Need for PLEAD: BlackTech Pursuit

Sveva Vittoria Scenarelli and Rachel Mullan
November 2019
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

- Bluether
- Bifrose
- Frontshell
- DDNS
- Drigo
- KIVARS
- Waterbear
- Linopid
- xBow
- PLEAD
- Routers
- ShroudedCrossbow Taiwan
- HongKong
- GOODTIMES
- TSCookie
- WhiteGriffin
- BlackTech
History lessons

2010: Shrouded Crossbow first operations begin

2014: PLEAD named (targeting TW gov entities)

2014: 64-bit KIVARS is introduced

Fileless PLEAD developed

BlackTech abuses vulnerable routers in TW, uses Drigo

TrendMicro connects PLEAD, Waterbear, and Shrouded xBow

xBOW revealed, linked to KIVARS and BIFROSE

The Four-Element Sword Engagement (KIVARS on media)

PLEAD variant TSCookie seen targeting JP organisations with gov lure

The PwC report: (P)Lead Actors: White Griffin, Red Djinn

BlackTech steals certs from D-Link, TW technology organisations

TSCookie variant and IconDown downloader detailed

BlackTech conducts router-level MitM attack to deploy PLEAD in TW

PwC report: TSCookie Timelining

Need for PLEAD: BlackTech Pursuit

PwC

25 November 2019
Once upon a time, a detection: Bluether

**ZIP archive: Bluether**
ad34b50772b67a62b927b2502123fb858e05c7e112817d8a4a44a98096b14751

**WmiPrvSE.exe**
4e6d5983775d52215ab6779a928796c60f57321b9c65f4b89135bc0c9b880103

**Injected shellcode**
fdcb5f779d0640659121a2a7c75d1707d0c8f37b833cd528675c405eaa1be650
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:

```
P L E A D
```

```
config
```

```
80 F9 43 cmp cl, 43h ; 'C'
74 2A jz short loc 695
42 inc edx
52 push edx
88 F9 41 cmp cl, 41h ; 'A'
74 1B jz short loc 68D
88 F9 4C cmp cl, 4Ch ; 'L'
74 25 jz short loc 690C
88 F9 45 cmp cl, 45h ; 'E'
74 27 jz short loc 683
88 F9 50 cmp cl, 50h ; '0'
74 29 jz short loc 69A
88 F9 47 cmp cl, 47h ; '0'
74 2B jz short loc 681
88 F9 44 cmp cl, 44h ; '0'
74 2D jz short loc 680
EB 30 jmp short loc 68D
```

Decoding loc_40125F: ; Decoding Subroutine
mou edx, eax
add edx, 11h
mou cl, [esp+edx*140h+var_124h]
mou dl, [ebx+eax*20h]
xor dl, cl
mou [ebx+eax*20h], dl
mou edx, [esp+140h+var_134h] ; in debugger: ebx+eax*20h
inc eax
add edx, 0FFFFFEB0h
cmp eax, edx
to short Decoding_loc_40125F ; Decoding Subroutine
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:

Backdoor status strings:
Recurrent User-Agent:
Malware Analysis: C2 comms

For C2 URL: Calls GetTickCount() ->
Dynamically-generated URRLS: %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.
### PLEDAD: Main Variants

<table>
<thead>
<tr>
<th></th>
<th>BLUETHER</th>
<th>TSCOOKIE</th>
<th>PLEAD Downloader</th>
<th>Fileless PLEAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Executable loader</td>
<td>Executable loader</td>
<td>Executable loader</td>
<td>Lure document</td>
</tr>
<tr>
<td>2.</td>
<td>Shellcode dropper</td>
<td>DLL downloader in memory</td>
<td>Shellcode downloader</td>
<td>Flash CVE-2015-5119</td>
</tr>
<tr>
<td>3.</td>
<td>Executable backdoor</td>
<td>Executable backdoor</td>
<td>Executable backdoor</td>
<td>Backdoor in memory</td>
</tr>
</tbody>
</table>

**WmiPrvSe.exe:**
```
4e6d5983775d52215ab6779a928796c60f57321b9c65f4b89135bc0c9b880103
```

**wuaclt.exe:**
```
FDCB5F779D0640659121A2A7C75D1707D0C8F378833CD528675C405EAA1BE650
```

**Exe:**
```
1da9b4a84041b8c72dad9626db822486ce47b9a3ab6b36c41b0637cd1f6444d6
```

**DLL:**
```
BFD549CDDDAD51B3113155F31D6389EE9C6101965433BD258F28227FCB347946
```

**Wmpnetwk.exe:**
```
a26df4f62ada084a596bf0f0603691bc9c02024be98abec4a9872f0ff0085f940
```

**PLEAD:**
```
e9082b1e8e9a2a4e48e3de1cc1233d202206a8ac2f0d2319c45213ca0204c51
```

**XLS:**
```
9db22b42c71b6532134060a7a175b4eae2c745fa956411389bd7d8c9805ec269
```

**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:

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.
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
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”.

- 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

<table>
<thead>
<tr>
<th><strong>Targeting</strong></th>
<th>East Asia (primarily TW, JP, HK), US Government</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Technology sector</td>
</tr>
<tr>
<td></td>
<td>Manufacturing, research…..</td>
</tr>
</tbody>
</table>

| **Tools**     | PLEAD, Drigo, BIFROST, Waterbear              |

<table>
<thead>
<tr>
<th><strong>Techniques</strong></th>
<th>Spear phishing targets with malicious lures often taken from victims</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RTLO</td>
</tr>
<tr>
<td></td>
<td>Stolen certificates, router exploitation</td>
</tr>
<tr>
<td></td>
<td>Specific CVEs (e.g. CVE-2012-0158)</td>
</tr>
</tbody>
</table>
## (P)Lead Actors:

### Red Djinn

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

Active since 2012

<table>
<thead>
<tr>
<th>Targeting</th>
<th>South East Asia (primarily MM), US Government Energy (renewables) Manufacturing, defence...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools</td>
<td>Defex/Superman, ShimRat, PLEAD?</td>
</tr>
<tr>
<td>Techniques</td>
<td>Spear phishing targets with malicious lures often taken from victims Infrastructure mimicking, proxying Watering holes</td>
</tr>
</tbody>
</table>
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
- Mailbox exfiltration
- User-Agent: “IE8.0”
- File upload

White Griffin
- Researching topics of interest to targets
- Breaching victims, using info/docs against targets
- Space padding .scr files
- PLEAD, Drigo KIVARS...
- Cloud storage link Attachments Router MitM
- RTLO, CVEs...
- User execution: AV DLL hijacking
- Shellcode in .DAT resources
- Shim databases
- UAC bypass
- Autorun registry Service registry
- User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
- PLEAD exfil via HTTP POST, RC4
- DRIGO file upload/email

Researching topics of interest to targets
Breaching victims, using info/docs against targets

Need for PLEAD: BlackTech Pursuit

PwC

25 November 2019
(P)Lead Actors: Diamond Model

Adversary

White Griffin (a.k.a. BlackTech)

Infrastructure

- Dynamic DNS
- Vulnerable routers
- Compromised gov infra for staging
- Routing traffic via breached infra

Capability

- RTLO
- Executables with DLLs injected
- Shellcode
- Spear phishing w/ links to Dropbox

Victim

- Taiwan, Hong Kong, Japan
- Government, Technology orgs
- Manufacturing
(P)Lead Actors: Diamond Model

**Adversary**
- Red Djinn (a.k.a. Mofang, Superman)

**Capability**
- Appl. shimming
- Executables with DLLs injected
- Spear phishing w/ links to Dropbox

**Infrastructure**
- Dynamic DNS
- Watering holes
- Compromised gov infra for staging
- Routing traffic via proxies on victims

**Victim**
- Myanmar, SK, 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

Attribution is hard

Analysis ongoing
Attribution = assessment
Constantly revisit
See the opportunity
Thank you
References


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


References - continued


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