Cisco Security Research

Attribution: A puzzle

Who am I?

Vitor Ventura

Security Researcher at Cisco Talos

- Android malware destroyer
- (In)Secure IM hater
- Previously did pentesting on ICS and Automotive industry

Located in Portugal

Talos
Cisco Security Research

Who am I?

Paul Rascagneres

Security Researcher at Cisco Talos

Worked on several investigations:

- WannaCry
- NotPetya / MeDocs
- Olympic Destroyer
- SeaTurtle/DNSpionage

3D printing hobbiest

Located in France

Talos
Cisco Security Research

Agenda

Why attribution is puzzling

1. Introduction
2. Attribution Points
   - *Context*
   - *Infrastructure*
   - *TTPS*
   - *Analysing the evidence*
3. Code Sharing
4. False Flags
5. Conclusion

Talos
Cisco Security Research

Introduction

Introduction

- The attribution of cyber attacks requires collecting diverse intelligence, analysing it and deciding who is responsible.
- The private sector attempts to associate cyber attacks to threat actors using the intelligence available to them.
- Private sector sources include open-source intelligence (OSINT), technical analysis (TECHINT) and possibly proprietary data.

Introduction

- Intelligence agencies have additional sources.
- Such intelligence is beyond the reach of private-sector researchers.

Introduction

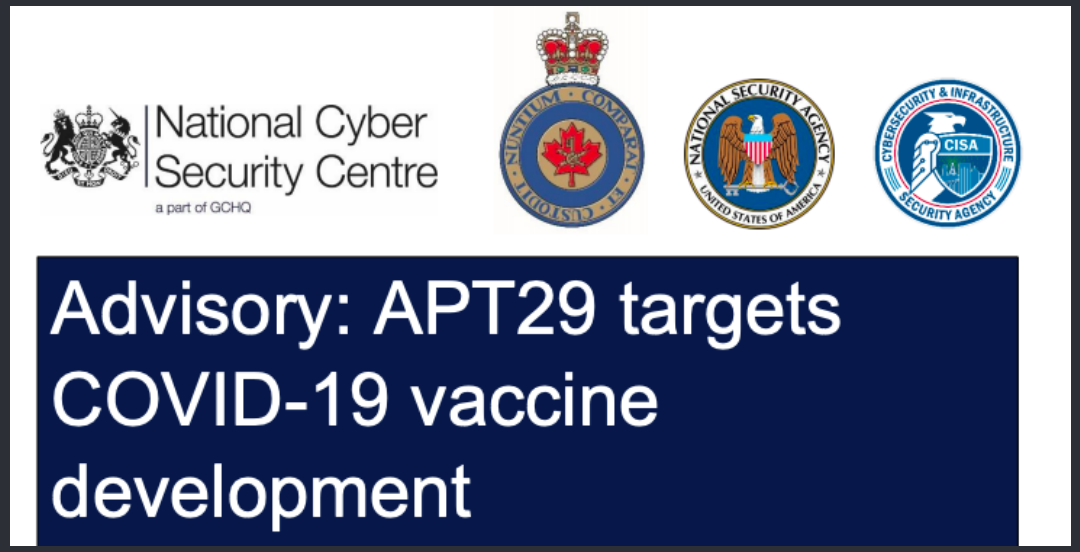
- Let’s take examples of attribution and examine the evidence available to us as a threat intelligence and security research group…
- And let’s see why attribution can be hard…

Attribution pivots

Context

Attribution pivots - Context

- WellMess attribution by UK's National Cyber Security Centre (NCSC)
- Endorsed by Canada's Communications Security Establishment (CSE), the U.S.'s National Security Agency (NSA) and Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA)



Attribution pivots - Context

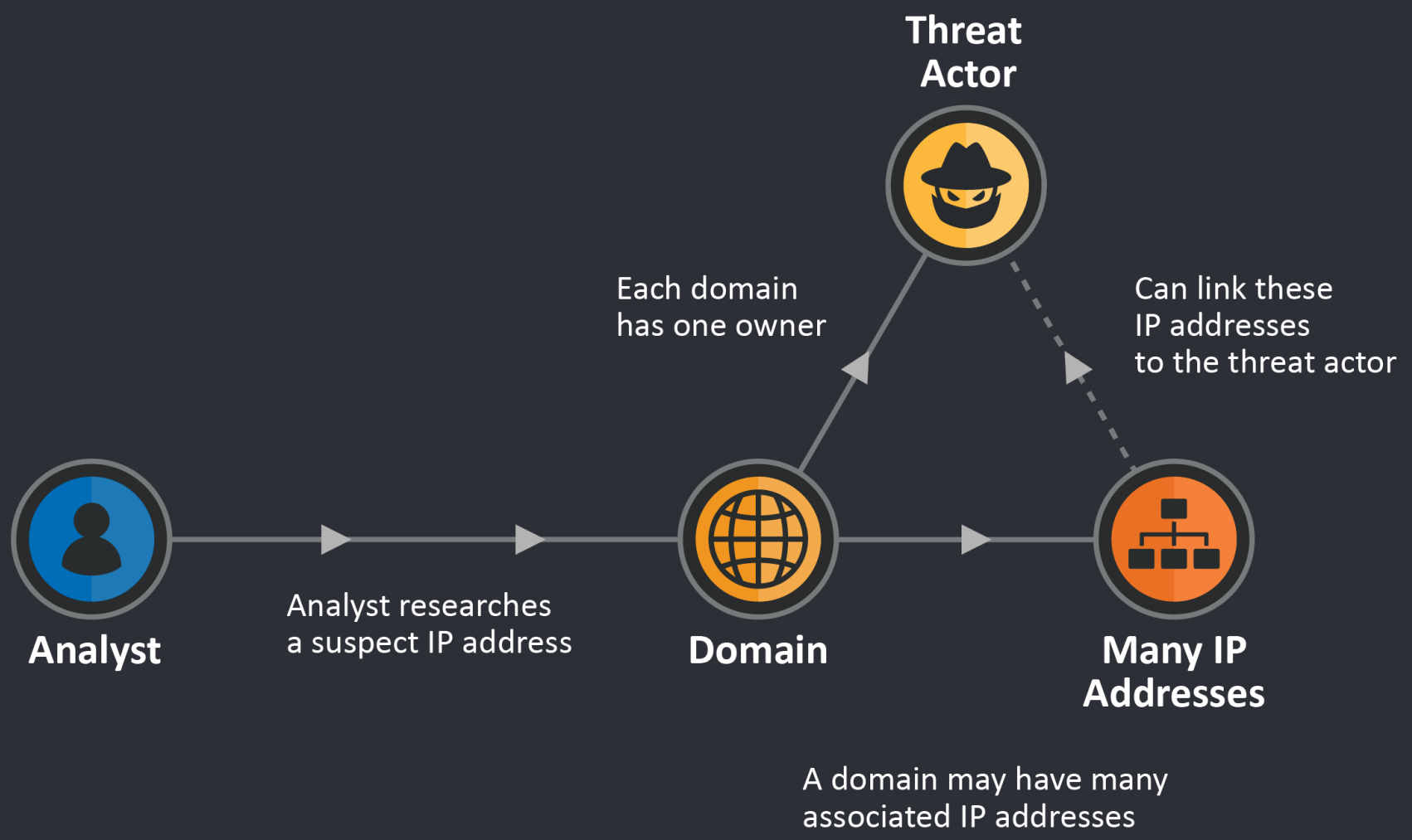
WellMess malware:

- First reported in June 2018 by the Japanese national CERT
- Written in Go (32 & 64 bits)
- Support Linux (ELF) and Windows (PE)
- Supports DNS, HTTP and HTTPS communication
- RAT

Attribution Pivots

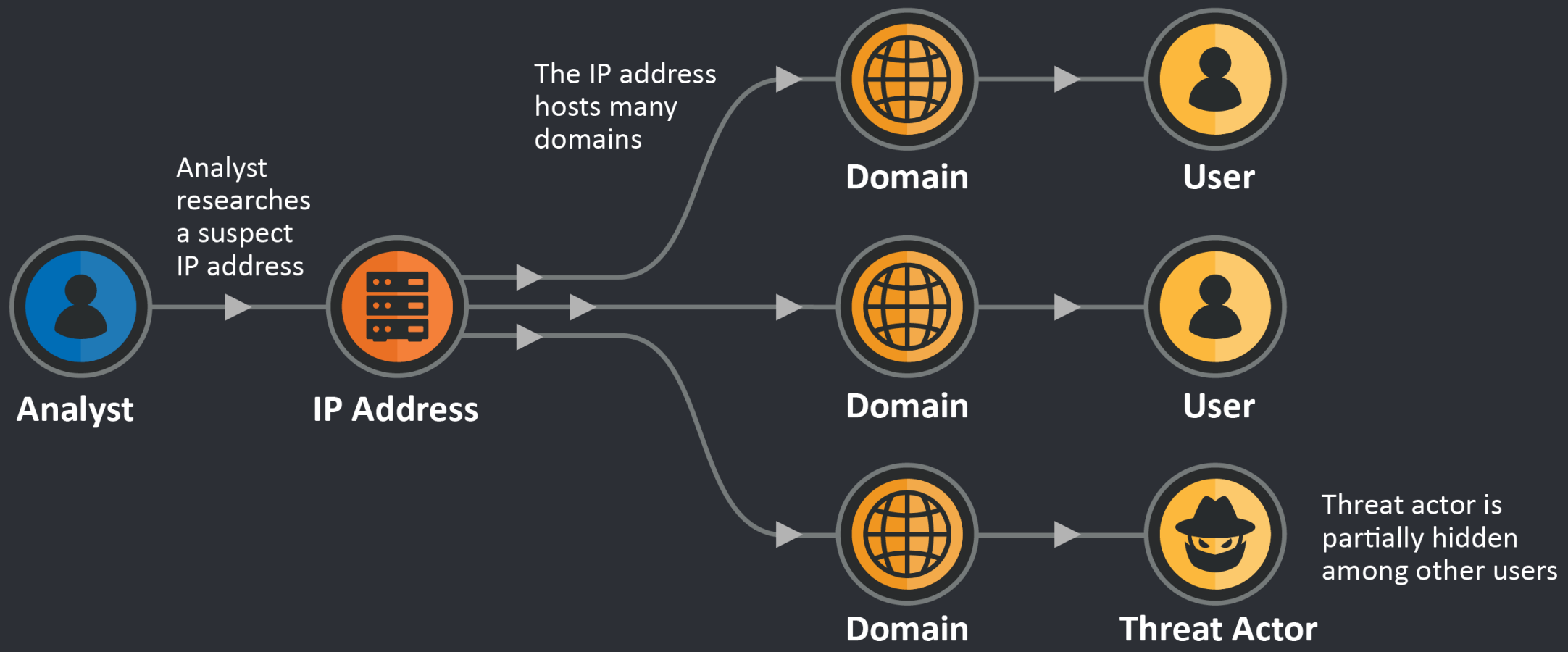
Infrastructure

Attribution pivots - Infrastructure



Cisco Security Research

Attribution pivots - Infrastructure



Cisco Security Research

Attribution pivots - Infrastructure

WellMess sample from May 23, 2018:
0b8e6a11adaa3df120ec15846bb966d674724b6b92eae34d63b665e0698e0193

C2 IPs: 45.123.190[.]168

- **2016-12-24 to 2019-12-04**
  layers[.]wincodec[.]com
- **2017-11-25 to 2018-11-18**
  onedrive-jp[.]com

Attribution pivots - Infrastructure

WellMess sample from May 23, 2018:
0b8e6a11adaa3df120ec15846bb966d674724b6b92eae34d63b665e0698e0193

IPs history of onedrive-jp[.]com

- **2020-07-17 to 2020-07-17**
  52.45.178[.]122
- **2018-11-22 to 2018-12-29**
  209.99.40[.]222
- **2018-11-21 to 2018-12-25**
  209.99.40[.]223
- **2017-11-25 to 2018-11-18**
  45.123.190[.]168
- **2017-12-19 to 2018-11-03**
  198.251.83[.]27

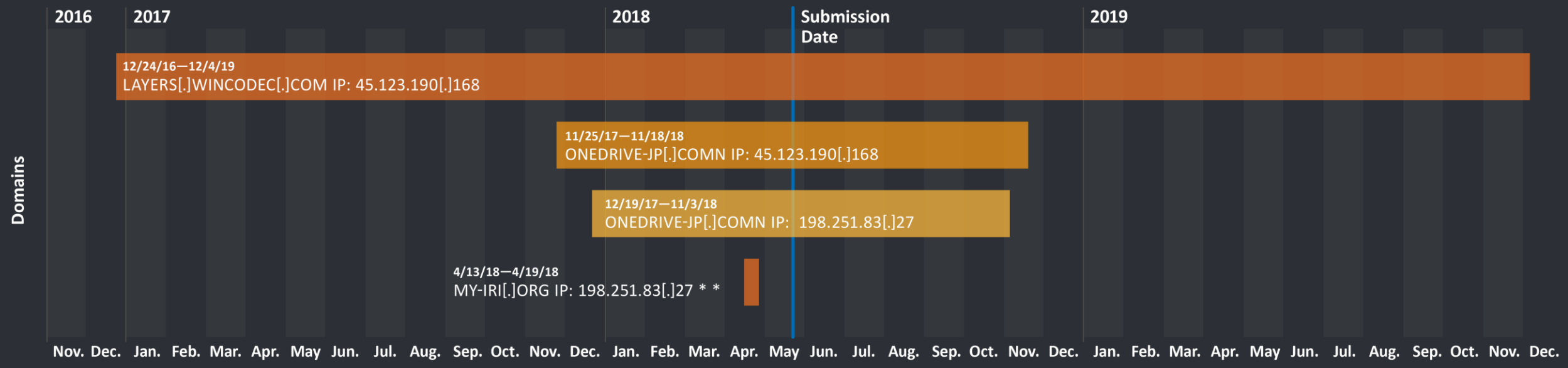
Attribution pivots - Infrastructure

WellMess sample from May 23, 2018:
0b8e6a11adaa3df120ec15846bb966d67
4724b6b92eae34d63b665e0698e0193

Domains history of 198.251.83[.]27

- **2018-04-13 to 2018-04-19**
  my-iri[.]org

Attribution pivots - Infrastructure



Talos
Cisco Security Research

Attibution pivots - Infrastructure

Sections

The Washington Post
Democracy Dies in Darkness

Get 1 year for $29 | Gift Su

Business

Microsoft says it has found a Rus operation targeting U.S. political institutions

Microsoft said Aug. 21 that it thwarted hacking attacks by a group with known ties to the Russian government against two conservative think tanks. (Reuters)

Why this a

The effort by the notorious APT28 hacking group, which has been publicly linked to a Russian intelligence agency and actively interfered in the 2016 presidential election, underscores the aggressive role that Russian operatives are playing ahead of the midterm elections in the United States. U.S. officials have repeatedly warned that the November vote is a major focus for interference efforts. Microsoft said the sites were created over the past several months and that the company was able to catch them early, as they were being set up. It did not go into more specifics.

The phony websites, which were registered with major web-hosting companies, were at *my-iri.org*, *hudsonorg-my-sharepoint.com*, *senate.group*, *adfs-senate.services*, *adfs-senate.email* and *office365-onedrive.com*, according to Microsoft. Their discovery underscores the central role that American tech companies, which frequently have been criticized for hosting Russian disinformation on their platforms, can play in ferreting it out.

Attribution pivots

Tactics, techniques & procedures (TTPs)

Attribution pivots - TTPs

WellMess sample from Jan. 21, 2020:
65495d173e305625696051944a36a031ea94bb3a4f13034d8be740982bc4ab75

The original name of the sample was "SangforUD.exe," the filename of the Sangfor VPN client.

- Trojan Horse
- TrojanSpy.Win32.DARKHOTEL.A
- Trojan.Agentb

Attribution pivots - TTPs

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS

MUST READ: Windows 10: New 20H2 insider preview arrives with epic list of fixes

PART OF A ZDNET SPECIAL FEATURE: CYBERWAR AND THE FUTURE OF CYBERSECURITY

DarkHotel hackers use VPN zero-day to breach Chinese government agencies

Targets included government agencies in Beijing and Shanghai and Chinese diplomatic missions abroad.

Attribution pivots

Analysing the evidences

Cisco Security Research

Attribution pivots – Analysing the evidences

- The NCSC report clearly attributes the attack to APT29. We can't confirm or refute this conclusion, mainly because their intelligence is not publicly available and can be assumed to combine several different types of intelligence sources.
- Our own TECHINT-based research of the infrastructure indicates that WellMess might be associated with APT28. However, our TTP pivots suggest the malware could be linked to DarkHotel.

Attribution pivots – Analysing the evidences

- The attribution concerning the Sangfor VPN servers hack may be incorrect. Was this an attack carried out by APT28 or APT29, rather than DarkHotel?
- Two different threat actors targeted the same VPN software at the same time by coincidence.
- Or, possibly, there is an unknown common factor between the threat actors that led to them targeting the same software.

Code Sharing

Code sharing

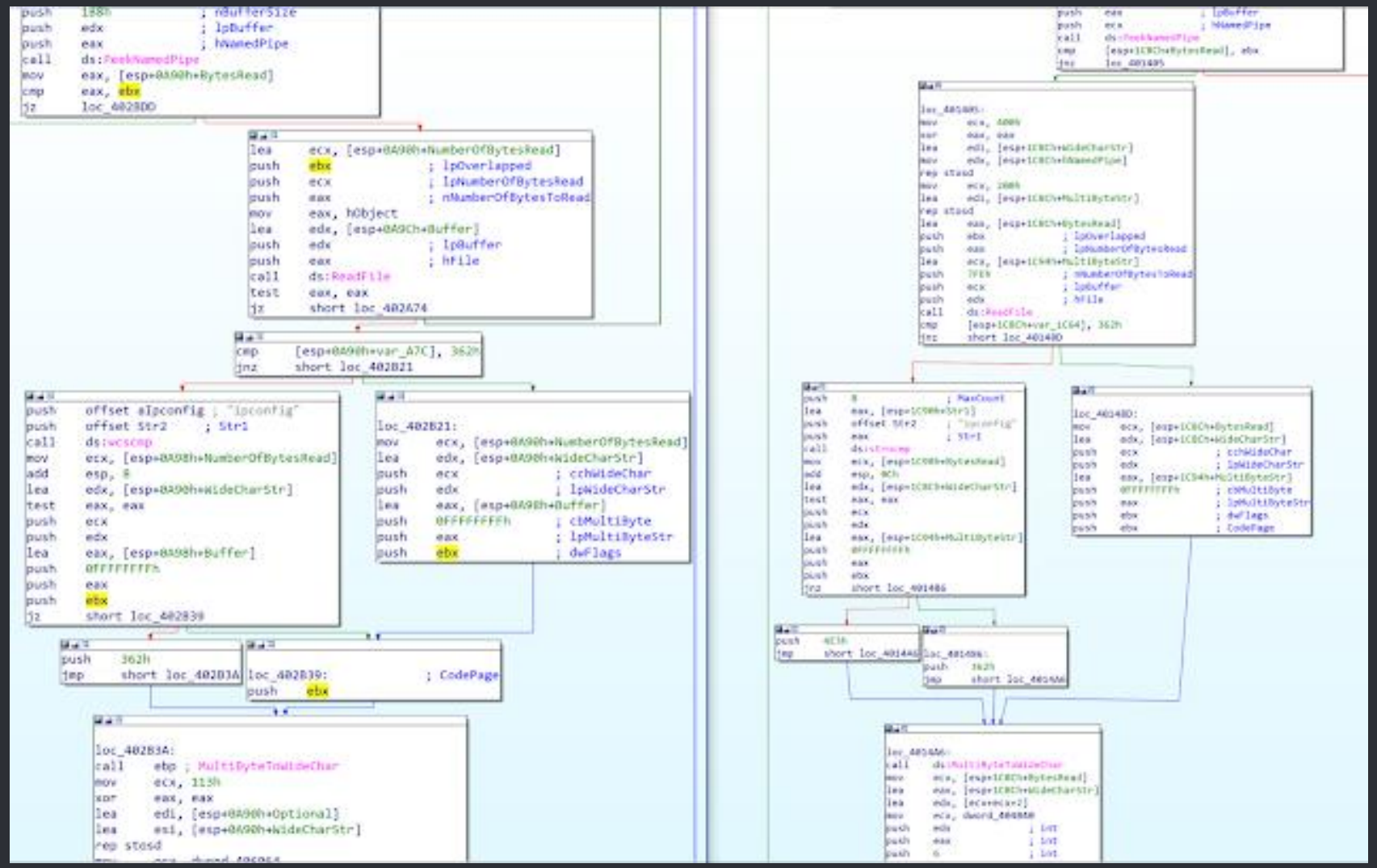
Neel Mehta
@neelmehta

9c7c7149387a1c79679a87dd1ba755bc @ 0x402560, 0x40F598
ac21c8ad899727137c4b94458d7aa8d8 @ 0x10004ba0, 0x10012AA4
#WannaCryptAttribution

6:02 PM · May 15, 2017 · Twitter Web Client

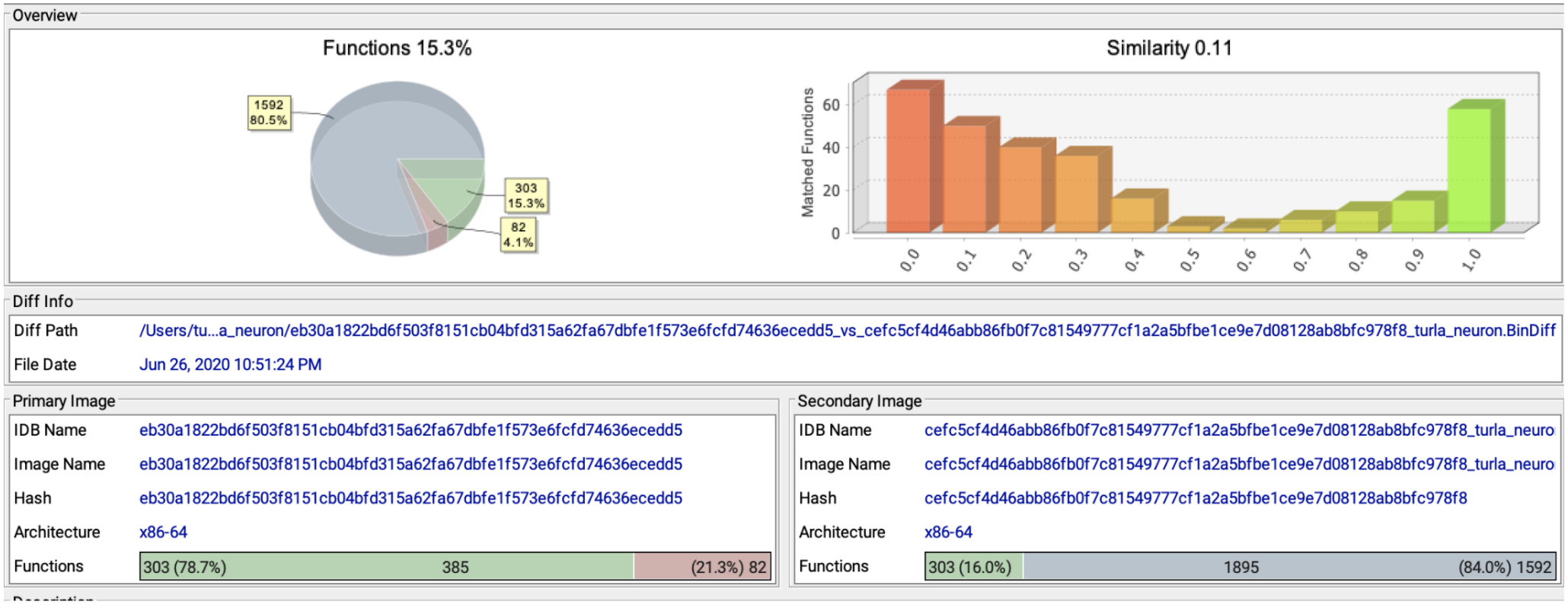
Source: https://twitter.com/neelmehta/status/864164081116225536

Code sharing



Source: https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html

Code sharing

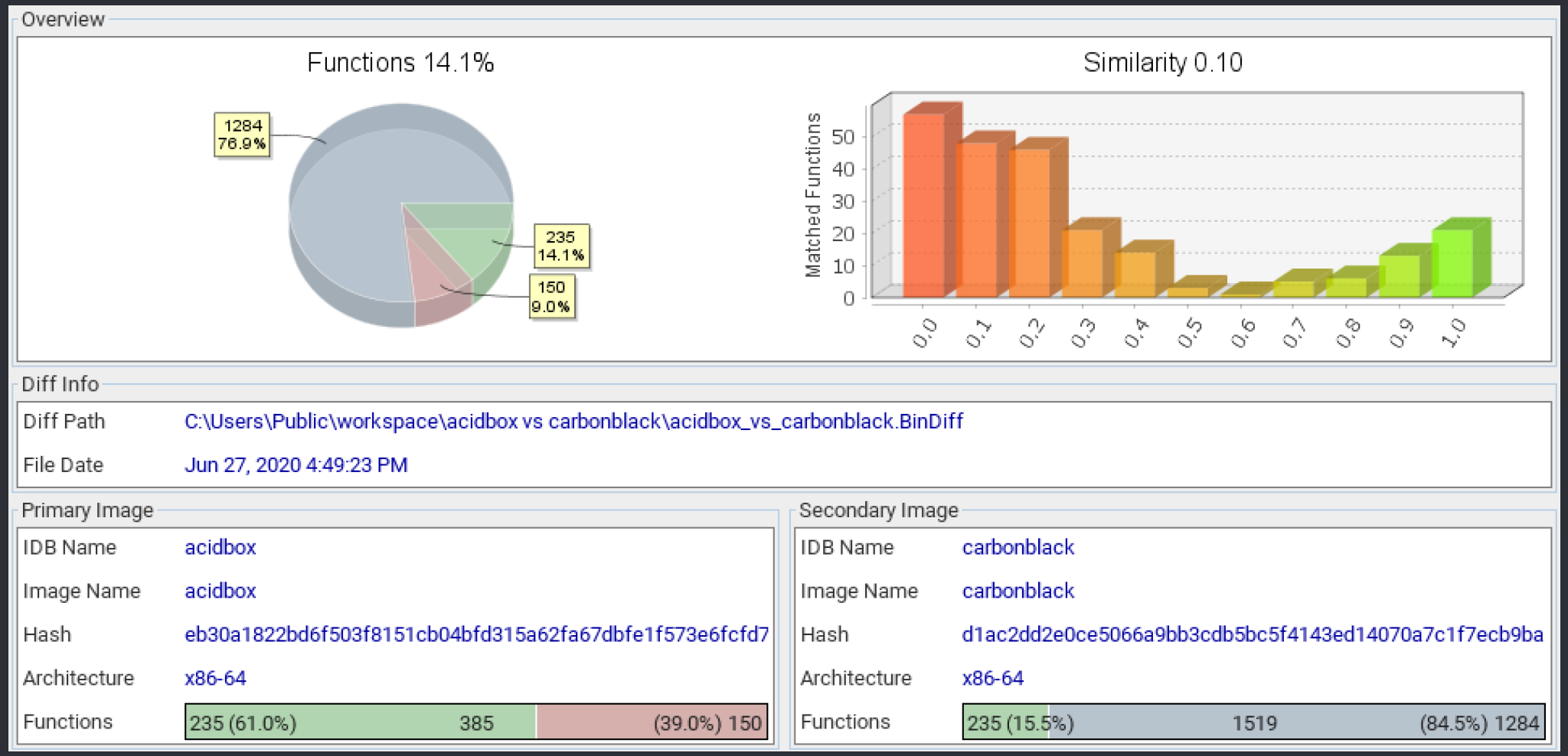


ACIDBOX (left) and Turla Nautilus Payload (right)

Source: https://www.epicturla.com/blog/acidbox-clustering

Talos
Cisco Security Research

Code sharing



Source: https://twitter.com/TheEnergyStory/status/1277652093235531782

False Flags

False Flags

```
push    ebp
mov     ebp, esp
push    ecx
push    8                   ; size_t
call    ??2@YAPAXI@Z        ; operator new(uint)
push    1
push    0
push    2
push    0
push    0
push    1
push    28022Ah
push    offset aIiqqiib ; "IIQQIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 28h
mov     dword_430AB0, eax
mov     esp, ebp
pop     ebp
retn
```

```
push    ebp
mov     ebp, esp
push    ecx
push    8                   ; size_t
call    ??2@YAPAXI@Z        ; operator new(uint)
push    1
push    0
push    2
push    0
push    0
push    1
push    1C022Ah
push    offset aIiiiiib ; "IIIIIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 28h
mov     dword_430A70, eax
mov     esp, ebp
pop     ebp
retn
```

```
push    0
push    2
push    0
push    0
push    0
push    0
push    1
push    38022Ah
push    offset aIiqqqqiib ; "IIQQQQIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 30h
mov     dword_430A90, eax
mov     esp, ebp
pop     ebp
retn
```

```
push    1
push    24022Ah
push    offset aIiiiiiiib ; "IIIIIIIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 30h
mov     dword_430A50, eax
mov     esp, ebp
pop     ebp
retn
```

False Flags

```
push    ebp
mov     ebp, esp
push    ecx
push    8                   ; size_t
call    ??2@YAPAXI@Z        ; operator new(uint)
push    1
push    0
push    2
push    0
push    0
push    1
push    28022Ah
push    offset aIiqqiib ; "IIQQIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 28h
mov     dword_430AB0, eax
mov     esp, ebp
pop     ebp
retn
```

```
push    ebp
mov     ebp, esp
push    ecx
push    8                   ; size_t
call    ??2@YAPAXI@Z        ; operator new(uint)
push    1
push    0
push    2
push    0
push    0
push    1
push    1C022Ah
push    offset aIiiiiib ; "IIIIIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 28h
mov     dword_430A70, eax
mov     esp, ebp
pop     ebp
retn
```

```
push    0
push    2
push    0
push    0
push    0
push    0
push    1
push    38022Ah
push    offset aIiqqqqiib ; "IIQQQQIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 30h
mov     dword_430A90, eax
mov     esp, ebp
pop     ebp
retn
```

```
push    1
push    24022Ah
push    offset aIiiiiiiib ; "IIIIIIIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 30h
mov     dword_430A50, eax
mov     esp, ebp
pop     ebp
retn
```

```
##########################
# info for modify session security context
##########################
WIN7_64_SESSION_INFO = {
        'SESSION_SECCTX_OFFSET': 0xa0,
        'SESSION_ISNULL_OFFSET': 0xba,
        'FAKE_SECCTX': pack('<IIQQIIB', 0x28022a, 1, 0, 0, 2, 0, 1),
        'SECCTX_SIZE': 0x28,
}

WIN7_32_SESSION_INFO = {
        'SESSION_SECCTX_OFFSET': 0x80,
        'SESSION_ISNULL_OFFSET': 0x96,
        'FAKE_SECCTX': pack('<IIIIIIB', 0x1c022a, 1, 0, 0, 2, 0, 1),
        'SECCTX_SIZE': 0x1c,
}

# win8+ info
WIN8_64_SESSION_INFO = {
        'SESSION_SECCTX_OFFSET': 0xb0,
        'SESSION_ISNULL_OFFSET': 0xca,
        'FAKE_SECCTX': pack('<IIQQQQIIB', 0x38022a, 1, 0, 0, 0, 0, 2, 0, 1),
        'SECCTX_SIZE': 0x38,
}

WIN8_32_SESSION_INFO = {
        'SESSION_SECCTX_OFFSET': 0x88,
        'SESSION_ISNULL_OFFSET': 0x9e,
        'FAKE_SECCTX': pack('<IIIIIIIIB', 0x24022a, 1, 0, 0, 0, 0, 2, 0, 1),
        'SECCTX_SIZE': 0x24,
}
```

False Flags

```
push    ebp
mov     ebp, esp
push    ecx
push    8                   ; size_t
call    ??2@YAPAXI@Z        ; operator new(uint)
push    1
push    0
push    2
push    0
push    0
push    1
push    28022Ah
push    offset aIiqqiib ; "IIQQIIB"
push    eax
mov     [ebp+var_4], eax
```

```
push    ebp
mov     ebp, esp
push    ecx
push    8                   ; size_t
call    ??2@YAPAXI@Z        ; operator new(uint)
push    1
push    0
push    2
push    0
add     esp, 28h
mov     dword_430A70, eax
mov     esp, ebp
pop     ebp
retn
```

```
push    0
push    2
push    0
push    0
push    0
push    0
push    1
push    38022Ah
push    offset aIiqqqqiib ; "IIQQQQIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 30h
mov     dword_430A90, eax
mov     esp, ebp
pop     ebp
retn
```

```
push    1
push    24022Ah
push    offset aIiiiiiiib ; "IIIIIIIIB"
push    eax
mov     [ebp+var_4], eax
call    sub_401A60
add     esp, 30h
mov     dword_430A50, eax
mov     esp, ebp
pop     ebp
retn
```

```
##########################
# info for modify session security context
##########################
WIN7_64_SESSION_INFO = {
        'SESSION_SECCTX_OFFSET': 0xa0,
        'SESSION_ISNULL_OFFSET': 0xba,
        'FAKE_SECCTX': pack('<IIQQIIB', 0x28022a, 1, 0, 0, 2, 0, 1),
        'SECCTX_SIZE': 0x28,
}

WIN7_32_SESSION_INFO = {
        'SESSION_SECCTX_OFFSET': 0x80,

WIN8_64_SESSION_INFO = {
        'SESSION_SECCTX_OFFSET': 0xb0,
        'SESSION_ISNULL_OFFSET': 0xca,
        'FAKE_SECCTX': pack('<IIQQQQIIB', 0x38022a, 1, 0, 0, 0, 0, 2, 0, 1),
        'SECCTX_SIZE': 0x38,
}

WIN8_32_SESSION_INFO = {
        'SESSION_SECCTX_OFFSET': 0x88,
        'SESSION_ISNULL_OFFSET': 0x9e,
        'FAKE_SECCTX': pack('<IIIIIIIIB', 0x24022a, 1, 0, 0, 0, 0, 2, 0, 1),
        'SECCTX_SIZE': 0x24,
}
```

THESE ARE LOADED BUT NEVER USED!

Conclusions

Conclusions

- TECHINT may not be enough
- FALSE FLAGS play an important role
- Conflicting hypothesis

Conclusions

Government intelligence attribution

Talos
Cisco Security Research

Conclusions

right

$\neq$

unverifiable

$\neq$

wrong

Unverifiable – Is just that – Unverifiable

Talos
Cisco Security Research

Conclusions

Attribution is as much a science of collecting verifiable information as it is the art of assembling a hypothesis and being aware of the information missing to support that hypothesis.

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity