# Need for PLEAD: BlackTech Pursuit

**Sveva Vittoria Scenarelli and Rachel Mullan**
November 2019

# Who we are

**Sveva Vittoria Scenarelli**
Threat Intelligence Analyst
PwC
@cyberoverdrive

**Rachel Mullan**
Strategic Threat Intelligence Lead
PwC
@jaded_muse

# Cyber paleontology

> When the passage of time affords new evidence, [any judgement] is thus susceptible of change. Sherman Kent

This is the story of how we revisited old intelligence - with surprising results.

# What we'll cover today

**BlackTech pursuit:**

- Evolution of activity & TTPs
- Analysis of a recent campaign

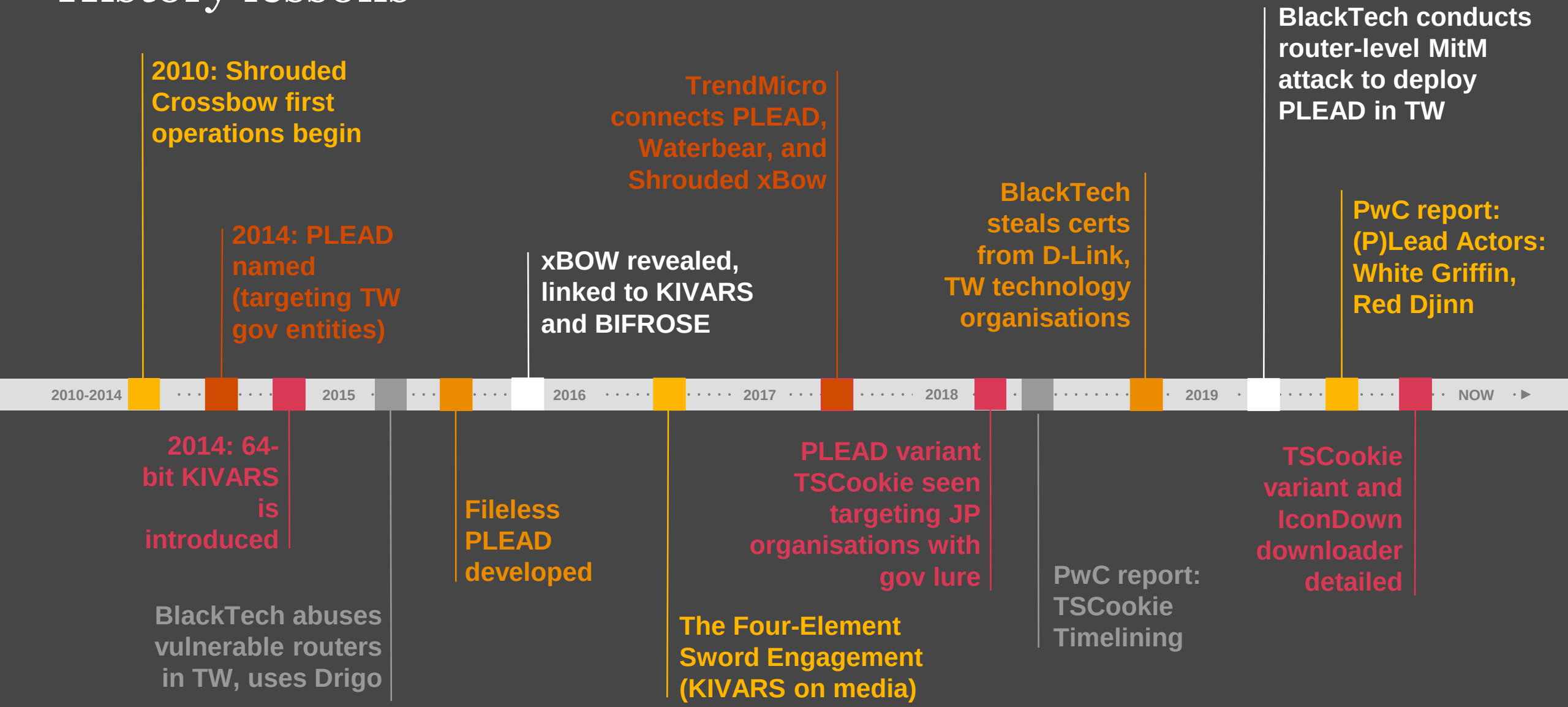
**Following the (P)Leads**

**Chasing the Djinn**

- Through the analysis process and down attribution road

# Names for days

# History lessons



# Once upon a time, a detection: Bluether

**ZIP archive: Bluether**

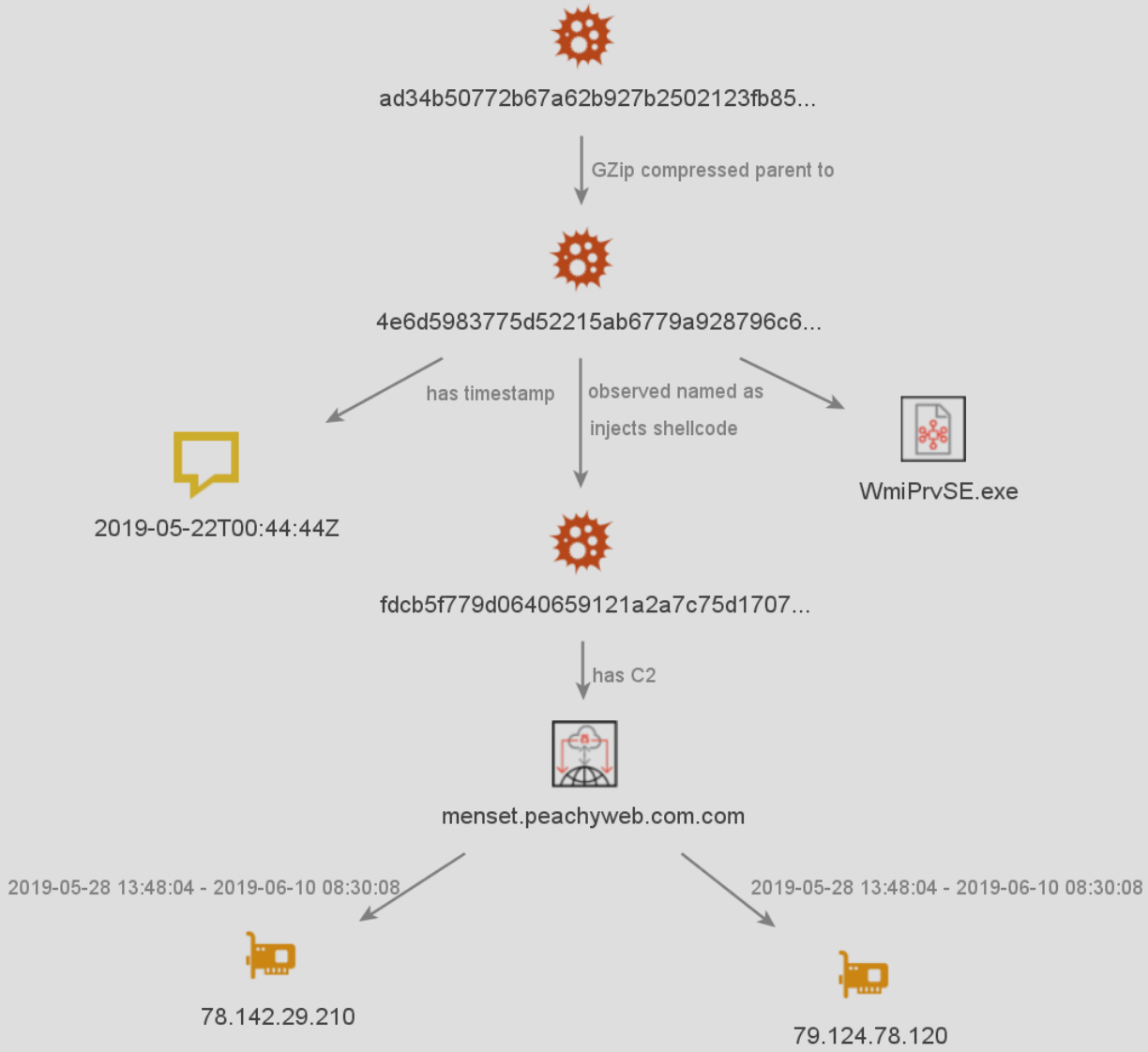
ad34b50772b67a62b927b2502123fb858e05c7e
112817d8a4a44a98096b14751

**WmiPrvSE.exe**

4e6d5983775d52215ab6779a928796c60f57321
b9c65f4b89135bc0c9b880103

**Injected shellcode**

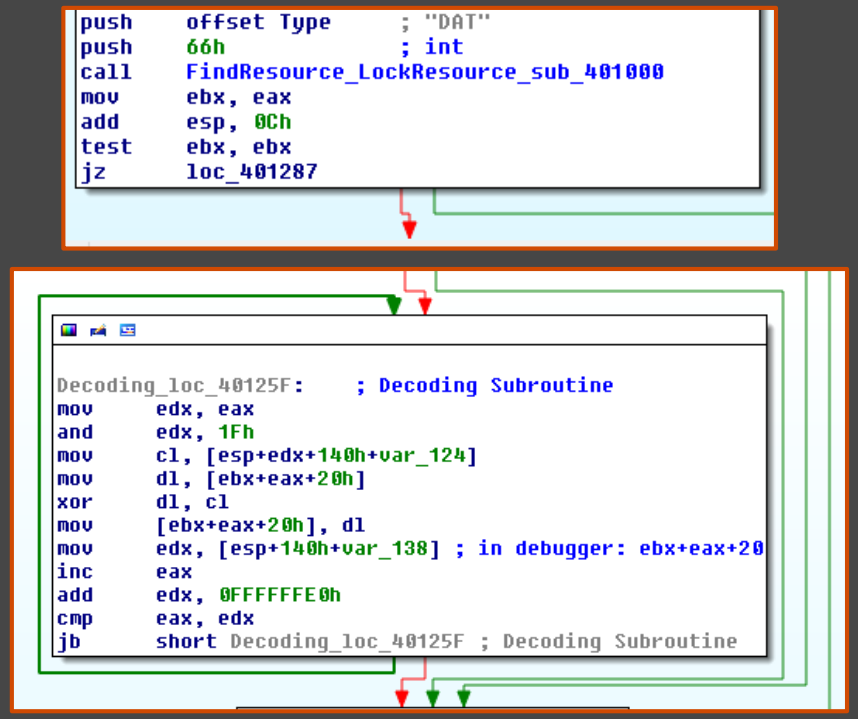
fdcb5f779d0640659121a2a7c75d1707d0c8f37
b833cd528675c405eaa1be650



# Malware Analysis: Execution chain

Sets auto-start key
HKCU\SOFTWARE\Microsoft\Windows
\CurrentVersion\Run, “MSUPD32”

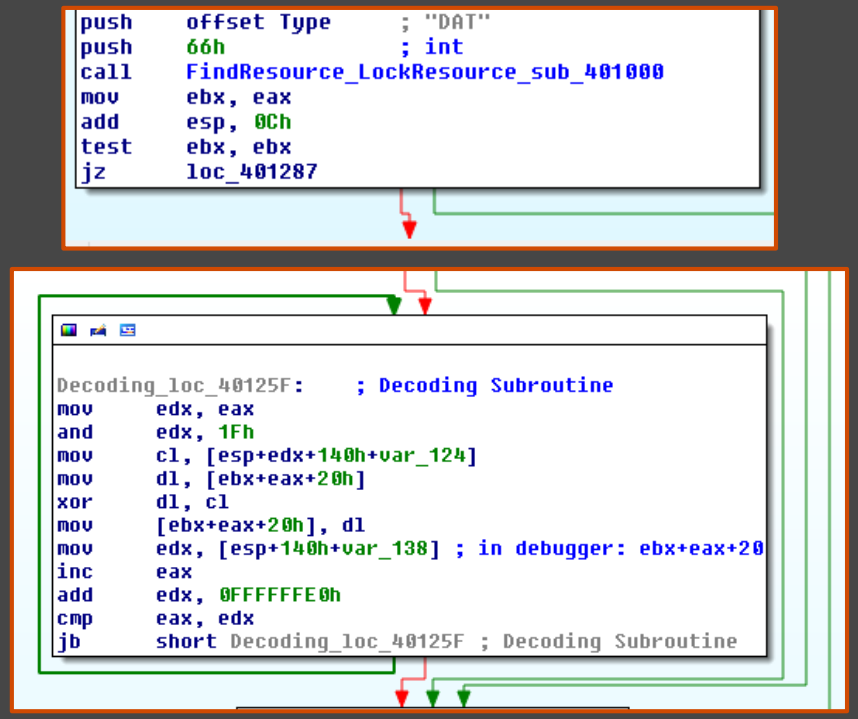
+ Passes execution to shellcode



# Malware Analysis: Execution chain

Sets auto-start key HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, “MSUPD32”

+ Passes execution to shellcode




Shellcode in memory drops binary wuaclt.exe in AppData\Roaming\Microsoft as “hidden”.

Tiny sample indicators of the PLEAD backdoor:

```
80 F9 43        cmp     cl, 43h ; 'C'
74 2A           jz      short loc_695
42              inc     edx
52              push    edx
80 F9 41        cmp     cl, 41h ; 'A'
74 1B           jz      short loc_68D
80 F9 4C        cmp     cl, 4Ch ; 'L'
74 25           jz      short loc_69C
80 F9 45        cmp     cl, 45h ; 'E'
74 27           jz      short loc_6A3
80 F9 50        cmp     cl, 50h ; 'P'
74 29           jz      short loc_6AA
80 F9 47        cmp     cl, 47h ; 'G'
74 2B           jz      short loc_6B1
80 F9 44        cmp     cl, 44h ; 'D'
74 2D           jz      short loc_6B8
EB 30           jmp     short loc_6BD
```

P L E A D

config

# Malware Analysis: Execution chain

Sets auto-start key HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, “MSUPD32”

+ Passes execution to shellcode

```
push    offset Type     ; "DAT"
push    66h             ; int
call    FindResource_LockResource_sub_401000
mov     ebx, eax
add     esp, 0Ch
test    ebx, ebx
jz      loc_401287
```

```
Decoding_loc_40125F:    ; Decoding Subroutine
mov     edx, eax
and     edx, 1Fh
mov     cl, [esp+edx+140h+var_124]
mov     dl, [ebx+eax+20h]
xor     dl, cl
mov     [ebx+eax+20h], dl
mov     edx, [esp+140h+var_138] ; in debugger: ebx+eax+20
inc     eax
add     edx, 0FFFFFFE0h
cmp     eax, edx
jb      short Decoding_loc_40125F ; Decoding Subroutine
```

Shellcode in memory drops binary wuaclt.exe in AppData\Roaming\Microsoft as “hidden”.

Tiny sample indicators of the PLEAD backdoor:

```
80 F9 43        cmp     cl, 43h ; 'C'
74 2A           jz      short loc_695
42              inc     edx
52              push    edx
80 F9 41        cmp     cl, 41h ; 'A'
74 1B           jz      short loc_68D
80 F9 4C        cmp     cl, 4Ch ; 'L'
74 25           jz      short loc_69C
80 F9 45        cmp     cl, 45h ; 'E'
74 27           jz      short loc_6A3
80 F9 50        cmp     cl, 50h ; 'P'
74 29           jz      short loc_6AA
80 F9 47        cmp     cl, 47h ; 'G'
74 2B           jz      short loc_6B1
80 F9 44        cmp     cl, 44h ; 'D'
74 2D
EB 30
```

PLEAD

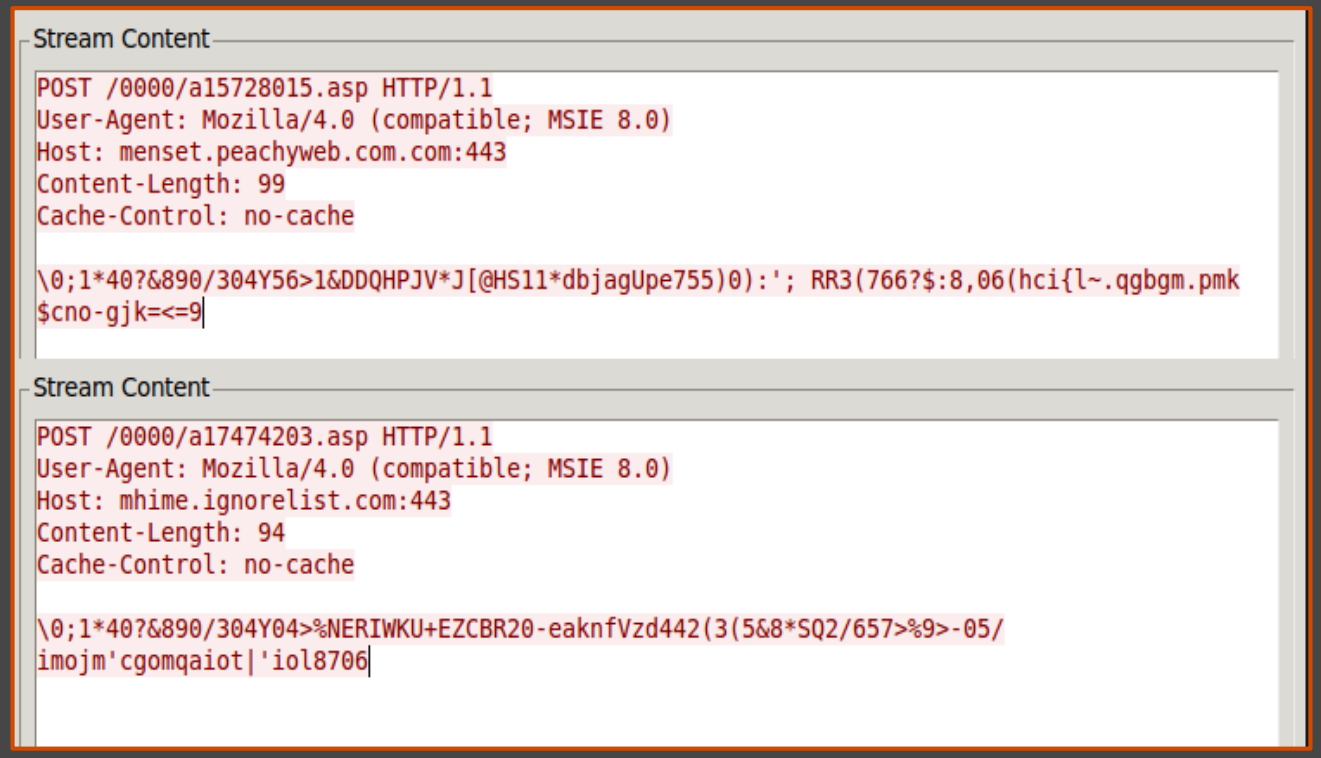
config

```
2  %04X/%c%d.asp
3  Software\Microsoft\Windows\CurrentVersion\Run
4
5  run ok!
6  %d/%s
7  is floppy disk!
8  is not exist path!
9  can't open!
10
11 <Software\Microsoft\Windows\CurrentVersion\Internet
   Settings\ProxyEnable\ProxyServer %s %s
12
13 #Mozilla/4.0 (compatible; MSIE 8.0)
```

Backdoor status strings:

Recurrent User-Agent:

# Malware Analysis: C2 comms




**For C2 URL:** Calls `GetTickCount() ->`
Dynamically-generated URLS: `%04X/%c%d.asp`
Server-side folder `/oooo/` will accept any value generated this way

## Information transmitted:

- machine's local IP address;
- computer name, user name, system version;
- unique moniker (campaign ID?);
- hardcoded C2 domain and ports; and,
- Autorun Registry Key value set by dropper.

**Encoding:** Each string byte is xor'ed – in this case xor value works like a rolling cypher, starting at 0 and resetting after 11.

# PLEAD: Main Variants

| BLUETHER | TSCOOKIE | PLEAD Downloader | Fileless PLEAD |
|---|---|---|---|
| 1. Executable loader<br>2. Shellcode dropper<br>3. Executable backdoor | 1. Executable loader<br>2. DLL downloader in memory<br>3. Executable backdoor | 1. Executable loader<br>2. Shellcode downloader<br>3. Executable backdoor | 1. Lure document<br>2. Flash CVE-2015-5119<br>3. Backdoor in memory |
| **WmiPrvSe.exe:**4e6d5983775d52215ab6779a928796c60f57321b9c65f4b89135bc0c9b880103 | **Exe:**1da9b4a84041b8c72dad9626db822486ce47b9a3ab6b36c41b0637cd1f6444d6 | **Wmpnetwk.exe:**a26df4f62ada084a596bf0f603691bc9c02024be98abec4a9872f0ff0085f940 | **XLS:**9db22b42c71b6532134060a7a175b4eae2c745fa956411389bd7d8c9805ec269 |
| **wuaclt.exe:**FDCB5F779D0640659121A2A7C75D1707D0C8F37B833CD528675C405EAA1BE650 | **DLL:**BFD549CDDDAD51B3113155F31D6389EE9C6101965433BD258F28227FCB347946 | **PLEAD:**e9082b1e8e9a2a4e48e3de1cc1233d202206a8ac2f0d23199c45213ca0204c51 | **ActivX1.bin:**d288327cdf5d58f8deeb1f15914fe7f1fe75b95a2555c0332ddada565c15d03d |

# What is consistent across time and samples?

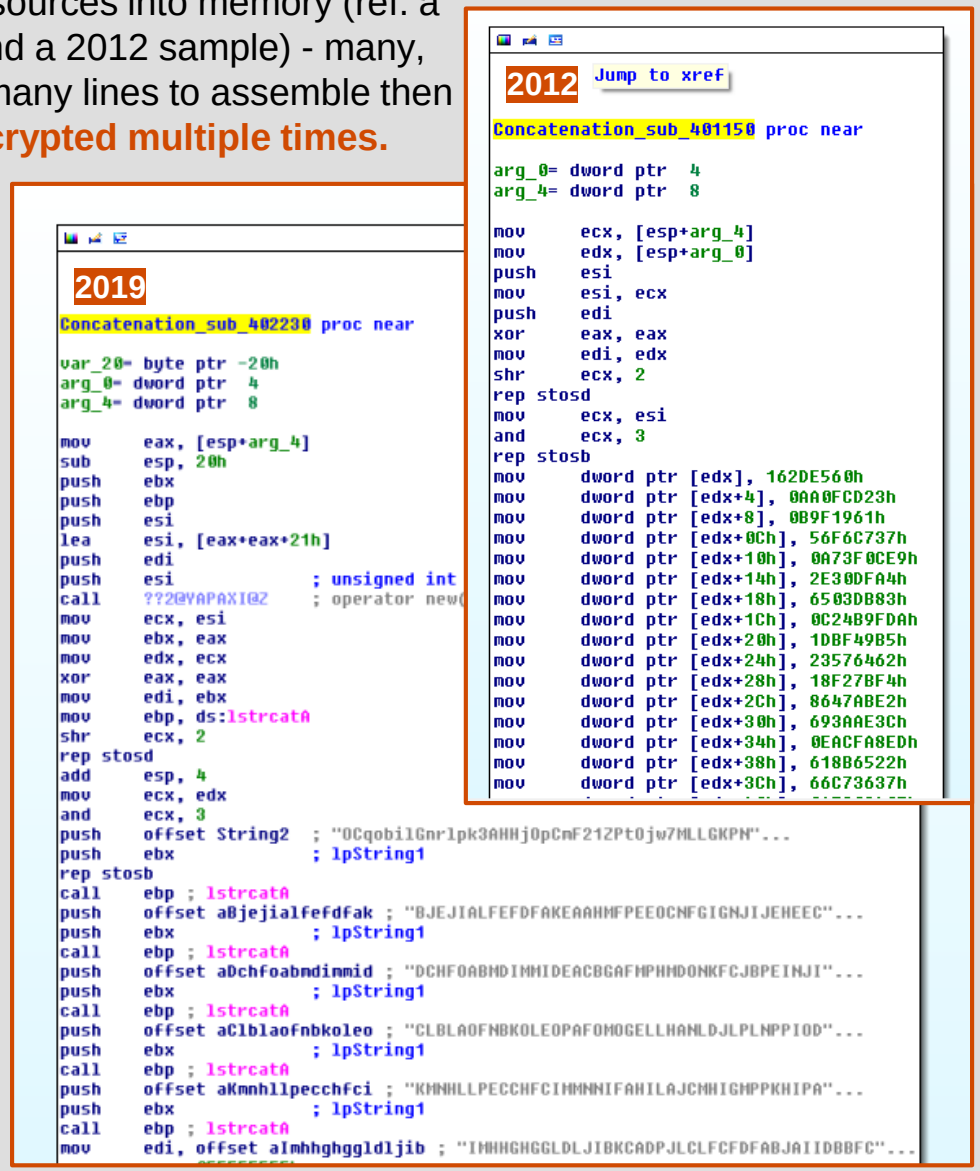
Mutex format (up to 2018):
`x....%02d%02d%02d_%02d%02d...x`

PLEAD C2 requests over HTTP (up to 2019):
`[C2]/0000/(GetTickCount()).[asp|aspx]`

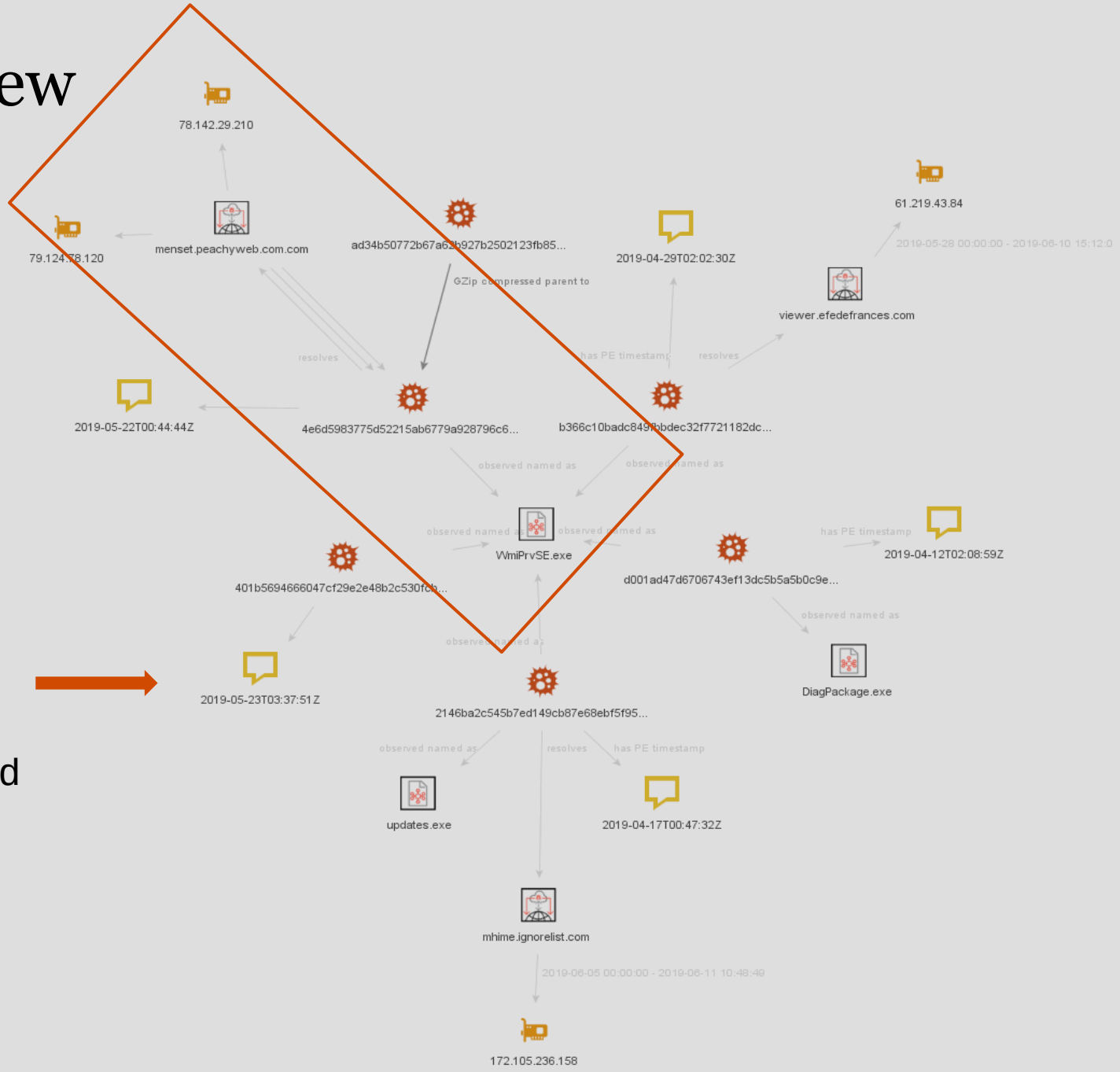
TSCookie cookie configuration:

```
String
L"Mozilla/4.0 (compatible; MSIE 8.0; Win32)"
L"%s:%d"
L"http://%s:%d"
L"Date: %s\r\nConnection: keep-alive\r\nAccept: */*\r\n"
L"Cookie: "
L"%s%02X"
L"%s%s\r\n"
L"Content-type: application/x-www-form-urlencoded\r\n"
L"Connection: keep-alive\r\nAccept: */*\r\n"
L"%sDate: %s\r\n"
L"/N%u.aspx?id=%u"
L"%s:%d"
"getaddrinfo"
"getnameinfo"
"freeaddrinfo"
"\\ws2_32"
"getaddrinfo"
"\\wship6"
"getaddrinfo"
"udp"
"tcp"
"65535"
"udp"
"%u"
```

**Binary blob-building subroutine** from resources into memory (ref. a 2019 and a 2012 sample) - many, many, many lines to assemble then **xor-decrypted multiple times.**



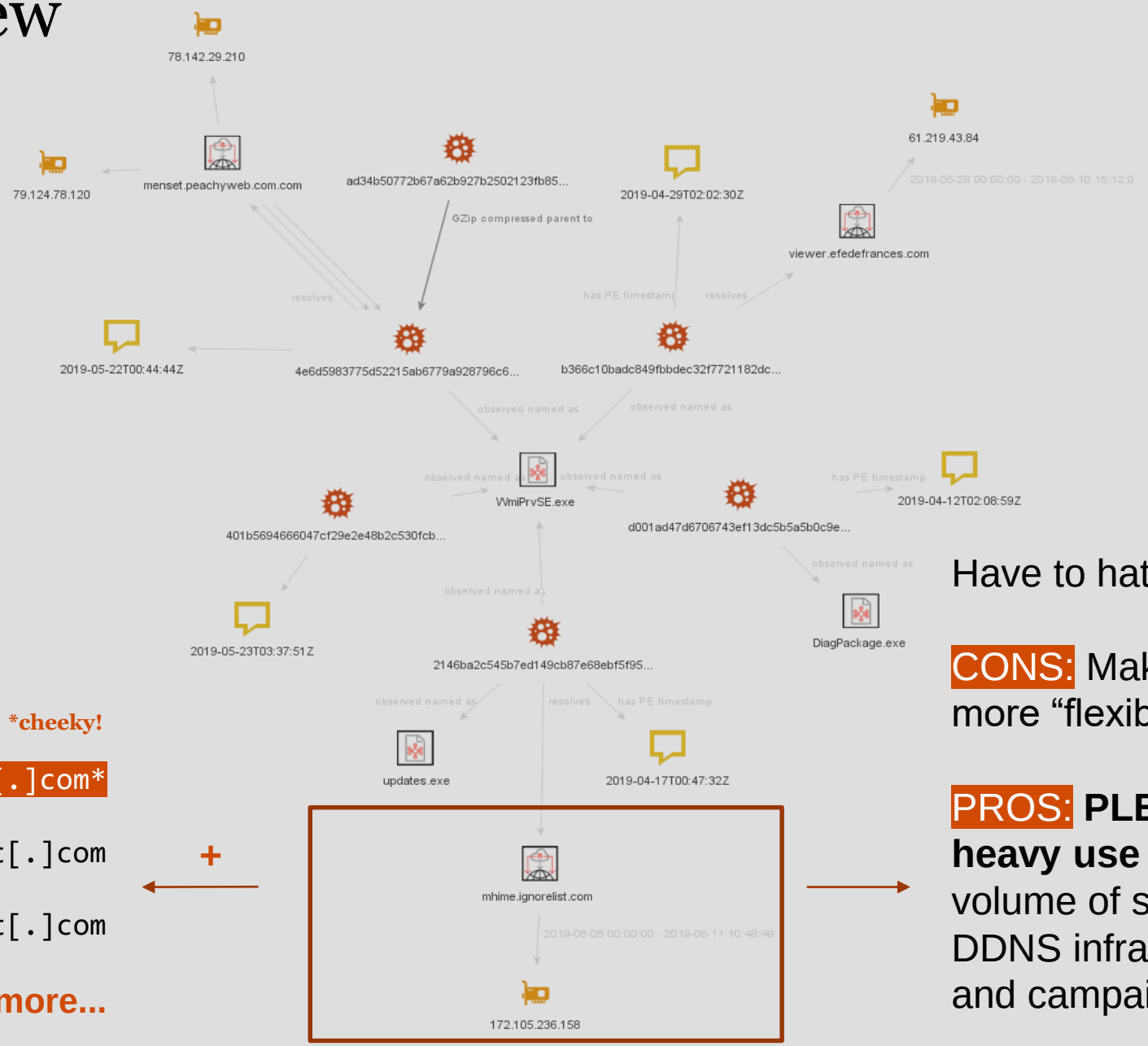
# Campaign View




**Cluster of PLEAD** activity we detected earlier this summer:

- Compile timestamps between early April and late May 2019
- C2 infrastructure active going into mid June 2019

# Campaign View




*cheeky!

`jpcert[.]ignorelist[.]com*`

`subnotes[.]ignorelist[.]com`

`injure[.]ignorelist[.]com`

**and more...**

Have to hate – or love? - DDNS.

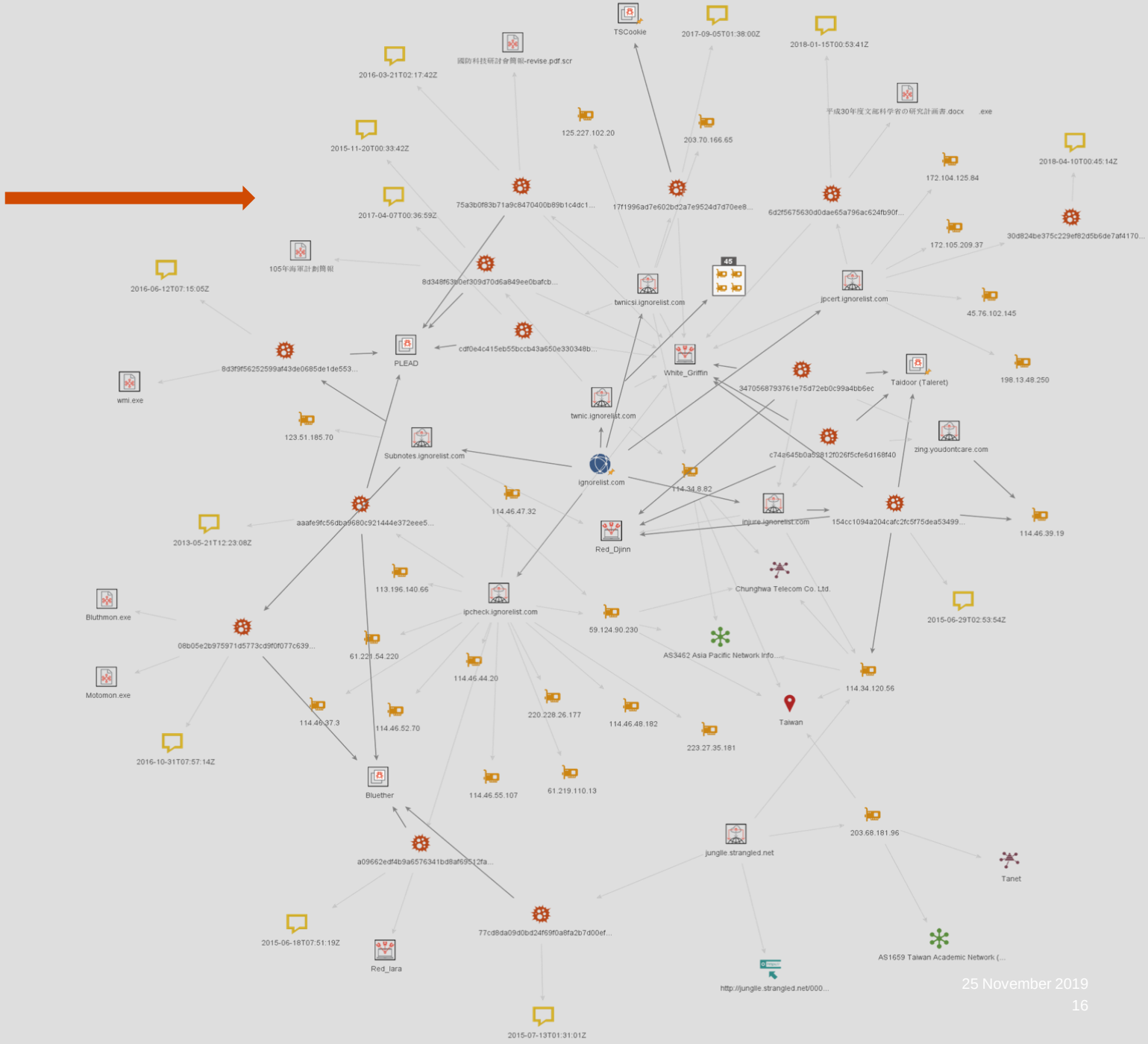
CONS: Makes infrastructure more “flexible” for threat actors.

PROS: **PLEAD actor known for heavy use of DDNS,** large volume of subdomains + reuse of DDNS infrastructure across years and campaigns!

# Following the (P)Leads

> “Someone called the way BlackTech* handles infrastructure “`subdomain explosion`”. That made me think of the Japanese for “fireworks”: 花火 “`hanabi`” (flower-fire). So I like to call it “`subdomain flower`”.
>
> *Mobwork

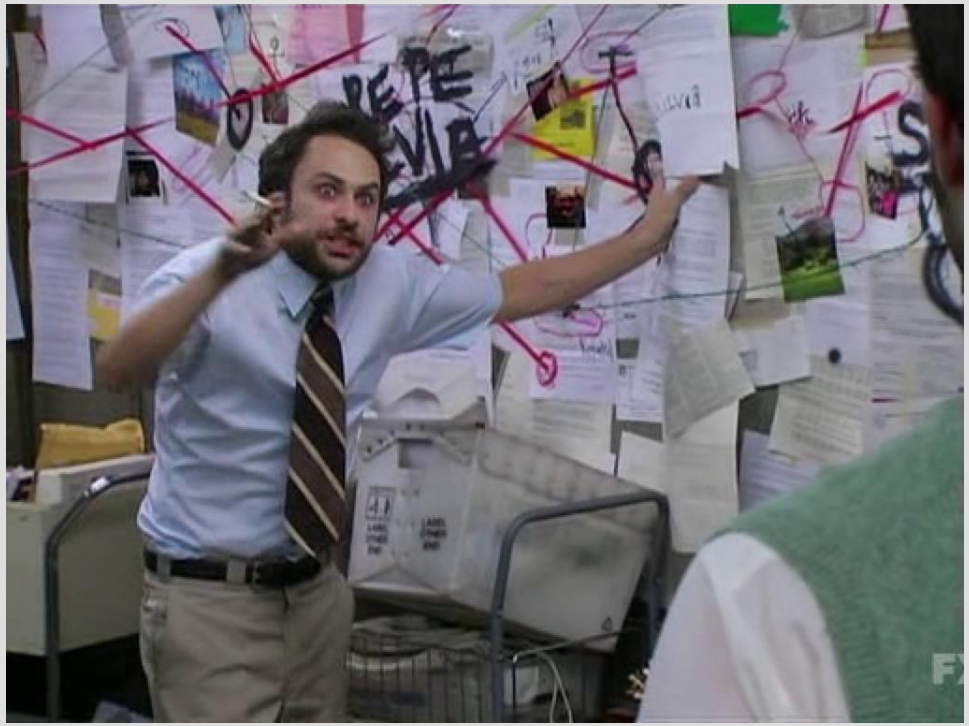
- Years of reuse of the same infrastructure
- Resolutions to TW, HK, occasionally JP
- HINET is a BIG favorite
- Mostly DDNS, compromised routers, compromised infrastructure
- Some adversary-registered domains used for years across different campaigns (e.g. `*[.]microsoftmse[.]com`, `*[.]mobwork[.]net`)

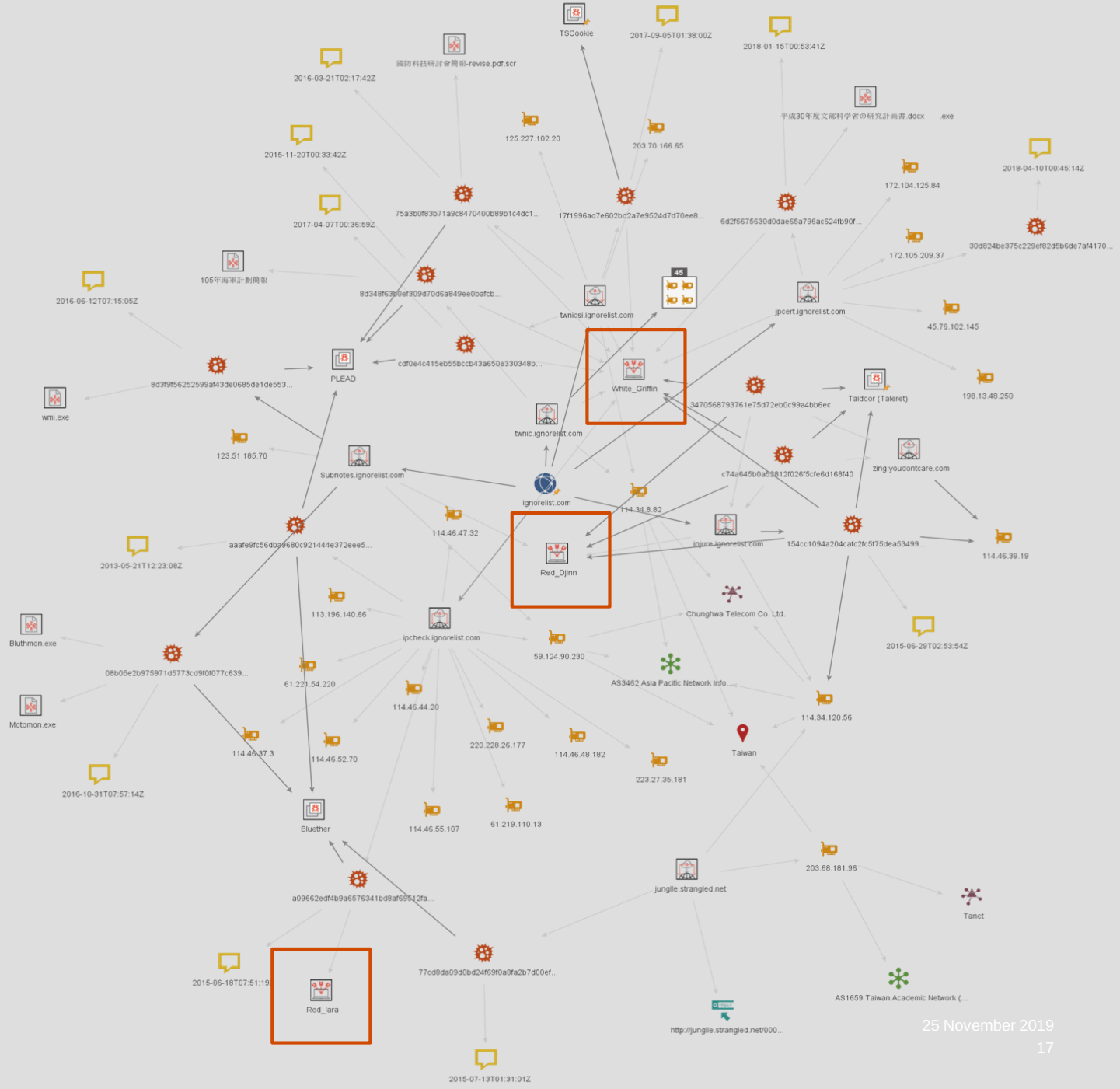


# Following the (P)Leads

**3 (!) threat actors in this graph:**

**White Griffin**
**Red Djinn**
**Red Iara**



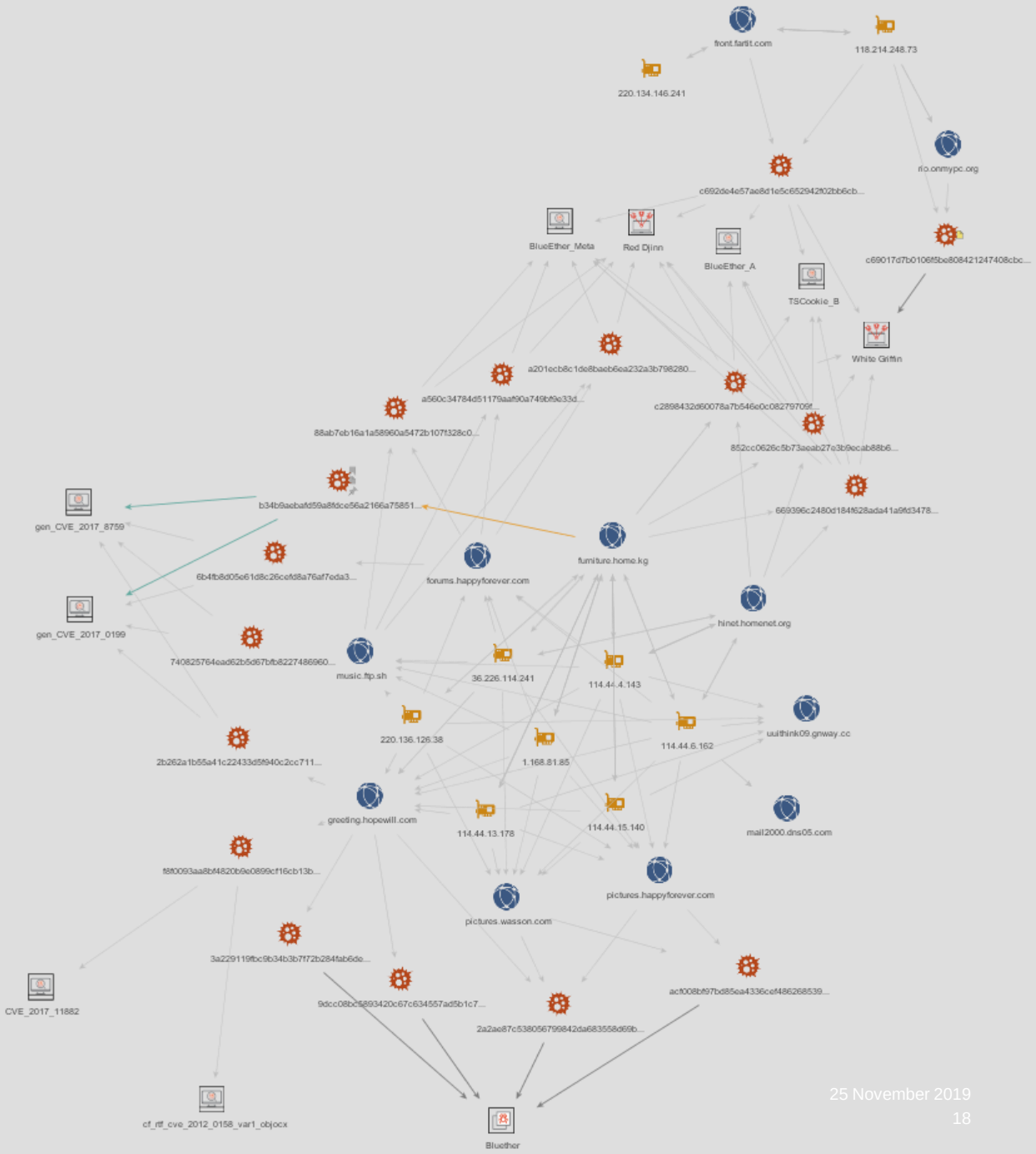


# Seeing Red: A DDNS Story

**PROBLEM:**

- Bluether malware flagged by a detection rule as Red Iara - yet another threat actor set….

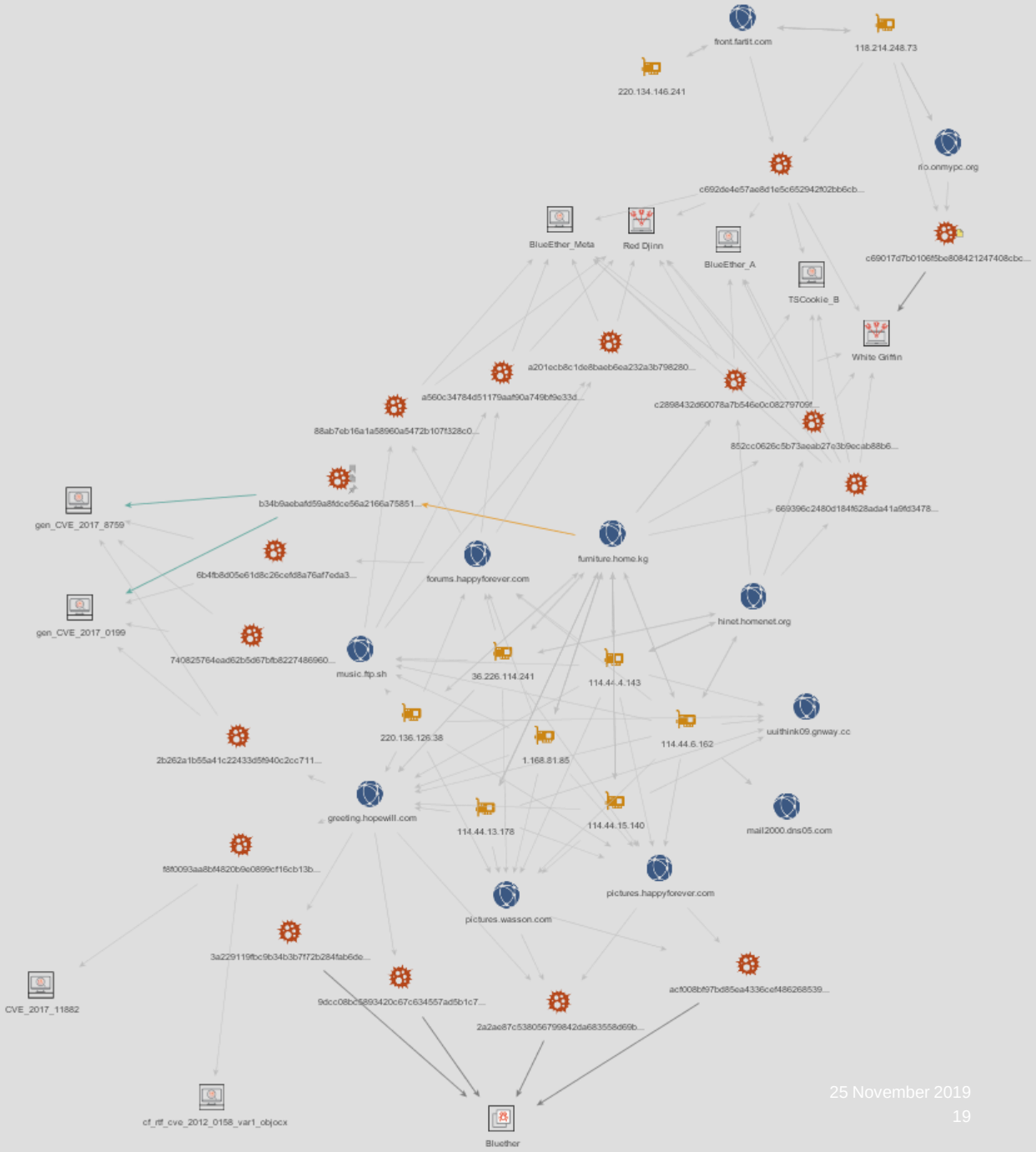
More analysis and a review of the threat actor we track as Red Djinn + associated intrusion set.



# Seeing Red - Part II

**NEW PROBLEM!**

Still confusion - infrastructure associated with Red Djinn delivering PLEAD…..

# Even more names

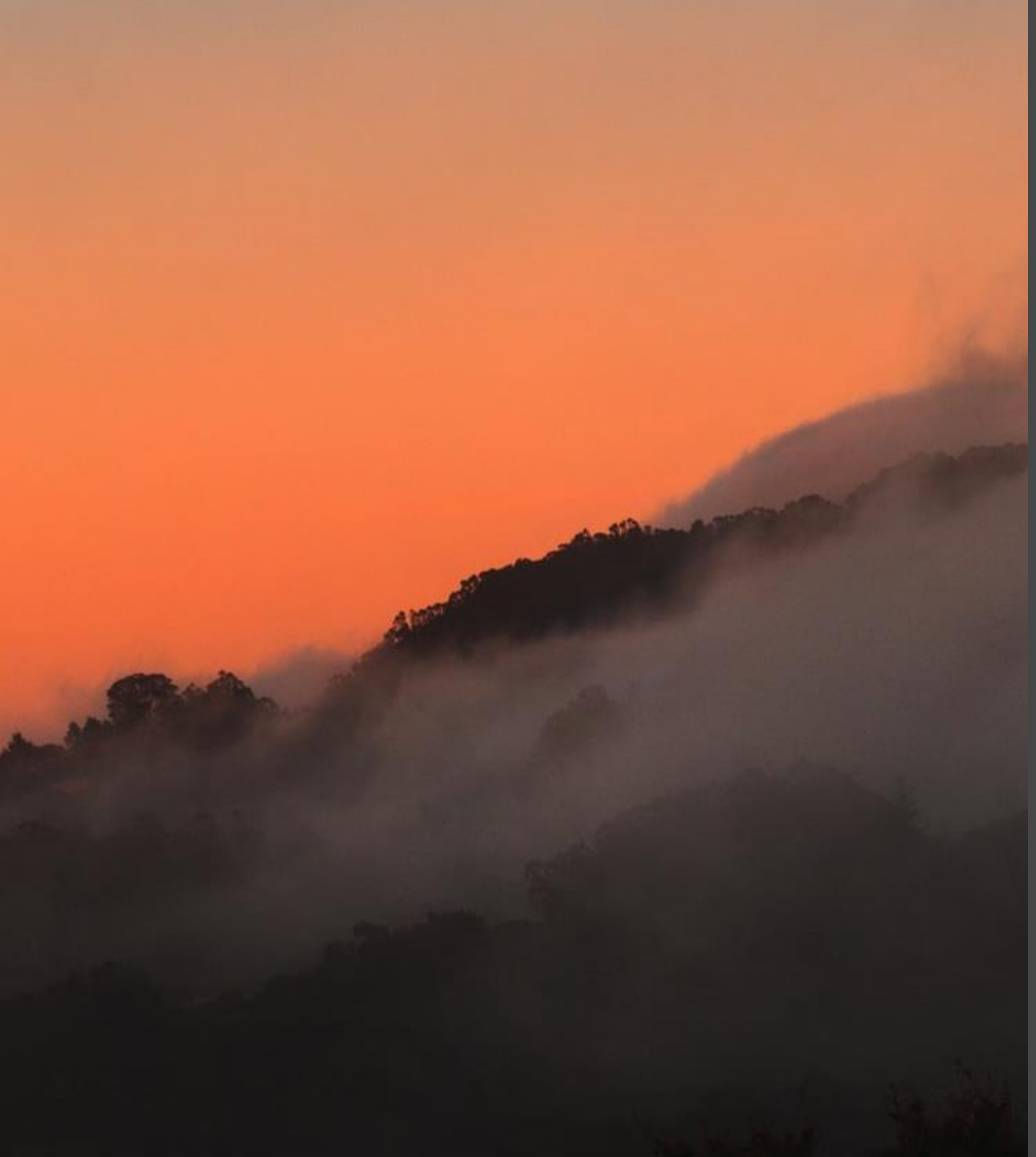
# (P)Lead Actors:

## White Griffin

***A.k.a. BlackTech***

Active since 2010

| | |
|---|---|
| **Targeting** | East Asia (primarily TW, JP, HK), US Government<br>Technology sector<br>Manufacturing, research….. |
| **Tools** | PLEAD, Drigo, BIFROST, Waterbear |
| **Techniques** | Spear phishing targets with malicious lures often taken from victims<br>RTLO<br>Stolen certificates, router exploitation<br>Specific CVEs (e.g. CVE-2012-0158) |



# (P)Lead Actors:

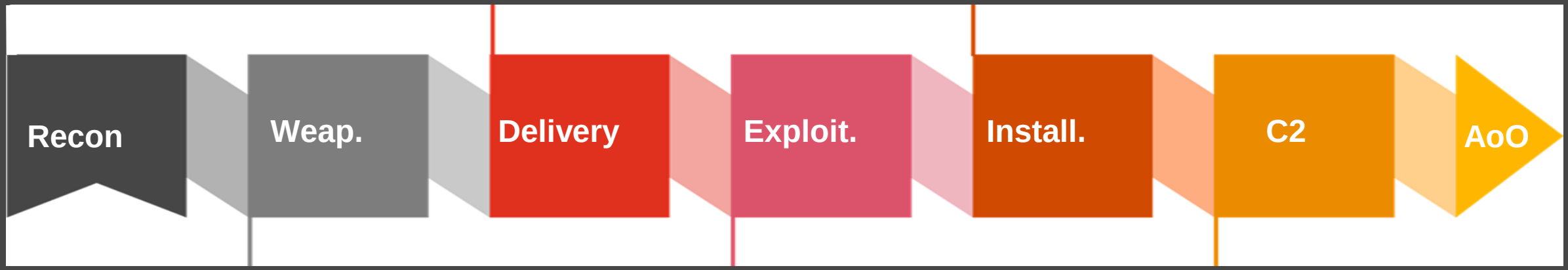
## Red Djinn

***A.k.a. Mofang, Superman***

Active since 2012

| | |
|---|---|
| **Targeting** | South East Asia (primarily MM), US Government<br>Energy (renewables)<br>Manufacturing, defence... |
| **Tools** | Defex/Superman, ShimRat, **PLEAD?** |
| **Techniques** | Spear phishing targets with malicious lures often taken from victims<br>Infrastructure mimicking, proxying<br>Watering holes |

# Kill Chains



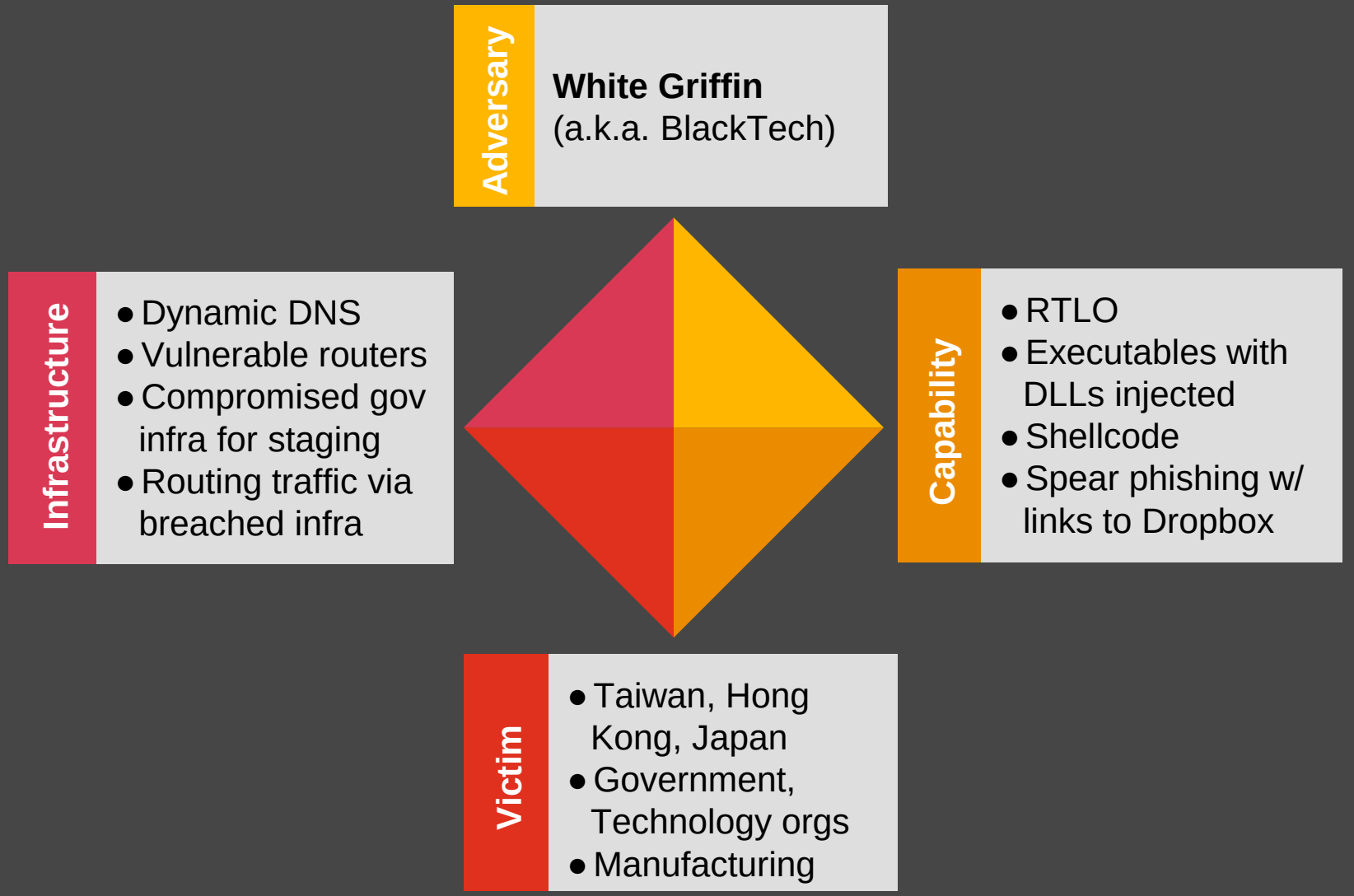

**Red Djinn**

| Recon | Weap. | Delivery | Exploit. | Install. | C2 | AoO |
|---|---|---|---|---|---|---|
| Emulating target environments<br><br>Using relevant/ stolen info/docs against targets | Space padding<br><br>.scr files<br><br>Superman/Shim RAT, Derusbi... | Cloud storage link<br><br>Attachments<br><br>Watering holes | User execution: AV DLL hijacking<br><br>Shellcode in .DAT resources | Shim databases<br><br>UAC bypass<br><br>Autorun registry<br>Service registry | Pre-configured HTTP proxies<br><br>User-Agent: “IE8.0” | Mailbox exfiltration<br><br>File upload |

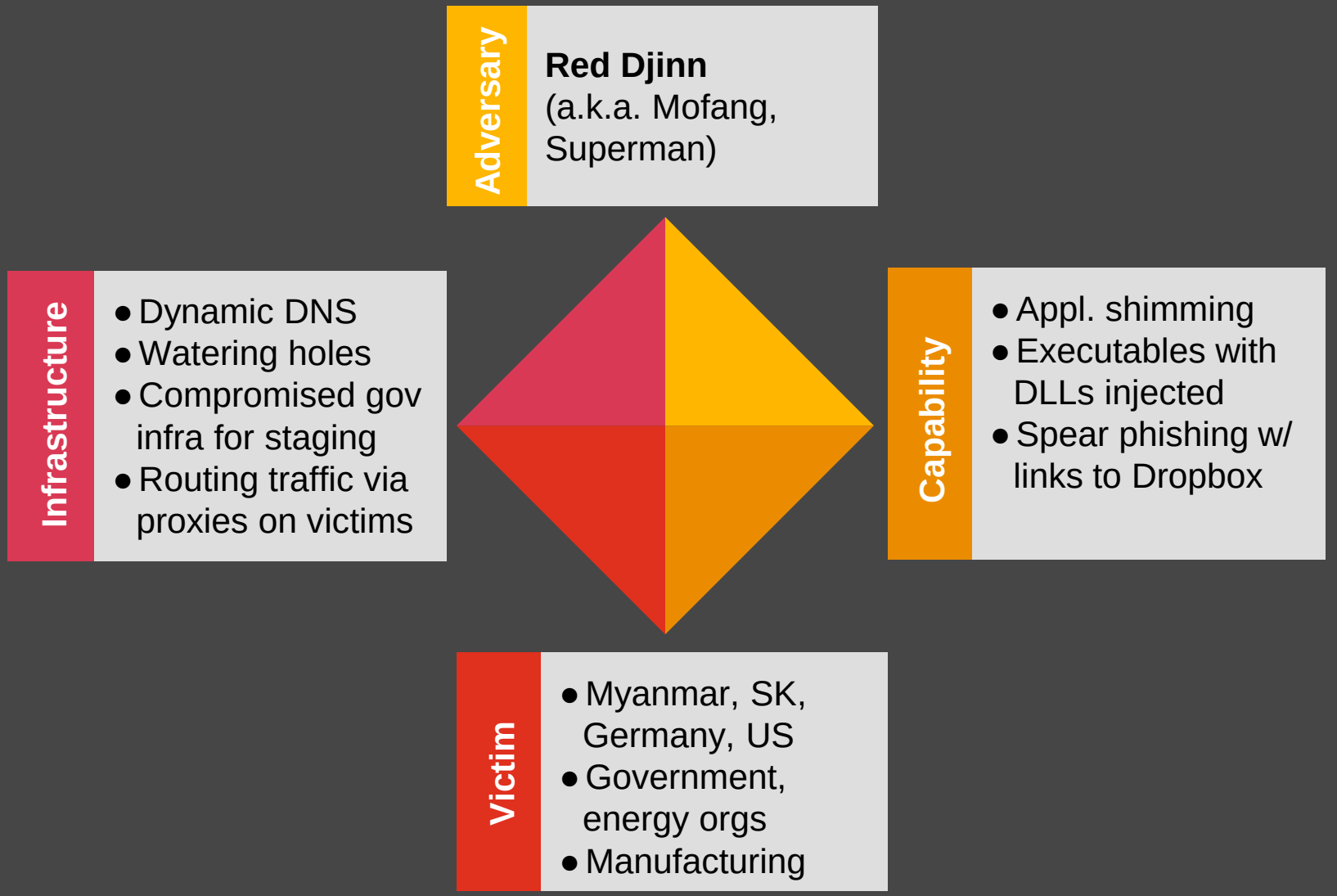
**White Griffin**

| Recon | Weap. | Delivery | Exploit. | Install. | C2 | AoO |
|---|---|---|---|---|---|---|
| Researching topics of interest to targets<br><br>Breaching victims, using info/docs against targets | Space padding<br><br>.scr files<br><br>PLEAD, Drigo KIVARS... | Cloud storage link<br><br>Attachments<br><br>Router MitM | RTLO, CVEs...<br><br>User execution: AV DLL hijacking<br><br>Shellcode in .DAT resources | Autorun registry<br>Service registry | User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)<br><br>.asp/.aspx/.jpg/ .ico/.png/.css | PLEAD exfil via HTTP POST, RC4<br><br>DRIGO file upload/email |

# (P)Lead Actors: Diamond Model



# (P)Lead Actors: Diamond Model



# We assess that it is likely Red Djinn and White Griffin are the same threat actor….

# Need for PLEAD


Analysis ongoing

Attribution = assessment

Constantly revisit

See the opportunity

# Thank you

pwc.com



190104-091457-JS-OS

# References


‘Sherman Kent’s Final Thoughts on Analyst-Policymaker Relations’, Jack Davis, The Sherman Kent Center for Intelligence Analysis, Occasional Papers: Volume 2, Number 3, Jun. ‘03, https://www.cia.gov/library/kent-center-occasional-papers/vol2no3.htm

‘New Targeted Attack Group Buys BIFROSE Code, Works in Teams’, TrendMicro: Razor Huang, https://blog.trendmicro.com/trendlabs-security-intelligence/new-targeted-attack-group-buys-bifrose-code-works-in-teams/ (10th December 2015)

‘PLEAD Targeted Attacks Against Taiwanese Government Agencies’, TrendMicro: Kervin Alintanahin, https://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/ (23rd May 2014)

‘PLEAD The Phantom of Routers’, Team T5: Charles, Zha0, https://hitcon.org/2015/CMT/download/day2-f-r0.pdf (July 2015)

‘ASERT Threat Intelligence Report 2016-03: The Four-Element Sword Engagement’, Arbor ASERT (March 2016)

‘Following the Trail of BlackTech’s Espionage Campaigns’, TrendMicro:Lenart Bermejo, Razor Huang, and CH Lei, https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/ (22nd June 2017)

‘Appendix: Following the Trail of BlackTech’s Espionage Campaigns’, TrendMicro, https://documents.trendmicro.com/assets/appendix-following-the-trail-of-blacktechs-cyber-espionage-campaigns.pdf (June 2017)

‘Malware TSCookie’, JPCERT: Shusei Tomonaga, https://blogs.jpcert.or.jp/en/2018/03/malware-tscooki-7aa0.html (6th March 2018)

# References - continued


Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign', ESET: Anton Cherepanov, https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/ (9th July 2018)

'Plead malware distributed via MitM attacks at router level, misusing ASUS WebStorage', ESET: Anton Cherepanov, https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/ (14th May 2019)

'Malware Used by BlackTech after Network Intrusion', JPCERT: Shusei Tomonaga, https://blogs.jpcert.or.jp/en/2019/09/tscookie-loader.html (18th September 2019)

'Downloader IconDown used by the attack group BlackTech, JPCERT: Shintaro Tanaka, https://blogs.jpcert.or.jp/ja/2019/10/IconDown.html (23rd October 2019)

'Mofang: A politically motivated information stealing adversary', FoxIT: Yonathan Klijnsma et al., https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf (17th May 2016)