, and CVE-2018-0798, which affect the *Microsoft Equation Editor*. CVE-2017-11882 and CVE-2018-0802 were patched by *Microsoft* in November 2017 and January 2018, respectively. The lesser-known CVE-2018-0798 was also patched in January 2018. Since then, RTF files exploiting these vulnerabilities in malspam campaigns pushing malware like LokiBot and Formbook have been

well documented. By now, exploits for *Equation Editor* vulnerabilities are old news, and more than 1,000 samples have been submitted to *VirusTotal* since November 2017. Chinese APT threat actors adapted these popular vulnerabilities into exploits immediately following their disclosure by *Microsoft*. The use of a specific weaponizer to exploit well-known vulnerabilities allows analysts both to attribute In-the-Wild (ItW) samples and to gain insight into the supply chain associated with numerous APTs across international boundaries.

DISTINGUISHING BETWEEN ROYAL ROAD VERSIONS

All identified weaponized RTF samples created by the Royal Road tool were found to share the unique RTF object dimensions `objh2180/objw300`. This shared dimension allowed us to draw connections between diverse samples created by the tool, as variation exists between different versions of the weaponizer which include unique object data spanning five distinct versions. Additionally, two distinct methods for executing post-exploitation payloads were found, which serve as the primary method for distinguishing between Chinese APT activity and activity associated with the Sidewinder APT. Finally, further variation was identified and documented in the methods used amongst disparate Chinese APTs to perform DLL side-loading following execution.

Four distinct clusters of Chinese APT activity have been observed utilizing RTF files that contain the Royal Road unique object dimensions. Version 1 utilizes the object data string `objw2180\objh300{\*\objclass Equation.3}{\*\objdata 01050000020000000B000000457175617400` and exploits CVE-2017-11882. Versions 2 and 4 utilize the object data string `objw2180\objh300{\objdata 554567{\*\objdata 01050000020000000B000000457175617469 6F6E2E` and exploit both CVE-2017-11882 and CVE-2018-0802. Several of these APT groups have utilized exploits for both CVE-2017-11882 (two versions) and CVE-2018-0802 at different times, representing a shared and evolving supply chain between Chinese threat actors. Version 4 of the Royal Road weaponizer was observed being utilized by the Sidewinder APT group, using the object data string `objw2180\objh300{\objdata 554567{{\*\objdata 1389E614020000000B000000457175617469 6F6E2` to exploit CVE-2017-11882. This string is highly similar to the object data string from Royal Road versions 2 and 4.

A fifth variation of the Royal Road builder was also observed in use by Chinese APT actors. The analysed RTF files share the same object dimension (`objw2180\objh300`) as used to track the RTF weaponizer. However, in this case the samples were not exploiting CVE-2017-11882 or CVE-2018-0802. After further analysis, it was discovered that the RTF files were exploiting the CVE-2018-0798 vulnerability in *Microsoft*'s *Equation Editor* (EQNEDT32). CVE-2018-0798 does not appear to be commonly exploited in the wild, even though is more reliable than its better-known *Equation Editor* RCE counterparts. Its reliability is rooted in its efficacy among all *Microsoft Word* versions that include the *Equation Editor*. Its counterparts CVE-2017-11882 and CVE-2018-0802 are limited to specific versions based on the patches that have been deployed. CVE-2017-11882 is only exploitable on an unpatched version prior to its fix, and CVE-2018-0802 is only exploitable on the version released to fix CVE-2017-11882. In contrast, a threat actor utilizing CVE-2018-0798 has a higher likelihood of success because it is not limited by version. Files containing the Royal Road object dimensions and the following string have been classified as Royal Road v5: `objw2180\objh300\objdata\object 5154\781\'e56\'2f7\objdata 01050000020000000b000000457175617 4696f6e2e330000000000000000000002e0000d01`.

Version	Object strings	Description
Royal Road v1	objw2180\objh300{*\objclass Equation.3}{*\objdata 01050000020000000B0000004571756174	No obfuscation Exploits CVE-2017-11882 8.t post-exploitation technique & execution of shellcode Used by Chinese APTs Temp.Periscope and Goblin Panda
Royal Road v2	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000B00000045717561 74696F6E2E	Started using RTF obfuscation gadgets to evade AV detection 8.t post-exploitation technique & execution of shellcode Exploits CVE-2017-11882 Used by Chinese APTs Nomad Panda, Dagger Panda and Goblin Panda
Royal Road v3 (Sidewinder)	objw2180\objh300{\objdata 554567{{*\objdata 1389E614020000000B00000045717561746 96F6E2	Similar RTF obfuscation gadgets to v2 Post-exploitation uses HTA download & execution of shellcode Exploits CVE-2017-11882 Used by Sidewinder APT
Royal Road v4	objw2180\objh300{\objdata 554567{*\objdata 01050000020000000b00000045717561 74696f6e2	Similar RTF obfuscation gadgets to v2. 8.t post-exploitation technique & execution of shellcode Exploits CVE-2018-0802 Used by Nomad Panda, Dagger Panda, Goblin Panda, the group responsible for the Reaver malware, and Temp.Hex
Royal Road v5	objw2180\objh300\objdata\object 5154\781\'e56\'2f7\objdata 01050000020000000b0000004571756174696 f6e2e330000000000000000002e0000d01	8.t post-exploitation technique & execution of shellcode Exploits CVE-2018-0798 Used by Nomad Panda, Dagger Panda, Goblin Panda, and Temp.Hex

Table 3: Table comparing the different versions of Royal Road weaponizer.

Among the Chinese groups to use Royal Road are the APTs Goblin Panda (Conimes), Temp.Trident (Dagger Panda and Nomad Panda, Ice Fog), Temp.Periscope (APT40, Leviathan, MudCarp), the APT group associated with the Reaver malware, and Temp.Hex (Maudi Surveillance Operation). Goblin Panda (Conimes) has historically targeted Vietnam, utilizing Royal Road RTF phishing attachments to deliver a payload identified as 'QCRat'. This payload is identifiable via the vulnerable *McAfee* DLL that was utilized for DLL side-loading (QCLite.dll and QCConsol.exe). This group has subsequently utilized additional malicious PE files side-loaded by legitimate dynamic-link libraries (DLLs) as well as PowerShell scripts in phishing campaigns to deliver malware families including Newcore RAT and Gh0st. Royal Road RTF samples are often attributable to Conimes by their distinctive Vietnamese language lures and file names, as well as through recognizable post-infection DLL side-loading techniques.

Actor	**Targeting**	**Potential motivation**	**Methodology**	**Unique tools**
Goblin Panda (Conimes)	Vietnam and Southeast Asia	Espionage aligned with commercial and South China Sea issues	RTF phishing followed by shellcode executed via an OLE package dropping distinctive source file 8.t	QCRat Gh0st Newcore
Temp.Periscope (APT40, Leviathan, MudCarp)	US Defence; maritime; academic institutions; international & political organizations	Intellectual property theft and military espionage	RTF phishing followed by shellcode executed via an OLE package dropping distinctive source file 8.t	DadBod EvilTech AirBreak HomeFry MurkyTop
Nomad Panda & Dagger Panda (Temp.Trident, Icefog)	Mongolia and Central Asia	Economic espionage for Belt & Road Initiative	RTF phishing followed by shellcode executed via an OLE package dropping distinctive source file 8.t	Fucobha Icefog (shared) Gh0st
Temp.Hex (The Maudi Surveillance Operation [5])	Mongolia	Local Chinese interests, human rights activists, Mongolian diplomatic affairs	RTF phishing followed by shellcode executed via an OLE package dropping distinctive source file 8.t	FireShadow Poison Ivy Maudi Tool Suite PlugX
APT responsible for the Reaver malware	SE Asia and India. Areas associated with dissidents tied to the Chinese Five Poisons	Five Poisons targeting	RTF phishing followed by shellcode executed via an OLE package dropping distinctive source file 8.t	Reaver Sun Orcal

Table 4: Table characterizing Chinese APT groups utilizing the Royal Road weaponizer.

Temp.Periscope (APT40, Leviathan) has historically targeted US and international institutions associated with naval and maritime issues affecting the South China Sea while supporting the theft of intellectual property. This was the first group observed utilizing the Royal Road weaponizer, however, it appears to have ceased using it around December 2017 following patch adoption for CVE-2017-11882.

Temp.Trident (Dagger Panda & Nomad Panda, Icefog) has historically targeted the Mongolia region (Dagger Panda) alongside Russia and Central Asia (Nomad Panda), likely as part of economic espionage efforts in support of the Chinese Belt and Road Initiative. Versions of the custom payload 'Fucobha' or 'Icefog', which was first identified in 2013, have been identified as part of these campaigns. These campaigns have also leveraged more common payloads utilized by Chinese APT groups like Gh0st RAT. Historically, Royal Road RTF samples attributed to this APT have included distinctive RTF metadata author information that recurs across campaigns.

The APT group responsible for the Reaver and Sun Orcal malware is also believed to utilize the Royal Road exploit builder. This group was the first to be observed utilizing Royal Road v4, which exploited CVE-2018-0802. Historically, this group is known to target groups that oppose the Chinese governmental doctrine of 'One China'. The targeted groups are often referred to as 'the Five Poisons' and include acolytes of Falun Gong, Muslim Uyghurs, supporters of Chinese democracy, supporters of an independent Taiwan, and Tibetans. Since these groups consist primarily of dissidents, the geography associated with Reaver and Sun Orcal targeting is diverse and is believed to be any location where these populations reside. Researchers at *Cylance* publicized Reaver RTF exploits built using the Royal Road tool in May 2019 and reinforced the observation of tool sharing among Chinese APT groups at that time [6].

Another Chinese APT group known to target Mongolia has been identified through this research. The APT known as Temp.Hex and the Maudi Surveillance Operation has been observed utilizing the Royal Road v5 weaponizer. In addition to these distinct Chinese APTs using a common RTF weaponizer, they all share a common post-exploitation execution technique. Rather than downloading and executing a malicious file, the RTF document drops and executes shellcode via an encoded OLE package which then drops a distinctive source file named '8.t' to execute a payload. This method was identified earlier by security analysts in open sources. *Anomali Threat Research* identified the presence of the unique object dimension `objw871\\objh811\\objscalex8\\objscaley8` in RTF files involved with this post-exploitation method. Signature alerts for this object's dimensions indicate the use of the 8.t exploitation technique. The presence of both a shared phishing weaponizer and a shared post-exploitation execution technique between these groups is indicative of a significant TTP overlap. It is noteworthy that, after the use of the 8.t source file that is dropped to the temp directory, different files, registries and DLLs are used to execute the malicious payload on the host. The weaponizer and exploitation techniques are shared, but different post-infection techniques and payloads are utilized. Varying degrees of overlap have been observed between the post-exploitation techniques of the five Chinese APTs using the Royal Road weaponizer.

An attribution timeline of publicly available samples is shown in Figure 8.

Unlike the Chinese groups, limited use of the Royal Road weaponizer by the Indian APT actor Sidewinder has been observed. Only version 3 of the weaponizer and three total samples have been observed. Specifically, the RTF exploit for CVE-2017-11882 utilized by Sidewinder contains the string `objw2180\objh300{\objdata 554567{{\*\objdata 1389E614020000000B00000045717561746 96F6E2`. These dimensions and format are notably

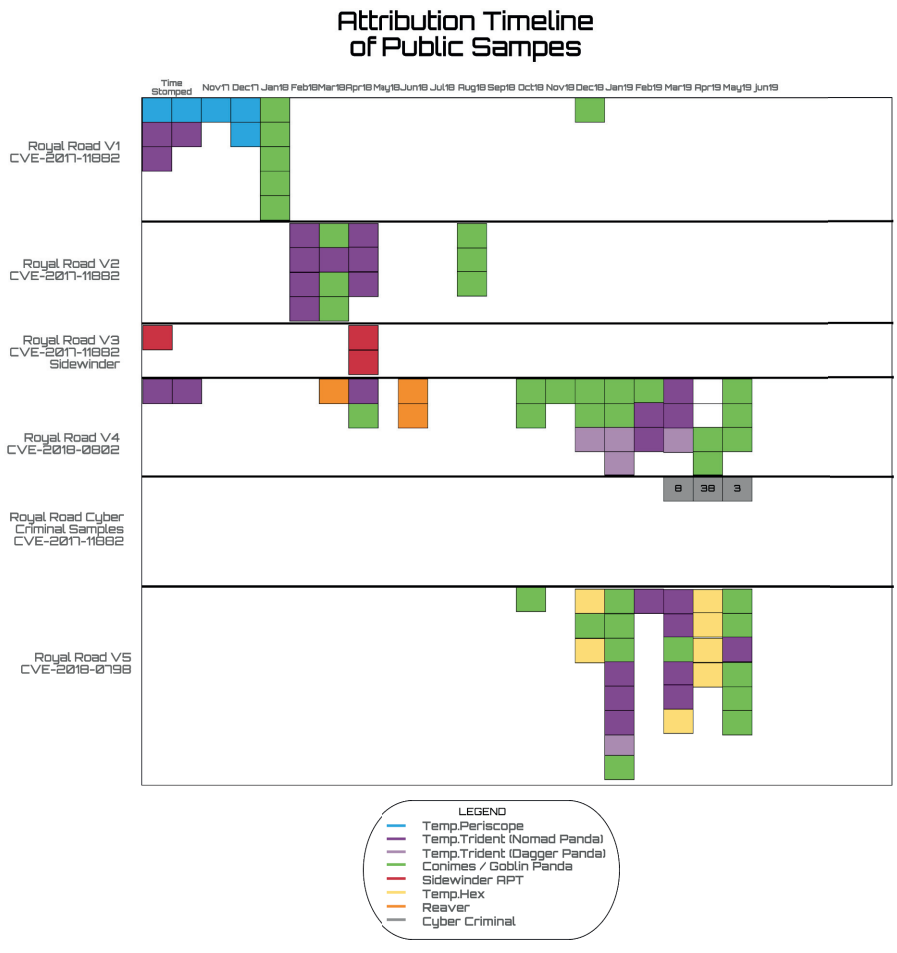

Figure 8: Attribution timeline of public Royal Road RTF samples.

similar to the format observed in the Royal Road CVE-2017-11882 v2 tool used by Chinese groups with only the object data obfuscation gadget varying between the samples. The post-exploitation methodology used by the Sidewinder operators deviates completely from what is utilized by other APT groups. The RTF downloads and executes a payload via an HTA file. The Sidewinder APT has historically targeted organizations linked to the Pakistani Military and is believed by security researchers to be an actor associated with Indian espionage interests, possibly operating as a contractor in the space. However, the use of weaponized RTF files with unique object dimensions in phishing campaigns relies on the successful exploitation of CVE-2017-11882, in which the opened RTF file downloads and executes HTA files on the victim's machine. Primarily English language phishing files that utilize topics involving the military borders of India, China and Pakistan were weaponized and required execution by the victim to pull down additional files including a malicious

HTA file. Once the HTA file was downloaded from a C2 domain and executed, a PowerShell payload contained in the HTA file was executed on the victim's system. Another noteworthy aspect of the use of the Royal Road weaponizer by the Sidewinder APT is that it was extremely brief. Three samples have been identified from mid-2018. Subsequent Sidewinder campaigns have been identified which suggest that the group is no longer utilizing RTF files as their initial phishing attachments, but are rather using '.docx' files which download RTFs that exploit the *Equation Editor* exploit CVE-2017-11882. These new RTFs do not contain object dimensions.

Utilization of the Royal Road weaponizer v5 exploiting CVE-2018-0798 was attributed to Temp.Trident (Nomad Panda and Dagger Panda), Conimes (Goblin Panda) and Temp.Hex. Researchers were able to identify multiple samples of malicious RTF documents using this weaponizer in the wild. However, determining a precise date of first use is challenging. Some of the analysed samples have a creation date of 19 November 2017 (five days after a patch was released for CVE-2017-11882) – however, that date appears to be manipulated based on the recent compilation dates of the payloads observed, many of which date to 2019. Researchers place a likely date of first usage in the wild around October 2018 based on a sample (e228045ef57fb8cc1226b62ada7eee9b) with a *VirusTotal* submission date of 29 October 2018 with the RTF creation time of 23 October 2018. This earliest observed sample has been attributed to Conimes. Multiple samples analysed by security researchers that we associate with CVE-2018-0798 have been mentioned in previous instances and detection signatures by others in the security community. We believe that some of these samples were misattributed to CVE-2017-11882 or CVE-2018-0802 based on their exploitation of the *Equation Editor*, despite being classified as CVE-2018-0798.

COMMODITY ACTORS ADOPT ROYAL ROAD

After the brief utilization of Royal Road by the Sidewinder APT and its continuous utilization by Chinese APT groups, a new pattern of usage emerged. On 10 March 2019, analysts discovered a new man-in-the-middle (MitM) phishing campaign that appeared ultimately to deliver the Formbook malware via CVE-2017-11882 RTF exploits. The campaign delivered malicious attachments to users in the address books of compromised victims. These weaponized RTF attachments included the object dimensions of the Royal Road weaponizer, `objw2180\\objh300`, along with additional object dimensions `objw1479\\objh975`.

Figure 9: Unique object dimensions present in weaponized commodity RTF attachments.

The malicious emails, while sharing a broad geographic clustering, did not appear to be targeted in nature because victims existed in different sectors and the phishing lures were found to have commodity purchase order and invoice themes. The use of the Formbook malware in MitM phishing attacks is not unique in itself. However, the tool that threat actors used to weaponize RTF phishing attachments for this campaign had only previously been used by the Chinese and Indian APT actors noted previously.

A similar campaign was observed on 6 May 2019 utilizing a tariff-themed phishing lure. After the user had executed the malicious RTF attachment it exploited CVE-2017-11882. This gave access to the svchost.exe and wmiprvse.exe processes via Remote Process Calls (RPCs). Wmiprvse.exe then spawns a command line shell as a child process that is used to execute the file '~afer125419.tmp'. This file is created on the host by a Visual Basic script that was previously downloaded from the *Pastebin* URL pastebin[.]com/raw/9t3R1Ng5 by the malicious RTF.

```
<html>
<head>
<script language="VBScript">
Window.ReSizeTo 0,0
Sub sbWait(iSeconds)
    Dim oShell  : Set oShell = CreateObject("WScript.Shell")
    oShell.run "cmd /c ping localhost -n " & iSeconds,0,True
End Sub
Sub window_onload
        const impersonation = 3
        Const HIDDEN_WINDOW = 12
        Set Locator = CreateObject("WbemScripting.SWbemLocator")
        Set Service = Locator.ConnectServer()
        Service.Security_.ImpersonationLevel=impersonation
        Set objStartup = Service.Get("Win32_ProcessStartup")
        Set objConfig = objStartup.SpawnInstance_
        objConfig.ShowWindow = HIDDEN_WINDOW
        Set Process = Service.Get("Win32_Process")
        Error = Process.Create("cmd /c echo|set /p ""=MZ"">%temp%\~F9.TMP", null, objConfig, intProcessID)
    sbWait(2)
        Error = Process.Create("cmd /c copy /B %temp%\~F9.tmp+%temp%\~191AEF9.tmp %temp%\~AFER125419.tmp", null, objConfig, intProcessID)
        sbWait(2)
    Error = Process.Create("cmd /c %temp%\~AFER125419.tmp", null, objConfig, intProcessID)
        sbWait(2)
        Error = Process.Create("cmd /c copy %temp%\~AFER125419.tmp ""%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\winhost.exe""", null, objConfig, intProcessID)
        window.close()
end sub
</script>
</head>
</html>
```

Figure 10: VBScript used to create malicious ~afer125419.tmp file.

In some samples from this campaign, the VBScript was found within a malicious HTA file that was downloaded directly from a C2 domain by the initial malicious RTF rather than from the above-referenced *Pastebin* URL. Notably, each of the malicious RTF files includes the RTF metadata author tag 'n3o'. This metadata information has been associated with malicious purchase order and invoice phishing campaigns since at least 2017. Specifically, the 'n3o' metadata author tag has been present in identified RTF phishing files that exploited *Equation Editor* vulnerabilities (CVE-2017-11882 and CVE-2018-0802) from both May 2018 [7] and December 2018.

The adoption of Royal Road by an additional commodity actor occurred in April 2019. The object dimensions `objw2180\\objh300` were seen in a malspam campaign which appears to have delivered the commodity ransomware Osiris, which is an older variant of the Locky ransomware. The campaign leveraged IT themes within its phishing lures and specifically referenced a *Samsung* printer [8]. The weaponized RTFs all included the metadata author tag 'wuyan' and included phishing lure themes from invoices, to payment documents and purchase orders. 'Wuyan' is also a known metadata author tag that has been associated with commodity campaigns that did not utilize the Royal Road weaponizer.

WEAPONIZER LIFE CYCLE

Phishing weaponizers are created, sold and distributed in the cyber threat landscape in a similar fashion to zero-day vulnerabilities and proof-of-concept (PoC) exploits. Like zero-day exploits, a weaponizer tool consisting of code that builds phishing exploits that target vulnerabilities has the most value (both in monetary and operational terms) prior to a vulnerability's disclosure. During this period often a single sophisticated actor is seen developing a weaponizer for a zero-day that has been identified through targeted vulnerability research. Upon a vulnerability's disclosure by a PoC or product vendor, a period of rapid tool development by multiple actors often occurs during the time when a vulnerability is unpatched ('1 Day') and during the initial 90 days following the release of a patch. Ninety days is a common duration for patch implementation at large enterprises, however, patching may occur faster or slower based on criticality prioritization within an organization. The current US Department of Defense Cybersecurity Discipline Implementation Plan strives to have all systems patched within 21 days of patch release and provides for the network removal of high-risk unpatched devices after a 120-day period [9]. During the initial patch-adoption period, targeted phishing attacks for a disclosed vulnerability will have a high success rate based on the limited degree of deployed patches in the threat landscape. Therefore, the largest number of new weaponizers for a specific vulnerability will be observed during this period.

Following the initial patch-adoption period, continued adoption, innovation, and diffusion of weaponizer tools is often observed with usage by less sophisticated actors including cybercriminal and commodity adversaries involved with malspam distribution. This adoption of once-sophisticated weaponizers by unsophisticated actors is accompanied by a decrease in the effectiveness of the targeted attacks that make use of the weaponizer because the number of patched machines rises over time. Although less effective in targeted attacks, late-stage weaponizer usage for large-scale, untargeted commodity campaigns like malspam allow additional value to be derived from a weaponizer like Royal Road. Late-stage actor adoption of such tools can be further driven by the publication of research that may include both samples and code writeups, allowing adversaries to adopt or recreate the published weaponizer.

The diagram shown in Figure 11 maps the adoption of the Royal Road weaponizer for CVE-2017-11882, CVE-2018-0802 and CVE-2018-0798 by multiple APT and cybercriminal adversaries. Royal Road has not been found to be a tool that exploited these CVEs as zero-days. CVE-2017-11882 and CVE-2018-0802 were disclosed in the threat landscape and patched by *Microsoft* in close succession. It is likely that sophisticated APT groups like Temp.Periscope immediately began developing or purchased a functional weaponizer for CVE-2017-11882 in the days following disclosure. This conclusion is based on the first functional Royal Road sample being observed just four days after the disclosure of CVE-2017-11882. Conimes/Goblin Panda was also seen utilizing the same weaponizer and post-infection DLL hijacking methodology within the initial 90-day patching cycle. Meanwhile, the APT group responsible for Reaver malware was found to be utilizing a functional exploit for CVE-2018-0802 created by the Royal Road builder within 90 days of initial exploit disclosure.

Following the initial patching period, new variations of the Royal Road weaponizer began to emerge, with Goblin Panda and Nomad Panda deploying an updated version that exploited CVE-2017-11882. These Chinese APT groups were subsequently observed adopting the Royal Road weaponizer version that now exploited CVE-2018-0802, first used by the Reaver Group. The Sidewinder APT, which is believed to originate from South Asia, was also seen briefly utilizing a different version of the Royal Road weaponizer for CVE-2017-11882 following the initial 90 days after patch disclosure.

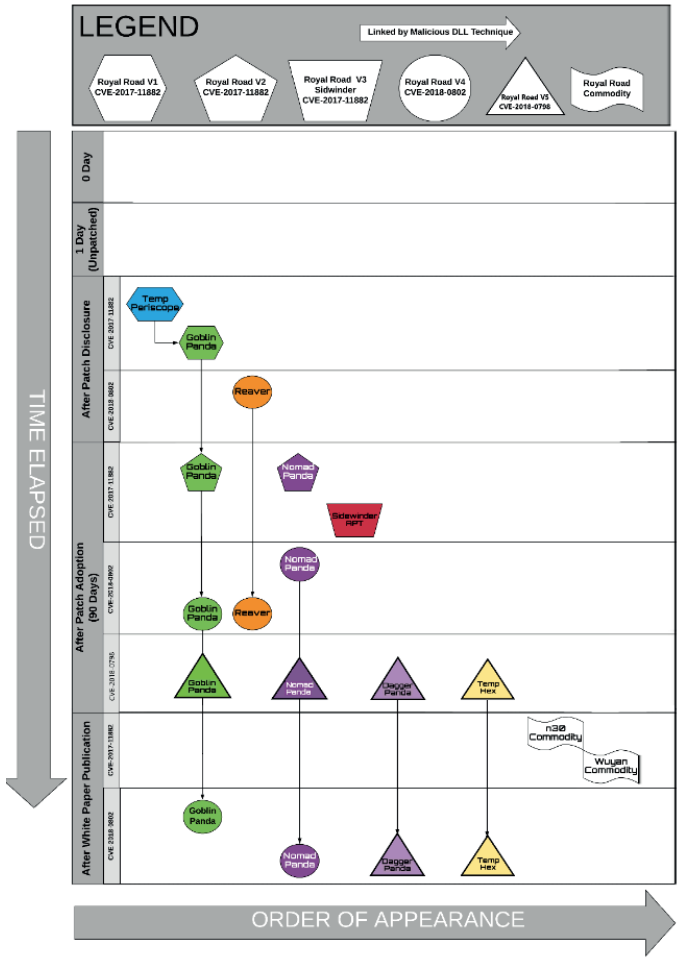

Figure 11: Royal Road adoption timeline.

The usage of the Royal Road version 4 weaponizer for CVE-2018-0802 persisted past the initial patching period and also continued following *Anomali*'s publication regarding the Royal Road tool that was released in February 2019 [10]. Interestingly, in the period following publication, an additional cluster of phishing emails using Royal Road version 5 were identified targeting Mongolian speakers that appeared to be related to a Chinese APT group referred to as Temp.Hex by *FireEye* and the Maudi Surveillance Operation by *Norman Shark*. Specifically, a Royal Road RTF attachment named 'Цэргийн багийн 8 ээлж ашиглагдах утасны дугаарын жагсаалт.doc', which translates to 'List of telephone numbers to be used in the 8th Military Team.doc' (1e78ebbfb5fd1ee66f44030d52f80806d184e6daa00dd7aaa1a30b53c629912d) was found to utilize the C2 mtanews.vzglagtime[.]net, which resolved to the IP 217.69.8[.]255 at the time of analysis [11]. The same IP was observed to be the C2

host used by a FIRESHADOW malware payload in a campaign in January 2019 which *FireEye* attributed to Temp.Hex and identified as targeting Mongolian transportation and telecommunications sectors. Additionally, another RTF file that *FireEye* associates with that January campaign (5cc1272272a6de91e1c43832f289c73f) utilizes the same post-infection mechanism for DLL side-loading as the above Royal Road sample. The samples drop the encoded 8.t file to the temp folder. When this file is decoded it is the malicious executable winhelp.wll. The malicious EXE is then copied to the following directory as %APPDATA%\Intel\Intel(R) Processor Graphics\RasTls.dll and side-loaded using the legitimate executable IntelGraphicsController.exe. It is worth noting that the malicious executable file name 'winhelp.wll' has historically been observed in campaigns linked to Dagger Panda and Nomad Panda as well.

While the functional CVE-2017-11882 and CVE-2018-0802 were in rapid development by the groups Conimes, Temp.Periscope and Reaver following their initial disclosure, a slower adoption was observed for CVE-2018-0798. This vulnerability, which also targeted the *Equation Editor*, was utilized by threat actors following the initial 90-day disclosure period. Although the exact date of actor adoption is not known for CVE-2018-0798 samples, since the earliest testing samples appear to be timestomped with dates from 2017, we believe ItW samples emerged in October 2018. The version 5 Royal Road weaponizer identifiable by the obfuscation gadget string `objw2180\objh300\objdata\object 5154\781\'e56\'2f7\objdata 01050000020000000b0000004571756174696f6e2e330000000000000000000002e0000d01` was seen twice in October 2018. This use continued intermittently until April 2019. Following this adoption, Royal Road version 5 exploiting CVE-2018-0798 weaponized RTF files became more ubiquitous among the APT groups, with Temp.Hex and Temp.Trident incorporating the tool in their tactics.

Finally, following the *Anomali* publication on the Royal Road weaponizer, and for the first time since its initial emergence in November 2017, the Royal Road object dimensions began to appear in commodity campaigns delivering malicious RTF files weaponized for CVE-2017-11882. Appearing first in March 2019 and continuing until June 2019, the timing of this release in the commodity landscape is striking. Although unsubstantiated at this time, it is possible that, following the *Anomali* publication about the Royal Road weaponizer, the exploit was released or sold for use by an exploit broker to commodity actors. Whereas the value of an exploit builder is greatest when no one knows of the vulnerability, its value is lowest when in-depth knowledge and detection signatures for a tool have been published. Researchers reiterate that this possibility remains unsubstantiated at this time and recognize that adoption of such a tool by both commodity and Indian APT actors could be the result of reverse engineering a sample encountered through fourth/Nth-party collection. Intermittent use of the Royal Road weaponizer in commodity phishing campaigns does not inform the origin of the tool as being created by an exploit broker or an APT developer. However, its commodity emergence does suggest an attempt to derive broader value from a tool following an open-source publication which previously documented it as part of multiple APT toolkits.

ADDITIONAL THREAT ACTIVITY CLUSTERS BASED ON RTF OBJECT DIMENSIONS

Researchers identified an additional 26 clusters of activity identifiable by their unique object dimensions, as show in Figure 12. It is believed that each of the unique object dimensions and their correlated activity represent a phishing weaponizer being utilized in the wild. The identified activity includes additional weaponizers utilized by the APT groups responsible for the Reaver malware and the

criminal campaigns dubbed 'Gorgon Group' by *Palo Alto Networks* (believed to be associated with the Pakistani APT group Subaat) [12, 13]. Several commodity and unidentified weaponizers were observed that are primarily in use as part of malspam and banking trojan campaigns. Additionally, three public phishing weaponizers were identified in open source as PoCs or *GitHub* projects which have been utilized in a range of campaigns including both cybercriminal and APT activity.

Classification	Object Dimension	CVE	Description
APT	objw2180\objh300	CVE-2017-11882 AND CVE-2018-0802	Royal Road Weaponizer (Chinese 8.t and Sidewinder APT)
APT	objw871\objh811	CVE-2017-11882 AND CVE-2018-0802	Chinese 8.t Groups malicious RTF for dll sideloading
APT	objw7238\objh2929	N/A RTF 2nd Stage w/ XLS Macro Enabled	Gorgon Group (Pakistani Cyber criminal activity related to the Subaat APT group).
APT	objw270\objupdate\objh270	N/A RTF Remote File Loaded by Template Injection	Gorgon Group (Pakistani Cyber criminal activity related to the Subaat APT group).
APT	objw2610\objh1305 AND objw11595\objh5796	CVE-2012-0158	Historic Reaver Weaponizer
APT	objw1500\objh749	CVE-2012-0158 AND CVE-2014-1761	Historic Reaver Weaponizer
Unidentified	objw180\objh340	CVE-2017-11882 OR CVE-2018-0802	Unidentified
Unidentified	objw200\objh220	CVE-2017-11882	Unidentified
Unidentified	objw840\objh360	CVE-2017-11882	Unidentified Cyrillic
Unidentified	objw9355\objh1018	CVE-2012-0158	Possibly related to Dridex. Commodity dropping hawkeye and troldesh. Either CVE-2012-0158 or CVE-2014-1761
Commodity	objw10281\objh11121	CVE-2017-11882 OR CVE-2018-0802	Commodity Wuyan Threat Actor
Commodity	objw1520\objh3560	CVE-2018-0802	Commodity Wuyan Threat Actor
Commodity	objw600\objh822	CVE-2017-11882 OR CVE-2018-0802	Commodity. Wuyan Threat Actor. Drops LokiBot, Hawkeye keylogger.
Commodity	objw564654221000\objh654654000	CVE-2017-11882	Commodity M1st Threat Actor.
Commodity	objw1479\objh975 AND objw2180\objh300	CVE-2017-11882	Commodity n3o Threat Actor.
Commodity	objw2885\objh2759	CVE-2017-11882	Commodity Azorult Payload/Purchase Order Phishing
Commodity	objw1986\objh1016	CVE-2017-0199	Commodity Bankslate Malspam
Commodity	objw600\objh810	CVE-2018-8570	Commodity dropping formbook and ave_maria stealers.
Commodity	objw6088\objh3882	CVE-2017-11882	Commodity MITM compromise scam involving agenttesla and nanocore rat samples.
Commodity	objw7063\objh2887	CVE-2018-0802	Commodity drops formbook and hawkeye keylogger.
Commodity	objw405\objh2036	CVE-2017-11882	Commodity drops azorult, formgrabber, agenttesla, and lokibot
Commodity	objw7244\objh2925	CVE-2017-0199	Commodity drops lokibot and quasar rat.
Commodity	objw9361\objh764 AND objw9361\objh874	CVE-2015-1641	Commodity drops cafebabe js shellcode and troldesh ransomware.
Commodity	objw4321\objh4321	CVE-2017-0199	Commodity. Dimensions also present in public weaponizers for CVE-2018-8174 and CVE-2018-8579.
Public	objw660\objh260	CVE-2017-11882 AND CVE-2018-0802	Public Builder https://github.com/Ridter/RTF_11882_0802/blob/master/RTF_11882_0802.py
Public	objw291\objh230	CVE-2017-0199	Metasploit
Public	objw380\objh260	CVE-2017-11882 OR CVE-2018-0802	Commodity POC for EMBEDI CVE-2017-11882. https://github.com/embedi/CVE-2017-11882/blob/master/webdav_exec_CVE-2017-11882.py

Figure 12: 26 additional RTF weaponizers identified using unique object dimensions.

CONCLUSION

The application of RTF attribution techniques across over 6,000 samples has ultimately identified 27 RTF weaponizers, 18 months of targeted APT activity spanning six adversaries, and has demonstrated the value derived from the analysis of unique object dimensions. While the continued analysis of other aspects of the RTF file format – including metadata, shellcode and obfuscation – remains valuable, object dimensions provide a unique visibility into weaponizer tool usage in the threat landscape. The relative ease and significant return of YARA signatures tracking these dimensions provides network defenders a high-veracity, repeatable method for identifying malicious RTF phishing attachments. This high-value boon to defenders is augmented by the long-term strategic context that tracking object dimension can offer as part of threat actor profiling. Should these object dimensions remain relatively obscure in the static detections employed by anti-virus signatures and therefore insignificant in the eyes of threat actors, we believe that attribution will remain in the object.

REFERENCES

[1] 2019 Data Breach Investigations Report. May 8, 2019. https://enterprise.verizon.com/resources/reports/dbir/.

[2] Raggi, M. A. Schrodinger's Backslash: Tracking the Chinese APT Goblin Panda Using RTF Metadata. SANS Cyber Threat Intelligence Summit. January 22, 2019. https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1548184559.pdf.

[3] Yang, J. How RTF Malware Evades Static Signature-based Detection. FireEye Threat Research. May 20, 2016. https://www.fireeye.com/blog/threat-research/2016/05/how_rtf_malware_evad.html.

[4] Larin, B. How RTF Malware Evades Static Signature-based Detection. Disappearing Bytes: Reverse Engineering the MS Office RTF Parser. February 21, 2018. https://securelist.com/disappearing-bytes/84017/.

[5] Fagerland, S. The Chinese Malware Complexes: The Maudi Surveillance Operation. Seebug.org. 2012. https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2012/NormanShark-MaudiOperation.pdf.

[6] Cylance Research and Intelligence Team. Reaver: Mapping Connections Between Disparate Chinese APT Groups. Threat Vector. May 14, 2019. https://threatvector.cylance.com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html.

[7] https://github.com/decalage2/oletools/issues/307; https://www.anquanke.com/post/id/168455.

[8] Scan from a Samsung MFP Malspam Delivers Locky Osiris. My Security Online. December 08, 2016. https://myonlinesecurity.co.uk/scan-from-a-samsung-mfp-malspam-delivers-locky-osiris/.

[9] United States Department of Defense. DoD Cybersecurity Discipline Implementation Plan. February 2016. https://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf.

[10] Raggi, M. A.; Saad, G. Analyzing Digital QuarterMasters in Asia. Anomali Blog. March 2019. https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain.n

[11] Beaumont, K. Twitter. April 17, 2019. https://twitter.com/GossiTheDog/statuses/1118478326908248064.

[12] Falcone, R.; Fuertes, D.; Grunzweig, J.; Wilhoit, K. The Gorgon Group: Slithering Between Nation State and Cybercrime. Unit 42. August 08, 2018. https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/

[13] Falcone, R.; Ash, B. Aggah Campaign: Bit.ly, BlogSpot, and Pastebin Used for C2 in Large Scale Campaign. Unit 42. April 17, 2019. https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/.

YARA SIGNATURES

```
rule Royal_Road_RTF_weaponizer

{
meta:
    author          = "Anomali"
    tlp             = "GREEN"
    version         = "2.0"
    date            = "2018-11-10"
    hash            = "9d0c4ec62abe79e754eaa2fd7696f98441bc783781d-
8656065cddfae3dbf503e"

    description     = "Detects malicious Royal Road RTF from object dimension"
strings:

$S1= "objw2180\\objh300"
```

```
$RTF= "{\\rt"

condition:

$RTF at 0 and $S1
}
rule RTF_Malicous_Object_8.t_Chinese_APT_Activity

{
meta:
    author          = "Anomali"
    tlp             = "GREEN"
    version         = "2.0"
    date            = "2018-11-10"
    hash            = "9d0c4ec62abe79e754eaa2fd7696f98441bc783781d-
8656065cddfae3dbf503e"
    description     = "Detects malicious RTF from object dimension indicating 8.t
post infection mechanism"

strings:

$S1= "objw871\\objh811\\objscalex8\\objscaley8"
$RTF= "{\\rt"

condition:

$RTF at 0 and $S1
}
```

INDICATORS OF COMPROMISE

Goblin Panda / Conimes

941868f366d65c8859253c869e405c5bbb91e1ed0227090656295c54bb0be9f2
a58366b412b6d3c5aeebd716ae81b892b51bd5dbafbe26c5bac79f06912085eb
9d0c4ec62abe79e754eaa2fd7696f98441bc783781d8656065cddfae3dbf503e
332aa26d719a20f3a26b2b00a9ca5d2e090b33f5070b057f4950d4f088201ab9
bd1e7b42a9c265266b8cc5cc966470497c4f9cba2b247d1f036b6b3892106b52
8f81142a9482c2a96c43c4b325f90794c2a32b61e8261da55f306a36df9ec18c
b70069e1c8e829bfd7090ba3dfbf0e256fc7dfcefc6acafb3b53abcf2caa2253
dd89d33e275e99e288e4c50bdafbb4584a9565189491af0a66f8a506eaf53859
42162c495e835cdf28670661a53d47d12255d9c791c1c5653673b25fb587ffed
c374f7f30b34d95dd99d9cf16f54192d439f830918d342558945e5809809b847
344fbc5e86e6477cdb24848ace149303e22b41f7b01b2eca923109868c1f458f
46714a1fd1a5ce598f761a885857dee8d90b6e7d6f4a303ecaec246a77b58fff
b45087ad4f7d84758046e9d6eb174530fee98b069105a78f124cbde1ecfb0415
44e564ab86be5be2ce5f31c9072cd05adb91663be4904759cbcafa30c5b87660

ab35b2b22718624fcaf1a290b3f138c009469b7449d1a280ec67767ea55b44ae
152f95a5bdf549c5ca789d0dd99d635ee69cca6fe464ced5b39d0316707a4914
f2e28b48ee338fddd97272b191a55641c7835ad687d7b65c8db1c5f747811c57
130daacff74d57bb2319fc5cf815e783c6505883f69e4adcd4c2b1cac3e598ce
eb772b325bdeaaa551a4f50399fe6059bc856e41ba23dd14fbc956605a9c838e
c6a01f392e4c317e6c9b6b3ce860f6368fad7687336ce995246d01fb52b83ca4
bf9987b84b3f7daaa460777e5850a60f10898d0238048d3d5d07d7ec1656e47a
afcbe545dc27d757fb1231019248fdd6b3ec2237e09007656d0ccd4de094f2ef
81f75839e6193212d71d771edea62430111482177cdc481f4688d82cd8a5fed6
d732a7741182741b6c14fdce201b839c8e380be242de034ce764c61778be8fc1
5e7663f662cedcc2c520b88928824a4c7caf5a6833f77cdb0051328d74ace1c8
41f0757ca4367f22b0aece325208799135c96ebe1dcafcd752d3f3c8dd4a5ccf
a9b3b44f048cc145bd4703ead369c9104746966f94b679da51d97bf7b70a26fb
aa4874e3d49e9765797b96aff5262b802352e575deee17308f7539f8916fac33

Reaver

1c6cb02ae9dceb3a647260f409dd837fa5c66794804623c9cf97395cf406d4df
9ac09ea38c9cf11ca13a2c3dbdcfbe0fe4a15cb609be451f7159ecebdd20d311
3df19abbf961a6d795362f5408d65aa5a31e34620aa3518a010d4d6d9e79c60e

Temp.Hex

5e3cd28d9ab02de8d816b7a0719e715330b4ad28cb2d2778a5f54a3396620991
16cb245d9a78c81c25605695a2cf8dbdb36d85bcb61726c56ee358254253df2e
1e78ebbfb5fd1ee66f44030d52f80806d184e6daa00dd7aaa1a30b53c629912d
5e3cd28d9ab02de8d816b7a0719e715330b4ad28cb2d2778a5f54a3396620991
1e78ebbfb5fd1ee66f44030d52f80806d184e6daa00dd7aaa1a30b53c629912d
16cb245d9a78c81c25605695a2cf8dbdb36d85bcb61726c56ee358254253df2e
9be6d671dd901326fc834296fbd2ed015d64e6037e83d8d1d08a9dcdc107cb33
5898e729b7305c4e5db54847396b15d06b74153213a242d295cf64c951a021ca
803c25767414c31259e15f058d62b6102dfe09d3cfacece57f527d7fb2a50632

Temp.Periscope / Leviathan / APT40

c63ccc5c08c3863d7eb330b69f96c1bcf1e031201721754132a4c4d0baff36f8
c92a26c42c5fe40bd343ee94f5022e05647876daa9b9d76a4eeb8a89b7f7103d
c67625e2b5e2f01b74e854c0c1fdf0b3b4733885475fe35b80a5f4bca13eccc7
138d62f8ee7e4902ad23fe81e72a1f3b7ac860d3c1fd5889ed8b8236b51ba64b
c0b8d15cd0f3f3c5a40ba2e9780f0dd1db526233b40a449826b6a7c92d31f8d9

Temp.Trident

f5365387320ae6e6907fd2700f340ba8712cb08f7e52b2ec4dccfe99b3d648ef
9d239ddd4c925d14e00b5a95827e9191bfda7d59858f141f6f5dcc52329838f0
a95bbc1f067783c1107566ed7897549f6504d5367b8282efe6f06dc31414c314
4e1a2f731688f9aab80b1f55d9101bb1cddec08214d4379621c434899a01efbf
597c0c6f397eefb06155abdf5aa9a7476c977c44ef8bd9575b01359e96273486
71c94bb0944eb59cb79726b20177fb2cd84bf9b4d33b0efbe9aed58bb2b43e9c
722e5d3dcc8945f69135dc381a15b5cad9723cd11f7ea20991a3ab867d9428c7
c580d77722d85238ed76689a17b0205b4d980c010bef9616b8611ffba21b142e
87114b56ef4de4500fd0c64af913915f159b95e3cbdb7932772230aae8bfed40
60ac67f0511fc984990e826d44e8a5eddd1ab7f21c7d847ee3a821875260cea6
61488eaafad84e8b86c6a2e87b022e133ccc77701f817c589ef4b01a89dd74ee
f3c120cde34e4e2a45d924ada9e53d3ebc7d73132e359eca8d48f813b6e021a1
ec46e1feed5199a332c76021a8bb446dca37b8e736bcd1e5505f35fb70526a04
5d4de75f7900b6e765d8878234e06d8e07490d5decc6ec5d41c704af38a0abc5
4fce3d38e0a308088cd75c2ef1bb5aa312e83447d63a82f62839d3609a283b02
4123a19cda491f4d31a855e932b8b7afdcf3faf5b448f892da624c768205a289
a3e81e5bbf5beeb9568f0c801b2407e33cf9bcc0c12842d6bd6bc62280add81d
70195e390a5cb92c2e32ded9ef80a935ad7bdda6d6d8e21cc4cf74e98998de32
532b68e6bbcea3980f5fc9a2d939b062b1e3f5f5175267adc158d3a877204e1e
b9e1145546dba4fe2428fdb43566a7eb5ac472bd8b5e5f30998477693a08ede1
e8e86359b06cefdc5c1115dacea21240aa090450e83744b495e784d8bff49a09
5238f8d8c3d16b52d39aa722daff663a5e6307c4b46e360969d84bf409a2690f
97c0ba7e6cb7eb507bb6e9d819786240292f2c3c72e4d7732dd007a9bbf4af5e
69f44ca082ed90c97d9c4ebaae589d7e41c69b02e582cc69886ebfd9cfb93951
4f6b8f51fdaf708bb4fa0dbbc72da50d24f694bce2996eff3df7eeb3c1592e62

Unattributed (Chinese APT) samples

0598a55dad563ffd3d7a0bcdf8699086527104cf3bad1a0d2192fe805bfef84d
fb2bfa7985be5b9855c7b114d3c201540effc6b7cb249256717d6c56cc069b09
484f52e80141809f7482f027f5eadb5305ee1966f55f64656765b7408e1c60dc
52730e7f52afbc6a99d3a83b12b6a8393d1e979e189cffbcf4fba2ff8a7ca99f
3504d4583c59ed0fe6c2d916619714f187638bde835908e02d78cf05b1a9be53
e757993b2cefe2a7dd7ea3e9222cf40e968af1c82370ee5775f768fa29d5efe5
3b593d85b18c9457f8c52cf0f2c5f1f549518f9422d0a5bb10fb1edf4c9ea303
3e04eb55095ad6a45905564d91f2ab6500e07afcdf9d6c710d6166d4eef28185
7079d8c92cc668f903f3a60ec04dbb2508f23840ef3c57efffb9f906d3bc05ff

Sidewinder APT

892859ea9d86fc441b24222148db52eb33cd106c2ac68eafbe83ab0064215488
22062b6bcda194e3734285fed6b2de341c694c52a8f60c9f389f880cefab7644
9001056791a03ec998f26805d462bc2ca336b2c3aeac2e210f73ff841dfe3eec

Formbook 'n3o' commodity campaigns

8ec1e8bc139cbd84858c3997f0635fb5640dbd85f73e8b537e3ae7e14d4870ce
47880521119cee06588476fdcc7c47a91903366671448650830b7dd310c3c3ea
129d74a8f31622e605cea1a03cdac723a5adb002f877c304ef2ceb5f6cdd2654
c81d67472715b6d3bf601147ff8e81f670a429ea0fb8ac3ba82a19c02ad38d0b
c8b5d8f4304725e19edd9ff9e7a8d3325ed06b91adecad691fea23f429072cbd
2f193d55f38d1e4149aa2424f79f184e3059469be4ee386276fb946bdc83bc30
2cfb86699b675919d17beeefa5d993f195358bce6119cc9cebea62d149739421
6e8cd76dba16d159c4e68ed15a60af7f86afb0964ed9d2ebe43c6d6af7749397
herramientasmalls\.com
anthemog\.com
theta-solutions\.net
lucpham\.com
zettacroft\.com
red-lemon\.biz
saleskompass\.biz
dvsprint\.com
esumaile\.com
frenchmole\.com
vip-jinhe\.com
hijaky\.com
theshadegame\.info
angryeggroll\.com
risingsunchicago\.info
uploadbusiness\.com
stlchimneys\.com
oakendalefarmct\.com
letitplay\.online
xn--183j3c007ntbf\.com
legendreality\.com
ysb21\.com
accuratext\.com

itsmcamiracle\.online
erdogandisticaret\.com
xdptb\.info

Wuyan commodity campaigns

299cc5c74b5c44aa4c270da19673f20670b00399038d7ad7dac412b91137a552
30298f89888e5104145ecb1c27053640812a1545f3b7c558ec76fe302d2afb04
2c8ee28cc3884d37019f7b29b37634468fcebaff4a6094564b1443de0c32cbd2
48257a0d98cc8d8c31b449f7e4737507031b06a4165b305b498a8b3f136dcd6b
30298f89888e5104145ecb1c27053640812a1545f3b7c558ec76fe302d2afb04
c9d2728ab7d43379b8b50b3bb05f10bb39f9d073d0ad0e2d533dfab77957d13c
5cd4f11155c34ba32382f297776891d6f2d9f747ffbfdba7594e5c4f1fcd0f59
d3428b542596490f320b86e5473a80249082580713116aaa8299634524507102
511522dd26bafc2aaf46a861e479455695f85fbde0873b23baaebcadec07bd7e
5fae7d03b8113987f3c776f0988af9522688cc9ad53c5072c7cb7ba445e78aef
b40fefbe1835c440da19145d825d8fbdea179d362009364af09e89b1819a6c52
6be40b52667cc4876a3eabf4b671235b053e0e44bf98f80fa5394c3b2030f4eb
0f515163f98845b2b2f85f8a56563a2fe29834643cb067099b209387ff14cb36
8a40970e308c4e00a03a44f7cfb8decf2b788ab054bdc695dbe7225742e15944
4d62e94a8adc8ab177d02ba20af3f50a0bb4a1db995630c5bbb7527c9e46d4be
42afaac637e3f9e805464e2bba017ebbf3d0fd87bbea9482088ed2710683942c
8dda3787bcee130ff447283fa05fdad2f68a73f6d5c321fbf723ced1660af0e5
d1a5280696f1581b0b82a067cff1b5426db0429428ed2553903cc0de3021a764
9341049cd265f8b03bc444de891d4e397cb6daec462e62e50306724fbe0b423f
8a40970e308c4e00a03a44f7cfb8decf2b788ab054bdc695dbe7225742e15944
9b7f09f16cd36ff6b50407e1823d7cf030445ad1e055cf9478ef964419c90580
9fa727fbb18f84d7572dc4017bc3d1410af1c469591317415f53e99c06d68b30
898117f2c43d6cfa52af70df919a366a47f31a7c902ee1bd9e2abfc52cf0b9e5
22c09d51ca46efe5bb00c88841fba6ce23247e7982501fcf5f95e0a64120bef6
07c59af6d98a4606a3b7a82c73a6714a6ac597192877a32e908245921d96d88c
d70e5230a21921169ad729c557a9759879774445648df99eee18aa54b181b2fa
90e3f6e5996b378801c0018d0aaaffd46e9e7a1fa058ad4605edf6a43078d23e
6347b1a237217fc9d736094eb3d32117f8b397ec808614cddc4cda8c190b8548
8414918e868dcacf59abffdfee10f487488381170f3c044338c5cec62693691c
c8ec45b617e378f6fbe29027523d53f20138cc1122f899a7f61320a6acf69226
126853c0b4fe9d83c06fd64cd0306b1d038bad12b2f162777e63dd0850afd7ea
b6f6600d8c655610a2bf3affcaf999b1030d0559ee457b52b2b184e30e95b47e

d74e7786c5c733e88eaccfbc265e155538a504f530e3ce2639c138277418c716
c16f7e2dba5a2c68c0ac0efd8579e9e1260857a1de2c334466c57287e64b67dc
4f57853be12840f120bf8dd4a22f16345536b2e38a4dfaa3b3ba1e3792a6e040
37f464da00d5ea3a3644f3856c13427d2c50c64c4af25b4bc9b3ae3c5837dfb9
bc785e8fec0e308cc587e557f3a7172b7af58bdeaa6a49c298fb2c5375e8ab6a
821eaae98f64db31a6e0dc4b3e4576cc33e8d94b1e122b6397661720704953e1