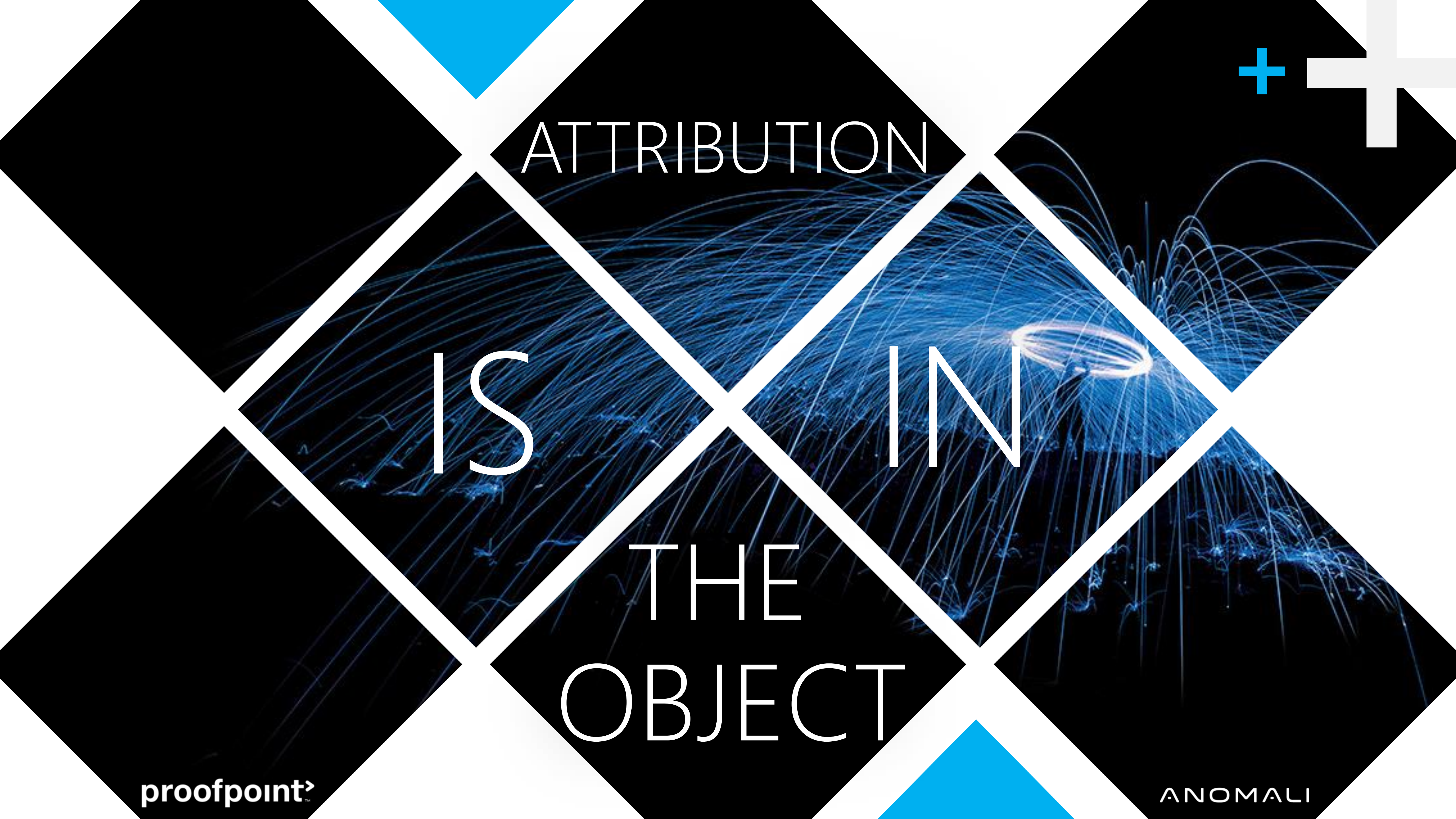
ATTRIBUTION IS IN THE OBJECT



proofpoint

ANOMALI

01

Ghareeb Saad

Threat Intelligence Manager Anomali

Michael Raggi

Senior Threat Research Engineer Proofpoint

02

Threat Research for Threat Analysts

‘Nothing made by a human can avoid personal expression’

-Hrant Papazian
Typographer

ATTRIBUTION IS IN THE OBJECT

Attribution is in the Object:

Using RTF object dimensions to track APT phishing weaponizers.

AGENDA

01 What are malicious Documents weaponizers?

02 Why do we need to track weaponizers?

03 The RTF file format and RTF weaponizers

04 Malicious RTF attribution techniques

05 Case Study: The Royal Road Weaponizer

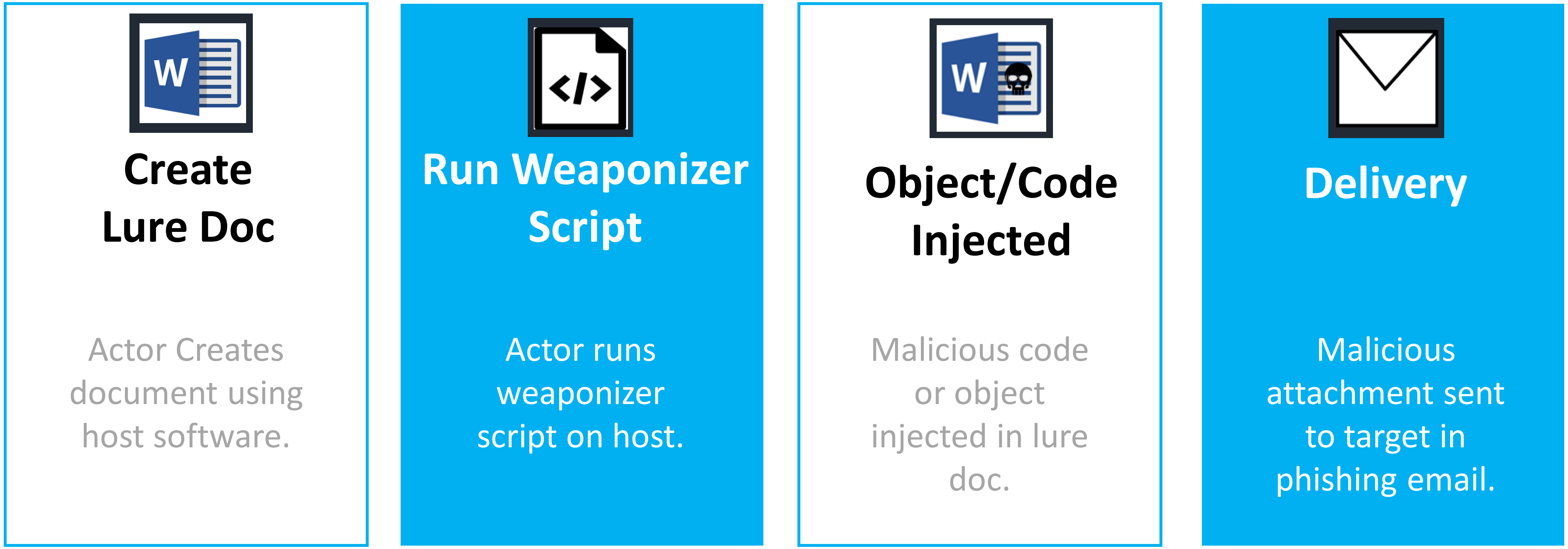
What are Document Weaponizers?

- Document Weaponizers - tools that create malicious attachments using exploits and zero days.

- Distinct tools developed separately from exploits.

- Often python scripts that inject the exploit into a separately prepared document attachment lure.

Phishing Weaponizer Process



Create Lure Doc

Actor Creates document using host software.

Run Weaponizer Script

Actor runs weaponizer script on host.

Object/Code Injected

Malicious code or object injected in lure doc.

Delivery

Malicious attachment sent to target in phishing email.

Why should we track Phishing Weaponizers?

- 2019 Verizon DBIR report cites weaponized ‘Email Attachments’ as the top malware infection vector.
- Weaponizer tracking allows analysts to:
    - Attribute attacks to known sophisticated actors.
    - Identify new payloads
    - Track actor objective & targeting.
    - Track introduction of new exploits into the wild.

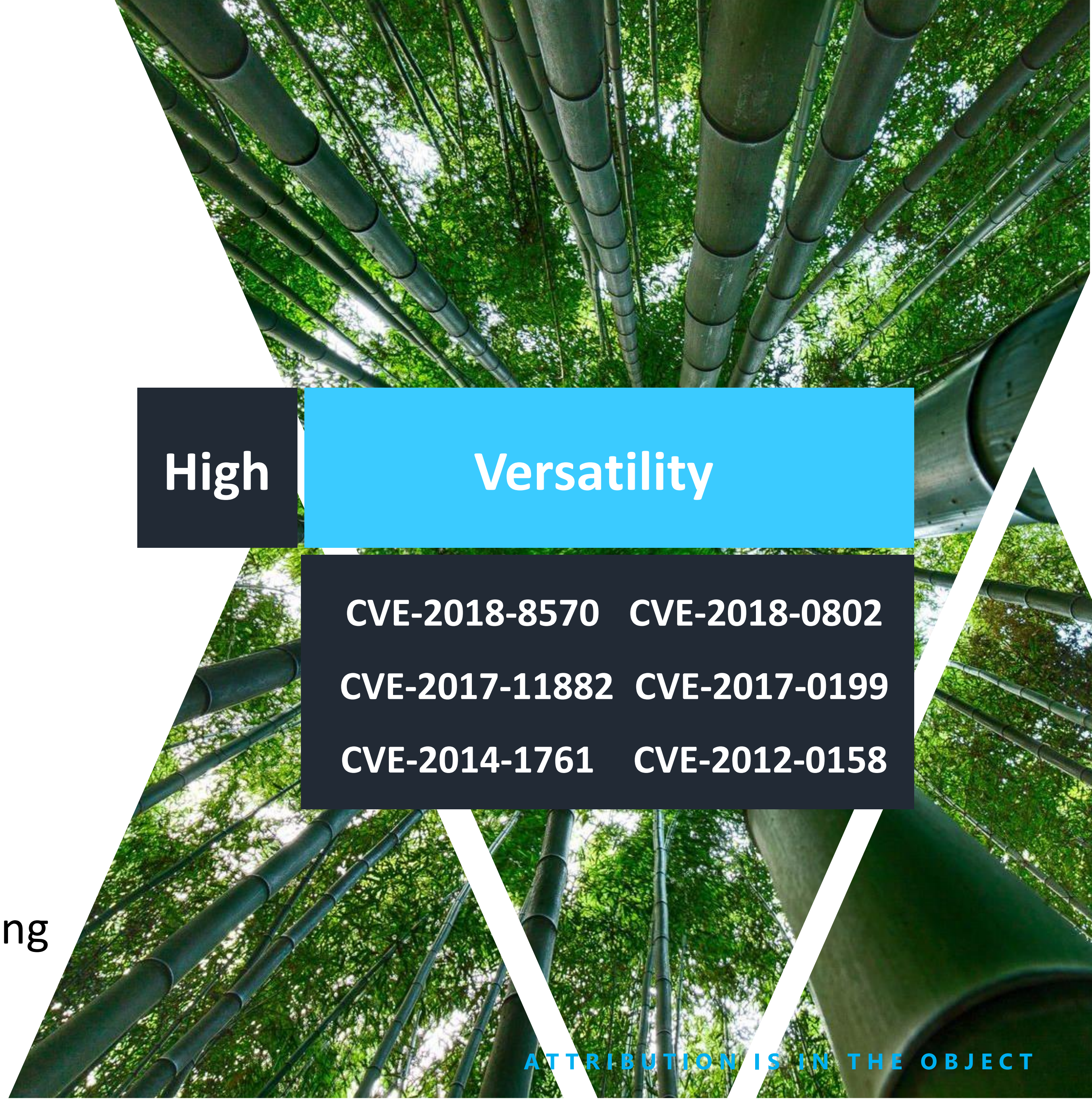
Why RTFs?

- RTF files are among the most popular file formats used in phishing attacks today.
- Their popularity is due largely to their ability to host different object types that can contain versatile CVEs.
- We studied RTFs to find the best methods for tracking, attributing, & alerting on tools that create these files.

This research identified 22 unique RTF phishing weaponizers that exploit six CVE’s ITW. This will share the findings of our research with the CTI community.

The Characteristics of RTF Files

- RTF developed by MSFT in 1987 to enable cross-platform document interchange. (Currently Supported)
- Capable of containing & rendering different object types: Annotations, Fonts, Pictures, OLE, & SWF.
- Various object types allow RTF phishing files to contain diverse CVEs.



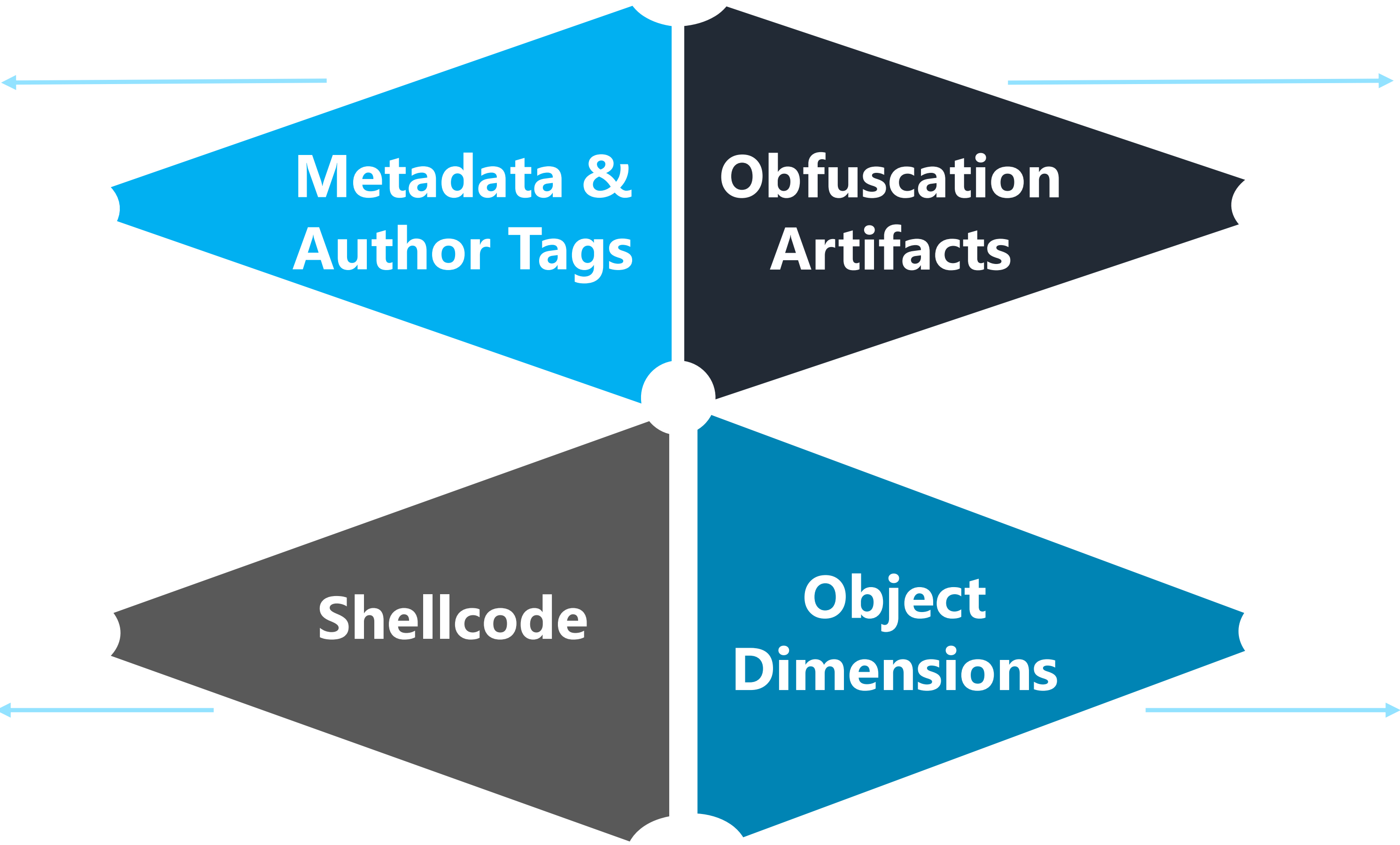
High Versatility

CVE-2018-8570 CVE-2018-0802

CVE-2017-11882 CVE-2017-0199

CVE-2014-1761 CVE-2012-0158

RTF TRACKING & ATTRIBUTION TECHNIQUES



RTF Metadata tags can include persona information.

Metadata & Author Tags

Obfuscation Artifacts

Strings inserted by Actor to obfuscate code.

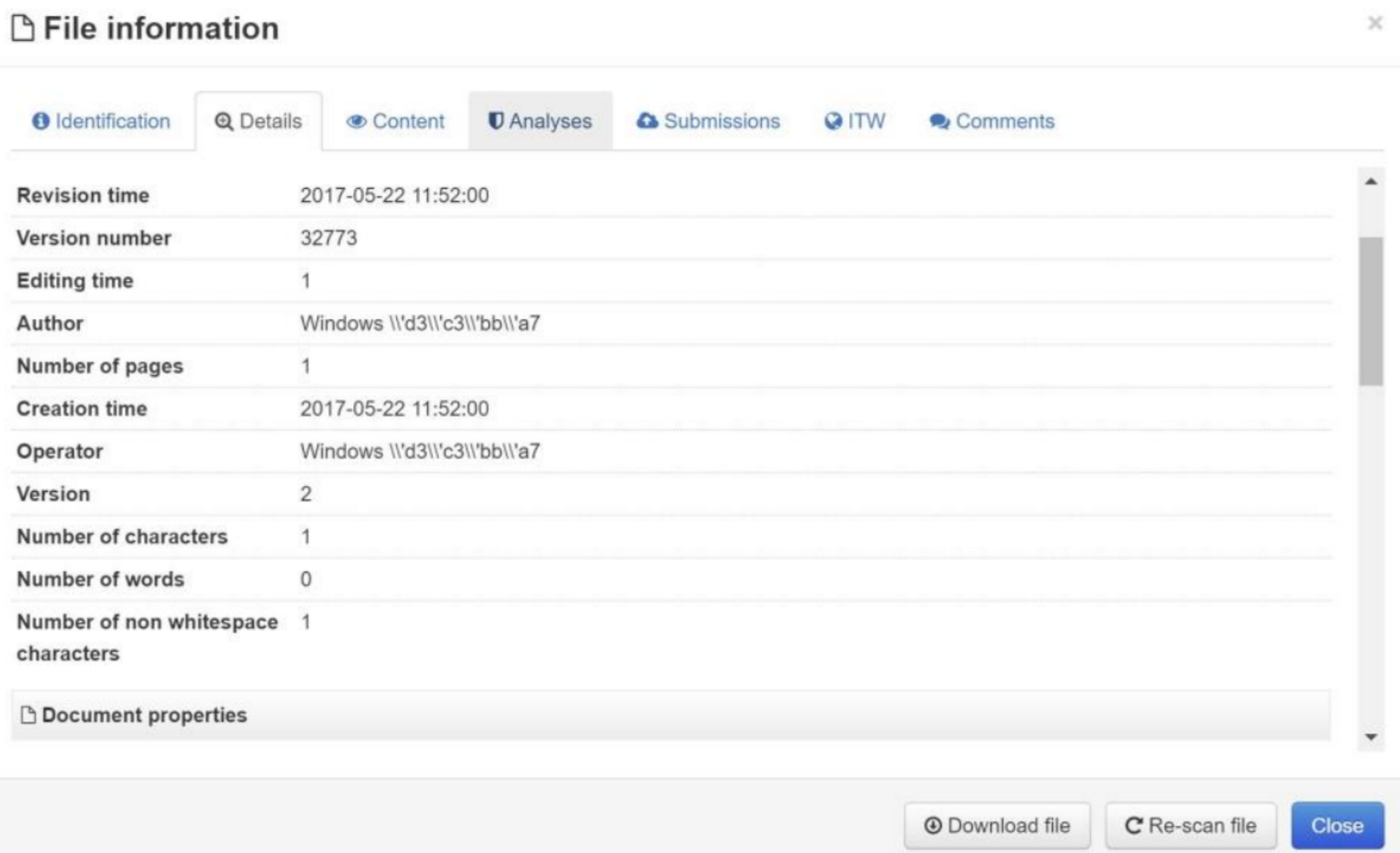
Commonalities in malicious code used by threat actor.

Shellcode

Object Dimensions

Unique dimensions of malicious RTF objects.

Metadata Author + Tag Attribution



File information

Revision time	2017-05-22 11:52:00
Version number	32773
Editing time	1
Author	Windows \\'d3\\'c3\\'bb\\'a7
Number of pages	1
Creation time	2017-05-22 11:52:00
Operator	Windows \\'d3\\'c3\\'bb\\'a7
Version	2
Number of characters	1
Number of words	0
Number of non whitespace characters	1

Document properties

\\'

\'

01 Simple method for tracking RTF files is Metadata tags including Author.

02 RTF metadata tags are applied during Lure document creation

03 Digital artifacts created by the actor's host . Useful for attribution.

ATTRIBUTION IS IN THE OBJECT

Shell Code Attribution

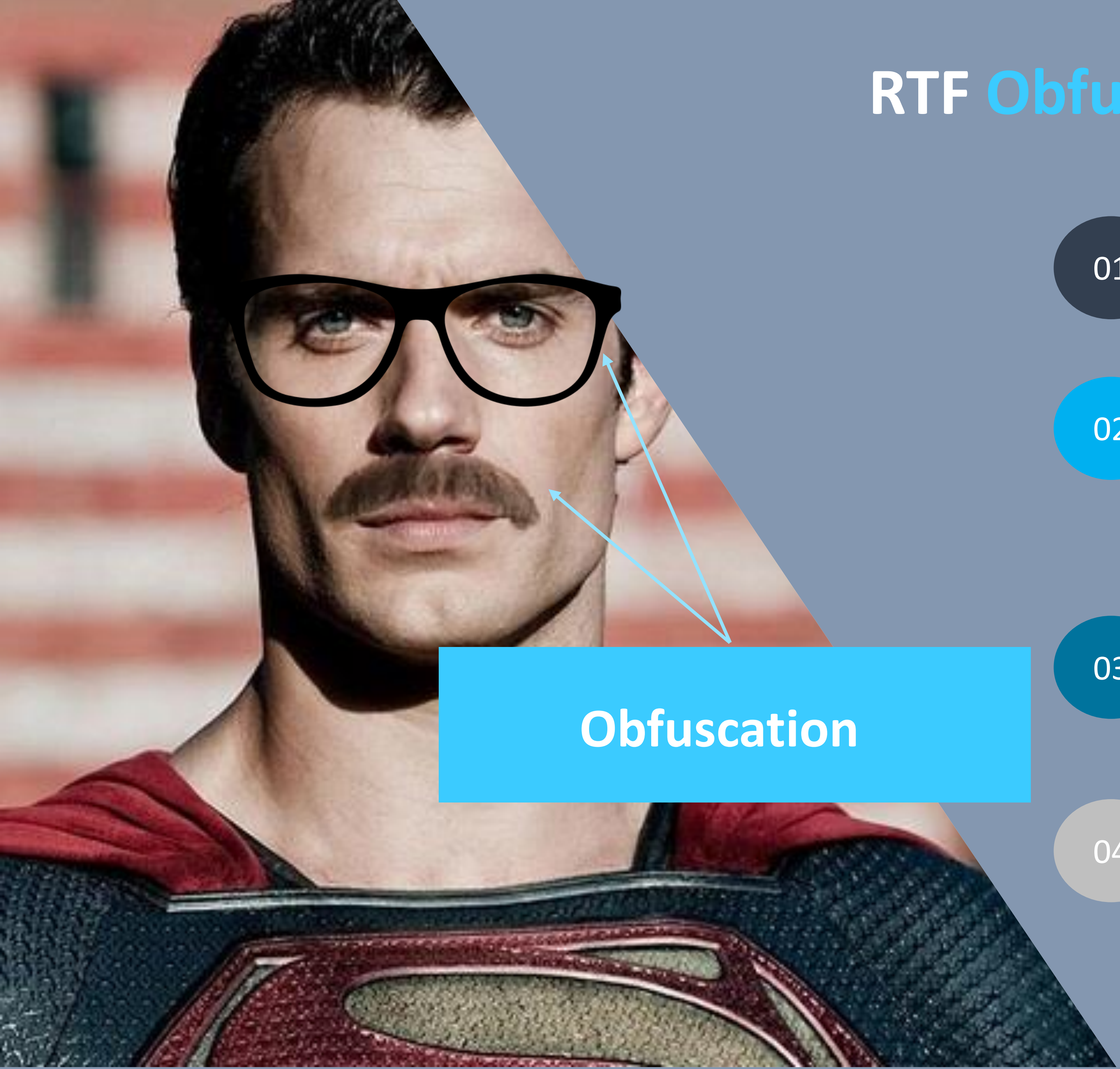
- Shellcode Bytes
- ROP Gadgets
- Egg Hunting Tags
- Dropped Files
- Payload Execution

01 Shellcode is the malicious code used by a threat actor to accomplish infection.

02 Unique aspects of this code are ideal artifacts for actor attribution.

03 Shellcode can be obfuscated and complex to identify and detect with signatures.

RTF Obfuscation Artifacts



01 RTF format is very flexible allows for different obfuscation methods.

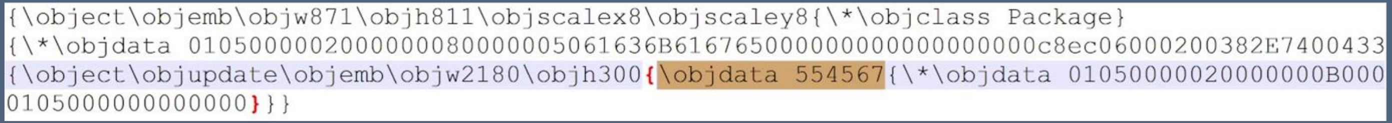
02 Actors will use this flexibility to obfuscate payloads and make static detection challenging.

03 Some obfuscation gadgets are unique to certain actors.

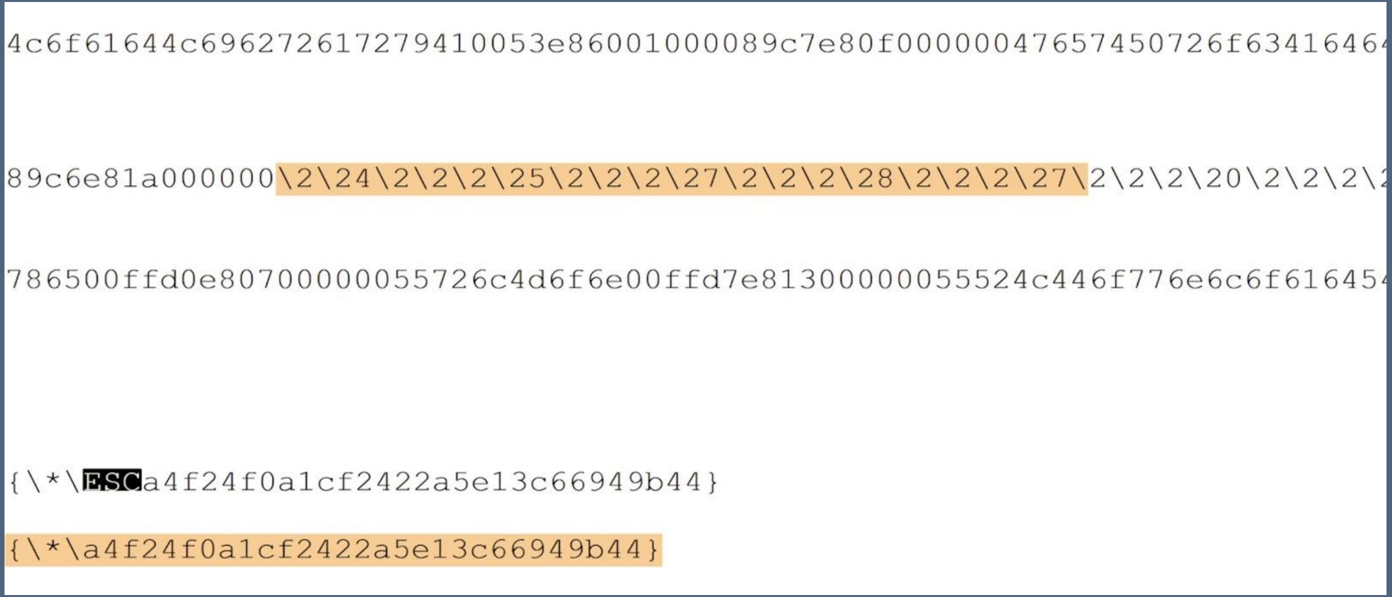
04 Obfuscation content (strings) make great signatures!

RTF Obfuscation Techniques

- Object data Cascading
- Different data representation options
- Use of escape characters
- Spaces and invalid tags
- Control strings and hexadecimal characters

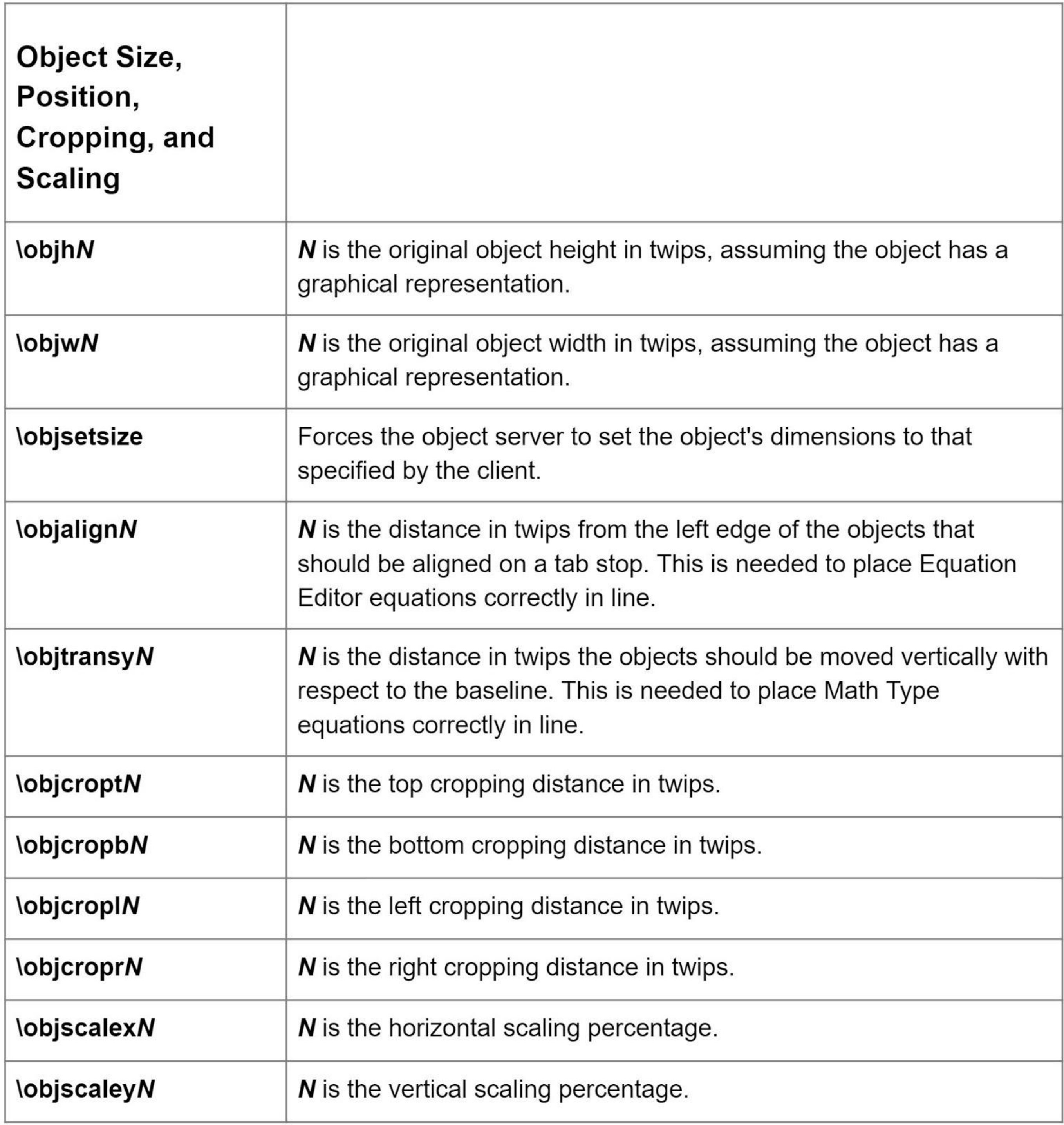


```
{\object\objemb\objw871\objh811\objscalex8\objscaley8{\*\objclass Package}
{\*\objdata 010500000200000008000000005061636B6167650000000000000000000c8ec0600200382E7400433
{\object\objupdate\objemb\objw2180\objh300{\objdata 554567{\*\objdata 0105000002000000B000
0105000000000000}}}
```



```
4c6f61644c696272617279410053e86001000089c7e80f000000476574507 26f6341646

89c6e81a000000\2\24\2\2\2\25\2\2\2\27\2\2\2\28\2\2\2\27\2\2\2\20\2\2\2\

786500ffd0e8070000000055726c4d6f6e00ffd7e813000000055524c446f776e6c6f61645


{\*\ESCa4f24f0a1cf2422a5e13c66949b44}

{\*\a4f24f0a1cf2422a5e13c66949b44}
```

RTF Object Dimensions



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 that 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 Math Type 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.

01 Some RTF objects can have graphical representations.

02 These object dimensions representations are included in the RTF object definition. (Strings)

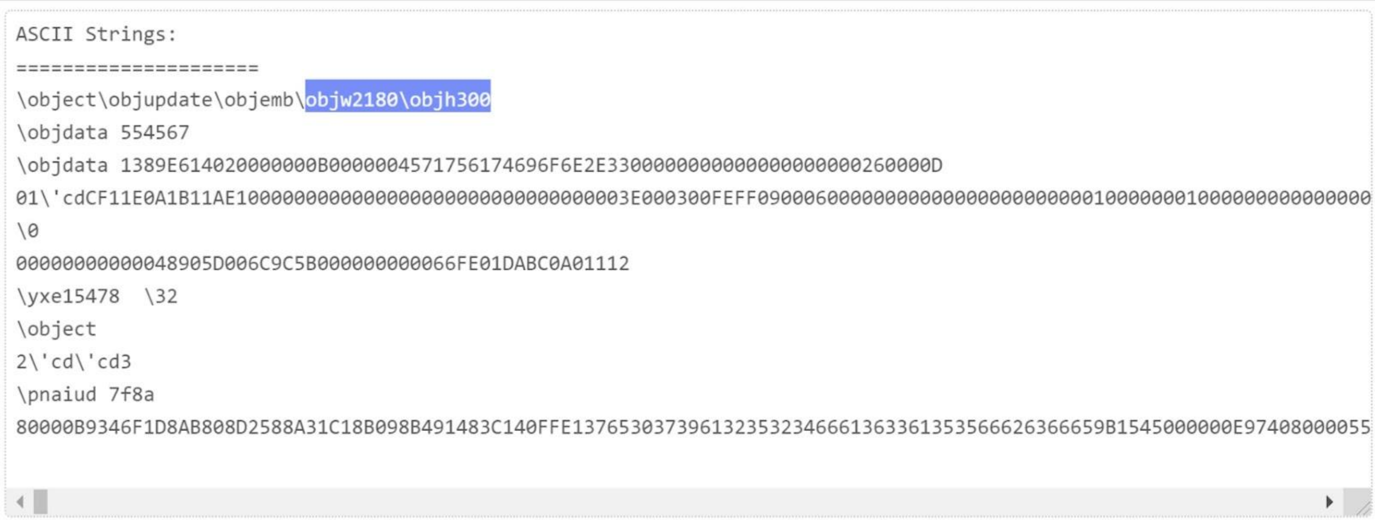
03 Many RTF phishing weaponizers have hard-coded object dimensions.

ATTRIBUTION IS IN THE OBJECT

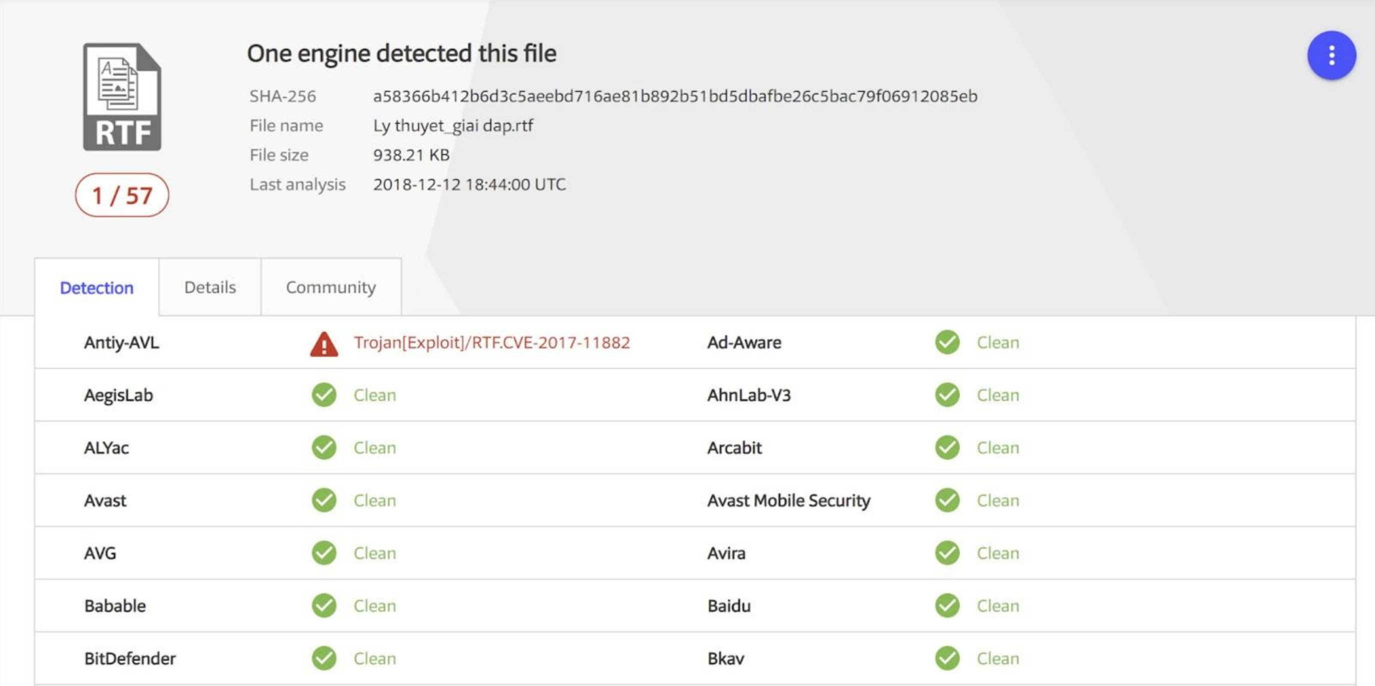
Object Dimensions Simple and Persistent Tracking Technique

01 Unique object dimensions can provide distinct strings for signatures that are not commonly altered by actors between campaigns.

02 The IOC is from the actor's tools. Requires altering the tooling to avoid detection.



```
ASCII Strings:
====================
\object\objupdate\objemb\objw2180\objh300
\objdata 554567
\objdata 1389E614020000000B0000004571756174696F6E2E33000000000000000000000260000D
01\'cdCF11E0A1B11AE1000000000000000000000000000000003E000300FEFF0900060000000000000000000000000100000001000000000000000000
\0
00000000000048905D006C9C5B000000000066FE01DABC0A01112
\yxe15478  \32
\object
2\'cd\'cd3
\pnaiud 7f8a
80000B9346F1D8AB808D2588A31C18B098B491483C140FFE1376530373961323532346661363361353566626366659B1545000000E97408000055
```



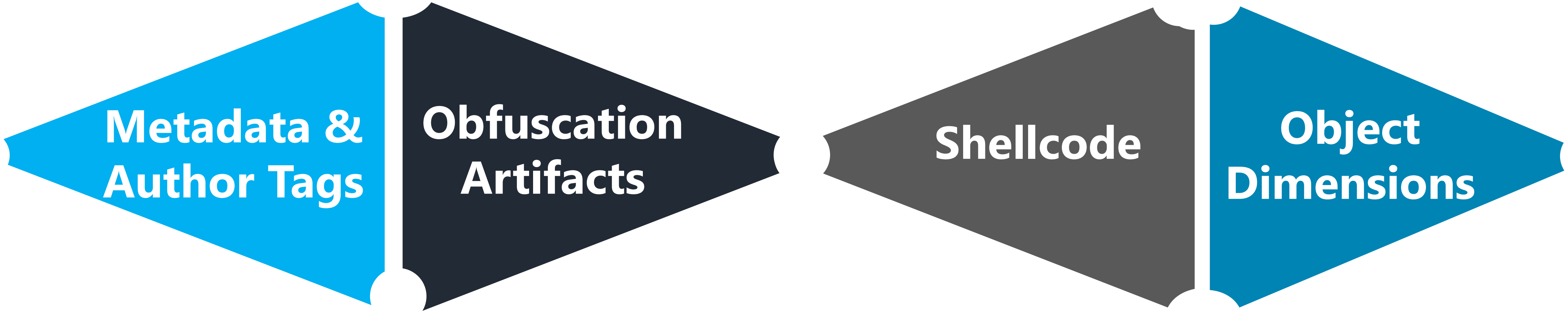
1 / 57

One engine detected this file

SHA-256 a58366b412b6d3c5aeebd716ae81b892b51bd5dbafbe26c5bac79f06912085eb
File name Ly thuyet_giai dap.rtf
File size 938.21 KB
Last analysis 2018-12-12 18:44:00 UTC

Antiy-AVL	⚠ Trojan[Exploit]/RTF.CVE-2017-11882	Ad-Aware	✓ Clean
AegisLab	✓ Clean	AhnLab-V3	✓ Clean
ALYac	✓ Clean	Arcabit	✓ Clean
Avast	✓ Clean	Avast Mobile Security	✓ Clean
AVG	✓ Clean	Avira	✓ Clean
Babable	✓ Clean	Baidu	✓ Clean
BitDefender	✓ Clean	Bkav	✓ Clean

Comparing Attribution Methods



Metadata & Author Tags

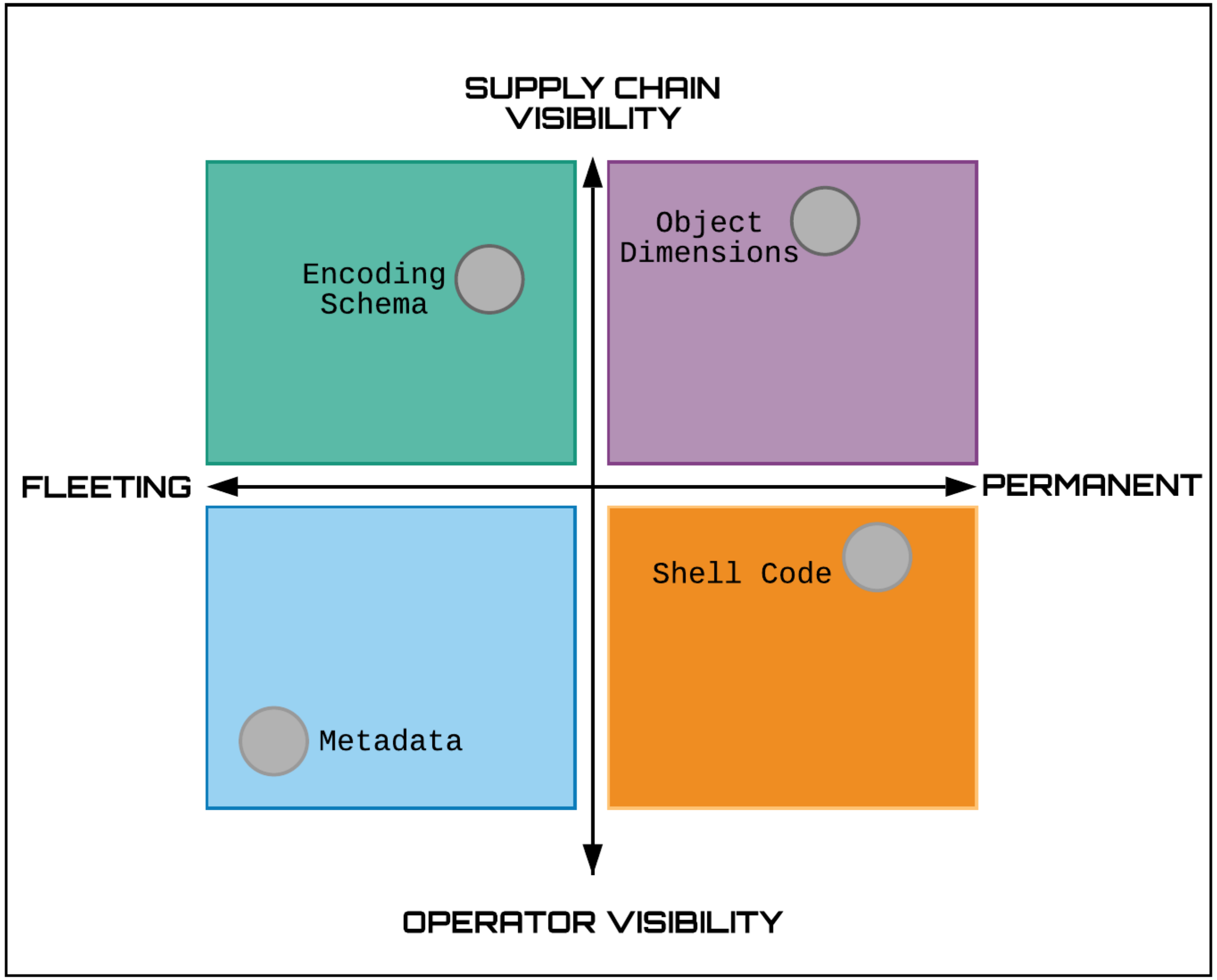
Obfuscation Artifacts

Shellcode

Object Dimensions

	Metadata	Shell Code	Obfuscation	Object Dimensions
Pro	Easy to Track Operator Visibility	Permanent Often Unique to Actor	Easy to Track Supply Chain Visibility	More Permanent Supply Chain Visibility Often Unique to Actor
Con	Very Impermanent Not Always Unique	Difficult to Track Often Obfuscated	Impermanent No Operator Visibility	No Operator Visibility

Comparing Attribution Methods



RoyalRoad RTF Weaponizer

Objw2180/Objh300

- Toolkit introduced in late 2017
- Remained in use through mid-2019
- Utilized by Multiple APT groups.
- Eventually adopted by crimeware.
- It exploits three distinct CVE’s
- **Identifiable by unique Object dimensions.**

Royal Road Targeted
Equation Editor Exploits

- Microsoft Word’s Equation Editor is a tool in MSWord to build equations using different data representation options.
- Beginning in 2017 numerous popular exploits affecting Equation Editor were disclosed.
- Multiple RoyalRoad versions targeted CVE-2017-11882, CVE-2018-0802, CVE-2018-0798.

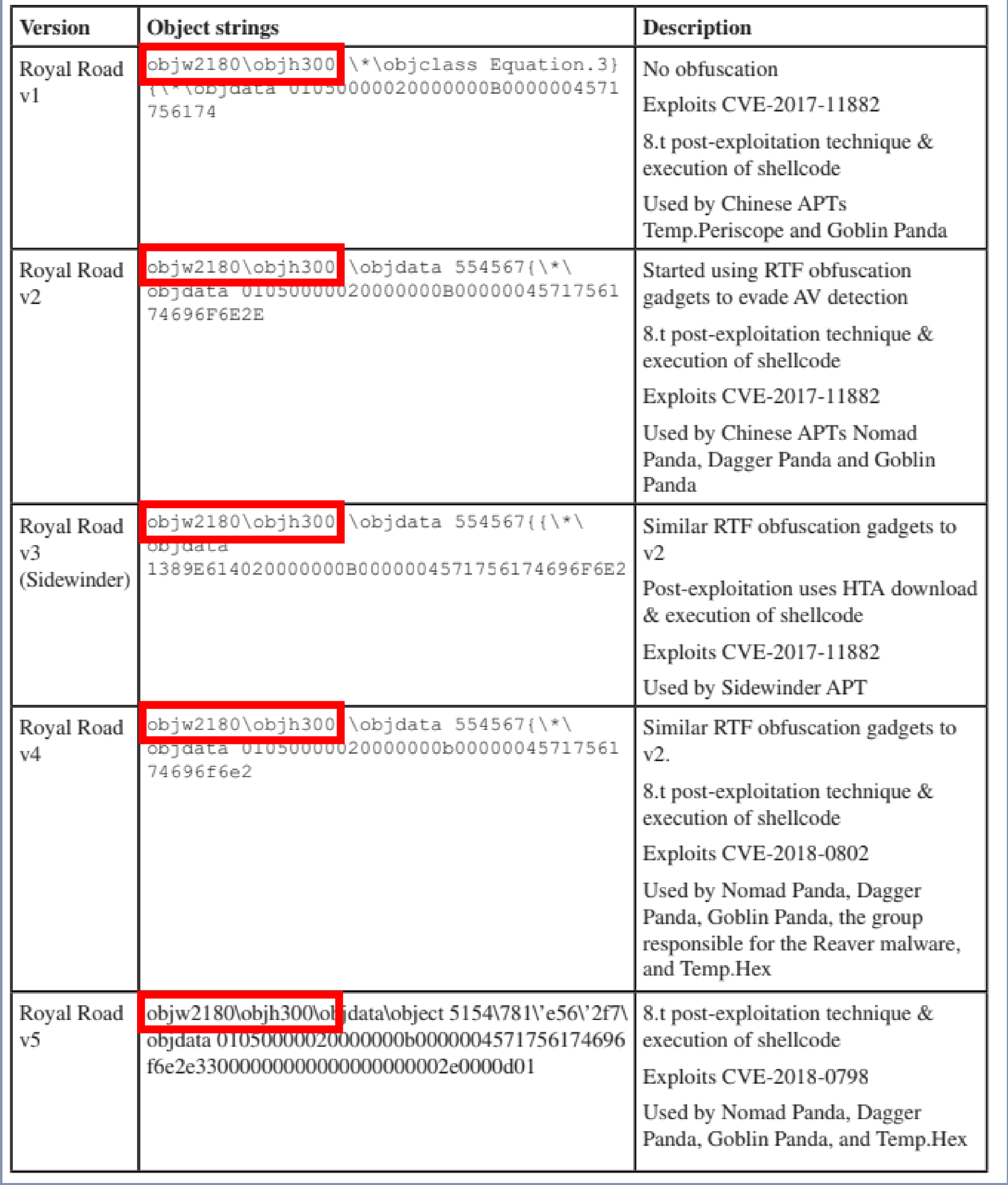
ATTRIBUTION IS IN THE OBJECT

The Constancy of Object Dimensions

01 5 RoyalRoad versions were observed identified by different obfuscation strings

02 These tools targeted 3 CVEs.

03 Despite varying obfuscation object dimensions in RTFs remained constant.



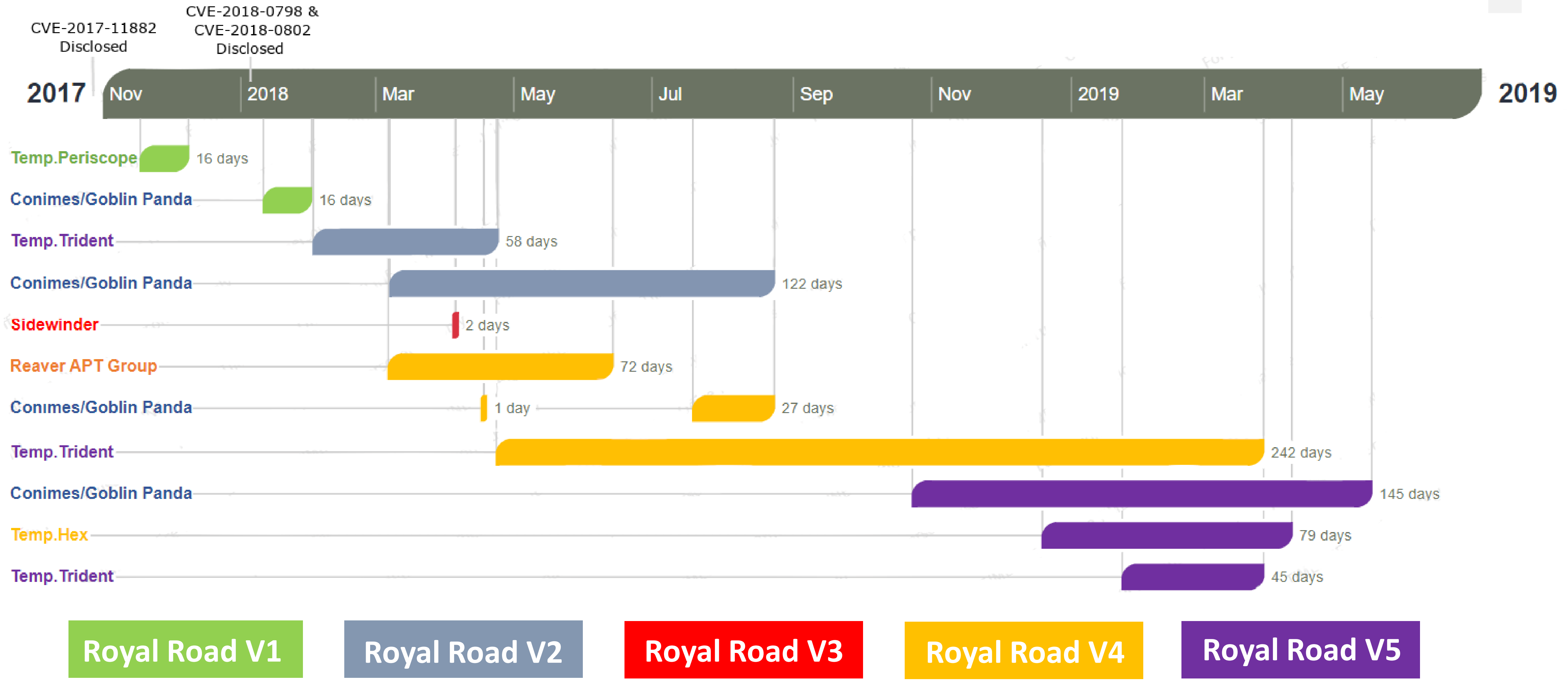
Version	Object strings	Description
Royal Road v1	objw2180\objh300 *\objclass Equation.3}{*\objdata 01050000020000000B0000004571756174	No obfuscation Exploits CVE-2017-11882 8.t post-exploitation technique & execution of shellcode Used by Chinese APTs Temp.Periscope and Goblin Panda
Royal Road v2	objw2180\objh300 \objdata 554567{*\objdata 01050000020000000B0000004571756174696F6E2E	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 1389E61402000000B00000045717561 74696F6E2	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 01050000020000000b0000004571756174696f6e2	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 01050000020000000b0000004571756174696f6e2e3300000000000000000000002e0000d01	8.t post-exploitation technique & execution of shellcode Exploits CVE-2018-0798 Used by Nomad Panda, Dagger Panda, Goblin Panda, and Temp.Hex

RoyalRoad & CVE-2018-0798

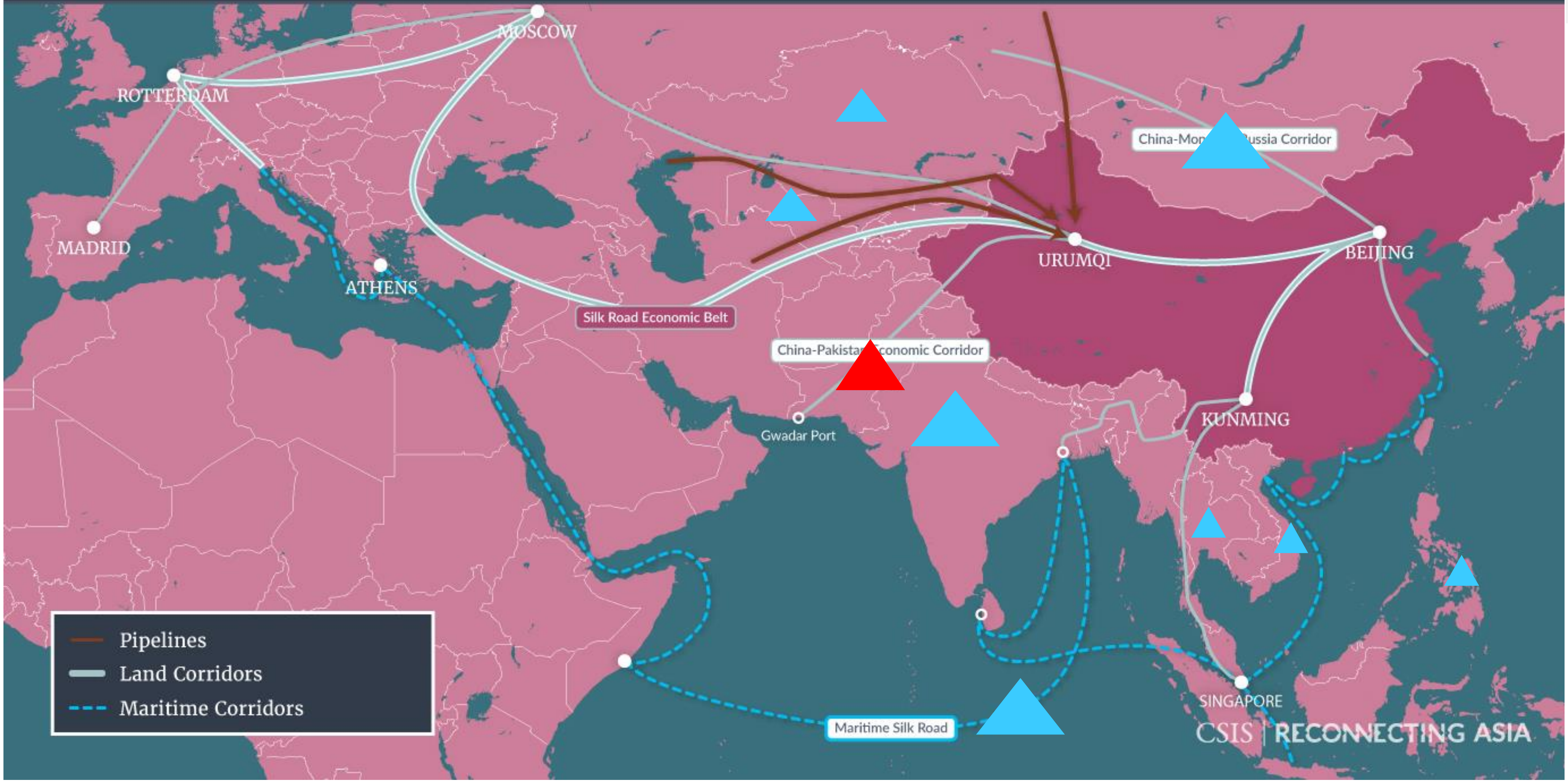
- Royal Road used CVE-2017-11882 and CVE-2018-0802 for over a year since end 2017.
- By end 2018 we noticed new RoyalRoad samples submitted to VT with low AVs detection .
- We discovered CVE-2018-0798 was being utilized in Royal Road samples since late 2018.
- Buffer overflow in Equation Editor when parsing Matrix type records

Actors changed to the CVE-2018-0798 because this exploit works with all versions of Equation Editor. While older CVEs were only effective in specific versions of EE.

Royal Road Adoption Timeline

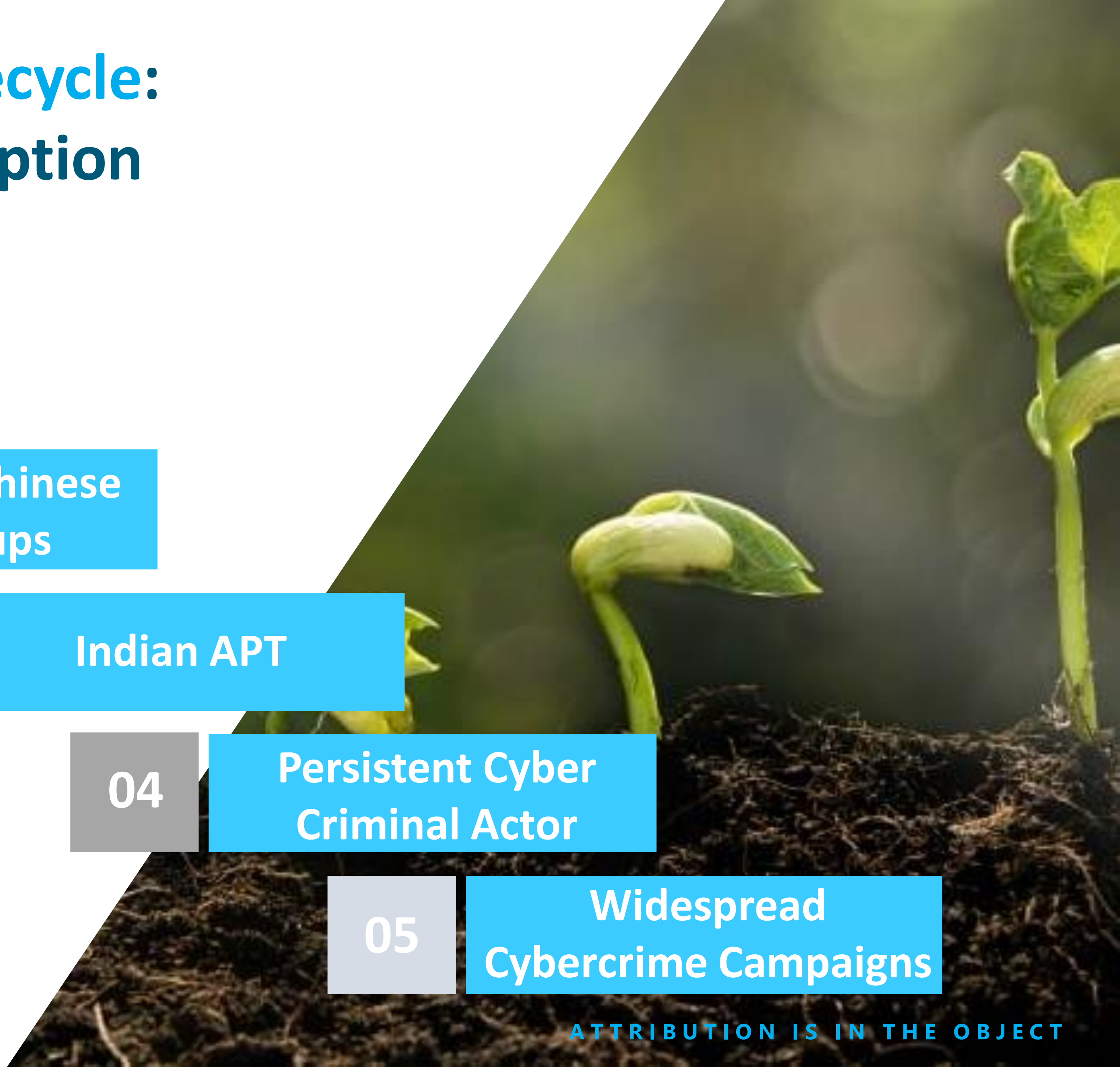


China's Vision



ATTRIBUTION IS IN THE OBJECT

Weaponizer Lifecycle: Royal Road Adoption



01 Sophisticated Chinese APT Group

02 Additional Chinese APT Groups

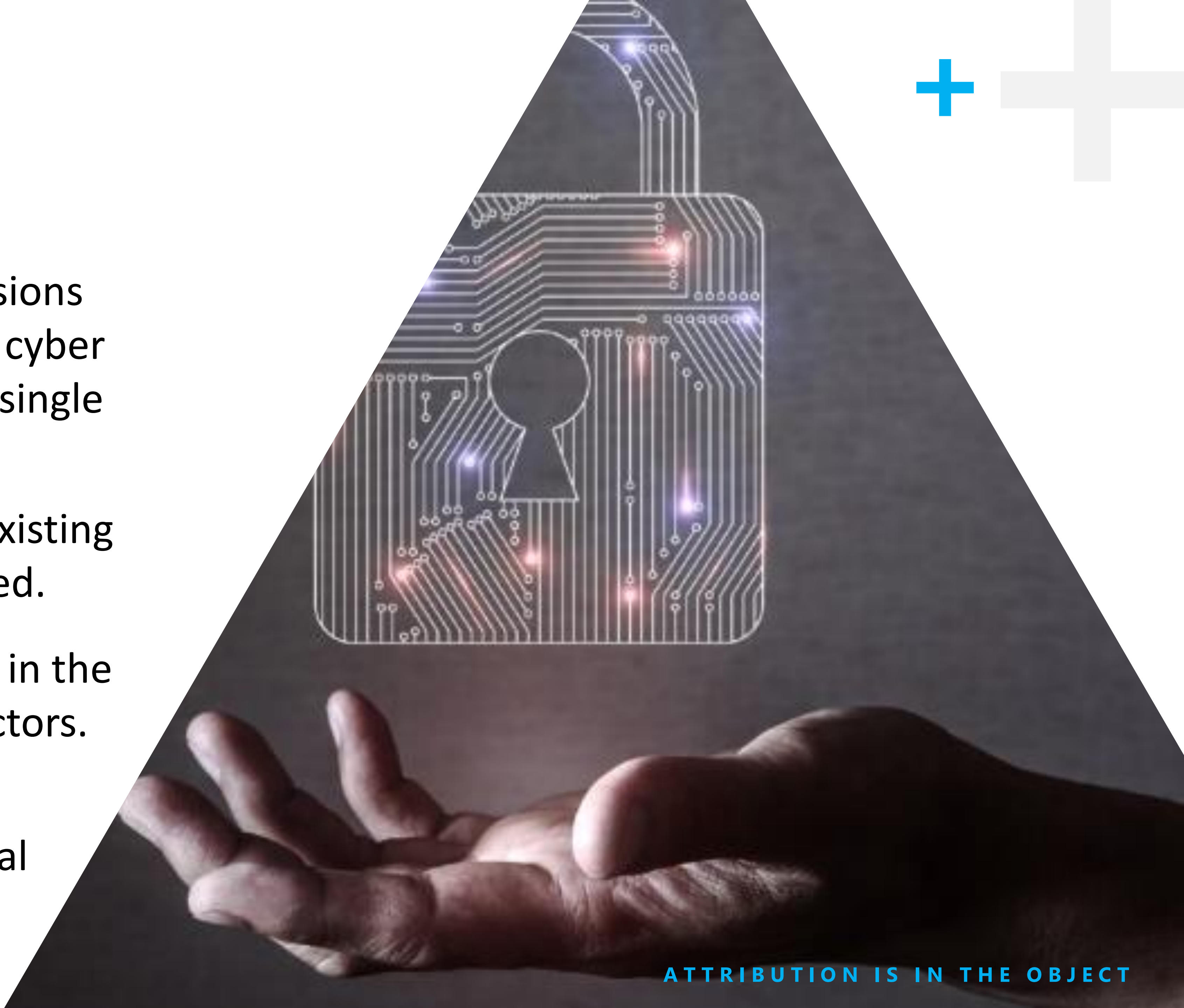
03 Indian APT

04 Persistent Cyber Criminal Actor

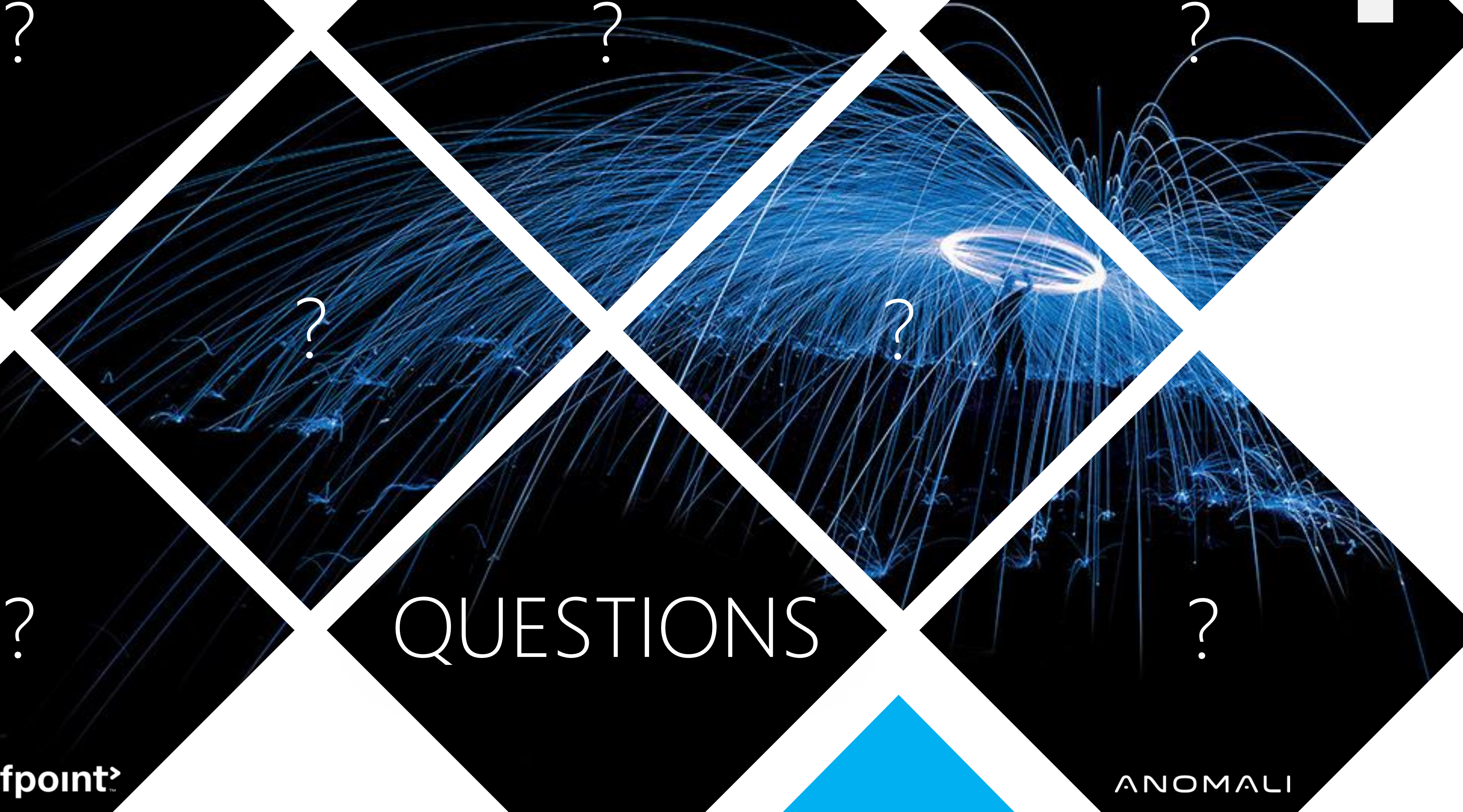
05 Widespread Cybercrime Campaigns

Royal Road:
Lessons Learned

- Shared RTF object dimensions identified multiple APT & cyber criminal actors utilizing a single tool to create exploits.
- New relations between existing APT groups were identified.
- A new CVE was identified in the wild being used by APT actors.
- APT weaponizers trickle down to the cyber criminal landscape.



ATTRIBUTION IS IN THE OBJECT



? ? ?

? ?

?

QUESTIONS

?

proofpoint

ANOMALI