Tracking Earth Aughisky's Malware and Changes

⁝ 10/4/2022

For over 10 years, security researchers have been observing and keeping tabs of APT group Earth Aughisky's malware families and the connections, including previously documented malware that have yet to be attributed.

By: CH Lei October 04, 2022 Read time: 3 min (872 words)

For security researchers and analysts monitoring advanced persistent threat (APT) groups' attacks and tools, Earth Aughisky (also known as Taidoor) is among the more active units that consistently make security teams vigilant. Over the last decade, the group has continued to make adjustments in the tools and malware deployments on specific targets located in Taiwan and, more recently, Japan.

Our research paper, "The Rise of Earth Aughisky: Tracking the Campaigns Taidoor Started," lists all the malware attributed to the group, the connections of these malware families and tools with other APT groups, and the latest updates in illicit activities potentially connected to real-world changes. Our research also covers recommendations and potential opportunities from the changes this APT group appears to be undergoing.

Malware families attributed

This blog post summarizes and highlights some of the malware families and tools with components that have yet to be identified, reported, or attributed to the group. For a full list of all the malware families and tools we attribute to Earth Aughisky, download our research here.

Roudan (also known as Taidoor)

While the name Taidoor has been interchangeably used to refer to the group and the malware, we analyzed that the threat actors named this malware family Roudan while looking at both the backdoor and backdoor builder. This classic Earth Aughisky malware, which was first disclosed over 10 years ago, has been observed for the different formats the group employed for callback traffic as it contains an encoded MAC address and data.

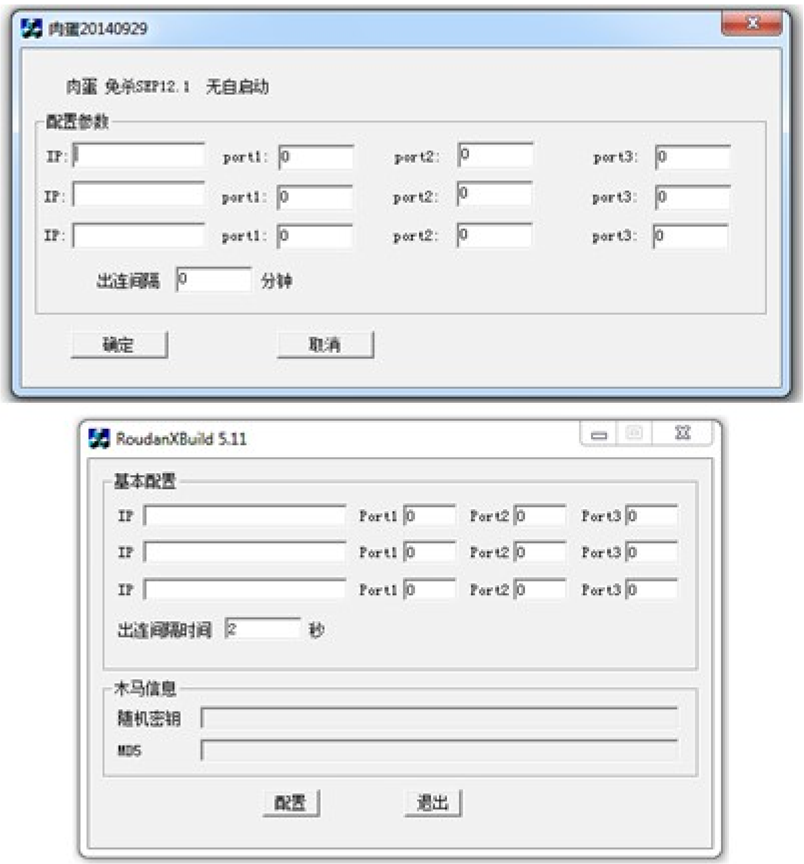
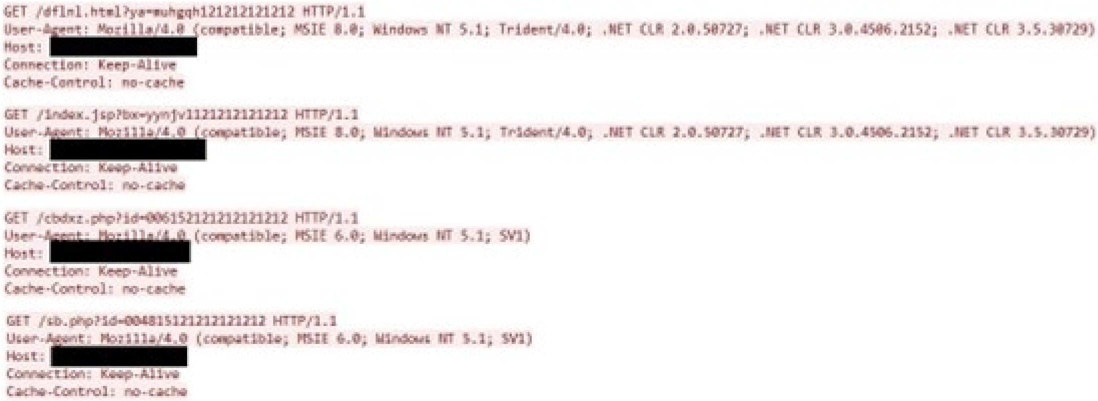


Figure 1. Some of the builders taken from different samples of Roudan



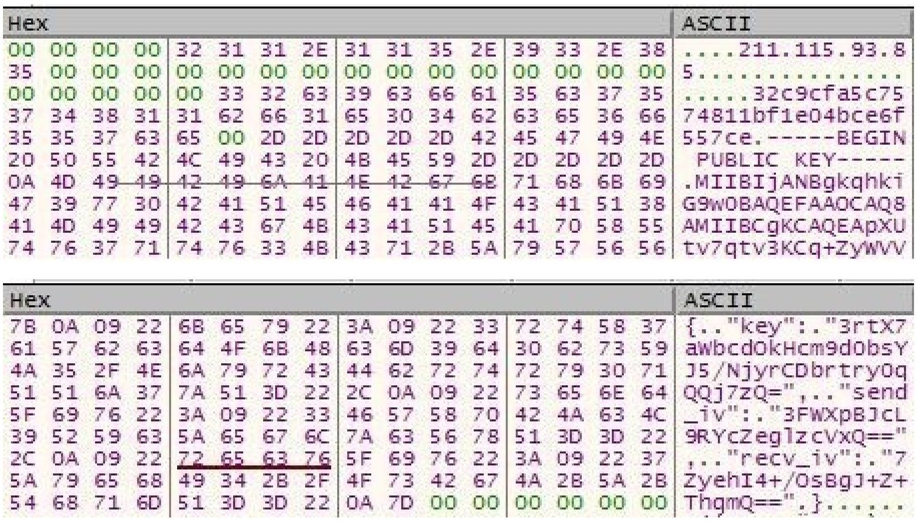
```
GET /dflnl.html?ya=muhgqh121212121212 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: [redacted]
Connection: Keep-Alive
Cache-Control: no-cache

GET /index.jsp?bx=yynjv1121212121212 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: [redacted]
Connection: Keep-Alive
Cache-Control: no-cache

GET /cbdxz.php?id=006152121212121212 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: [redacted]
Connection: Keep-Alive
Cache-Control: no-cache

GET /sb.php?id=004815121212121212 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: [redacted]
Connection: Keep-Alive
Cache-Control: no-cache
```

Figure 2. Roudan network traffic with encoded MAC addresses

LuckDLL

Still unreported, LuckDLL is a relatively new backdoor observed to be active after 2020. The public key is embedded inside the malware configuration and subsequently communicates with the C&C server. LuckDLL then proceeds to generate a random session key and initialization vector (IV) to encrypt the traffic.

The public key encrypts the session key and IV during initial communication, and shared with the C&C.



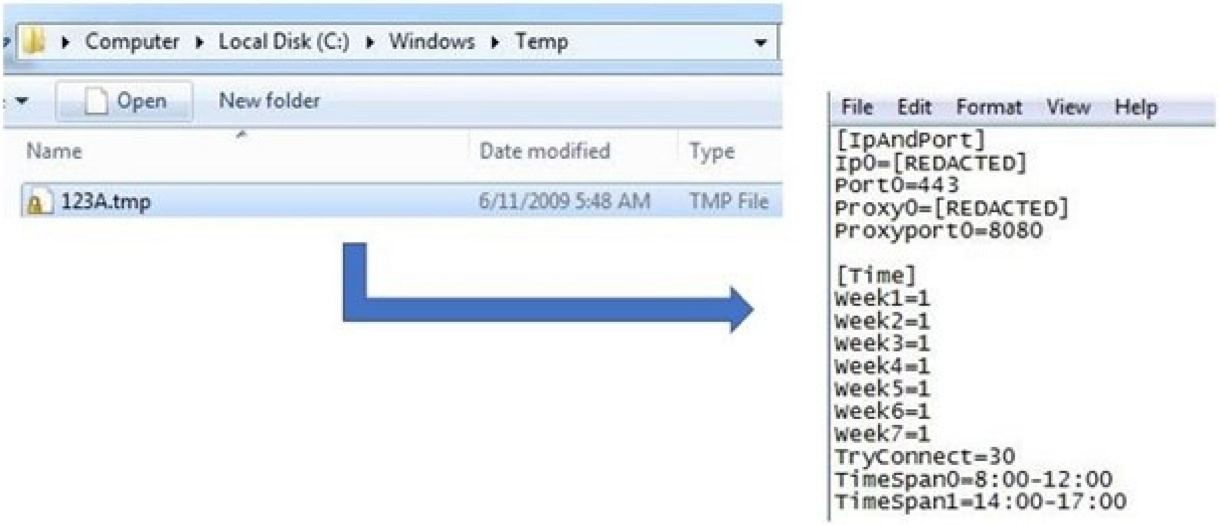
```
Hex                                                  ASCII
00 00 00 00|32 31 31 2E|31 31 35 2E|39 33 2E 38|....211.115.93.8
35 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00|5...............
00 00 00 00|00 33 32 63|39 63 66 61|35 63 37 35|.....32c9cfa5c75
37 34 38 31|31 62 66 31|65 30 34 62|63 65 36 66|74811bf1e04bce6f
35 35 37 63|65 00 2D 2D|2D 2D 2D 42|45 47 49 4E|557ce.-----BEGIN
20 50 55 42|4C 49 43 20|4B 45 59 2D|2D 2D 2D 2D| PUBLIC KEY-----
0A 4D 49 49|42 49 6A 41|4E 42 67 6B|71 68 6B 69|.MIIBIjANBgkqhki
47 39 77 30|42 41 51 45|46 41 41 4F|43 41 51 38|G9w0BAQEFAAOCAQ8
41 4D 49 49|42 43 67 4B|43 41 51 45|41 70 58 55|AMIIBCgKCAQEApXU
74 76 37 71|74 76 33 4B|43 71 2B 5A|79 57 56 56|tv7qtv3KCq+ZyWVV
```

```
Hex                                                  ASCII
7B 0A 09 22|6B 65 79 22|3A 09 22 33|72 74 58 37|{.."key":."3rtX7
61 57 62 63|64 4F 6B 48|63 6D 39 64|30 62 73 59|aWbcdOkHcm9d0bsY
4A 35 2F 4E|6A 79 72 43|44 62 72 74|72 79 30 71|J5/NjyrCDbrtry0q
51 51 6A 37|7A 51 3D 22|2C 0A 09 22|73 65 6E 64|QQj7zQ=",.."send
5F 69 76 22|3A 09 22 33|46 57 58 70|42 4A 63 4C|_iv":."3FWXpBJcL
39 52 59 63|5A 65 67 6C|7A 63 56 78|51 3D 3D 22|9RYcZeglzcVxQ=="
2C 0A 09 22|72 65 63 76|5F 69 76 22|3A 09 22 37|,.."recv_iv":."7
5A 79 65 68|49 34 2B 2F|4F 73 42 67|4A 2B 5A 2B|ZyehI4+/OsBgJ+Z+
54 68 71 6D|51 3D 3D 22|0A 7D 00 00|00 00 00 00|ThqmQ==".}......
```

Figure 3. Public key (top) and session key (bottom)

GrubbyRAT

Following our sensors' observations, GrubbyRAT is deployed only when Earth Aughisky is interested in important targets that follow certain criteria. Still unreported, the configuration file is sometimes installed under an existing application or general system folder and uses the same file name as the component. This suggests that this RAT is installed manually and after the threat actor has gained administrative privileges and control in the infected system.

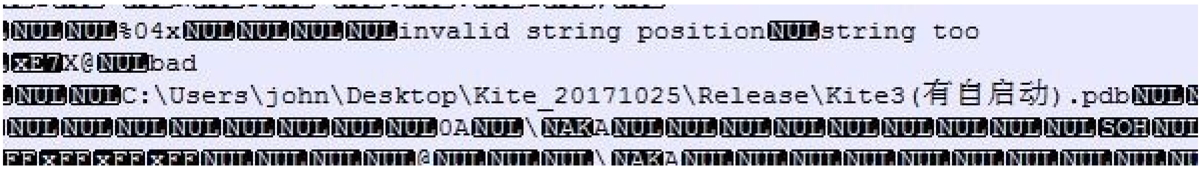


```
[IpAndPort]
Ip0=[REDACTED]
Port0=443
Proxy0=[REDACTED]
Proxyport0=8080

[Time]
Week1=1
Week2=1
Week3=1
Week4=1
Week5=1
Week6=1
Week7=1
TryConnect=30
TimeSpan0=8:00-12:00
TimeSpan1=14:00-17:00
```

Figure 4. Decrypted GrubbyRAT configuration

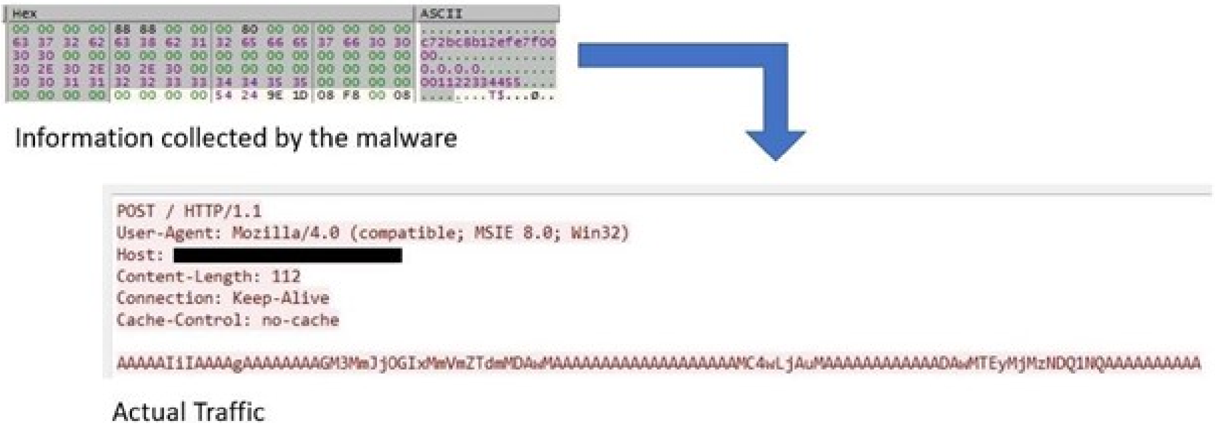
Taikite (also known as SVCMONDR)

While previously reported as SVCMONDR, this malware has yet to be attributed to Earth Aughisky. Previously identified with a 2015 report identifying a vulnerability, some samples of this dropped file observed in Taiwan had a .pdb similar to the APT group's other malware families and tools. The C&C callback traffic is encoded in Base64 and showed a detailed feedback data structure and behavior analysis.



```
NULNUL%04xNULNULNULNULinvalid string positionNULstring too
xE7X@NULbad
NULNULC:\Users\john\Desktop\Kite_20171025\Release\Kite3(有自启动).pdbNULN
NULNULNULNULNULNULNULNUL0ANUL\NAKANULNULNULNULNULNULNULNULNULSOHNUL
FFxFFxFFxFFNULNULNULNUL@NULNULNUL\NAKANULNULNULNULNULNULNULNULNULNU
```

Figure 5. The Taikite .pdb string



```
Hex                                                ASCII
00 00 00 00 88 88 00 00 00 80 00 00 00 00 00 00   ................
63 37 32 62 63 38 62 31 32 65 66 65 37 66 30 30   c72bc8b12efe7f00
30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00   00..............
30 2E 30 2E 30 2E 30 00 00 00 00 00 00 00 00 00   0.0.0.0.........
30 30 31 31 32 32 33 33 34 34 35 35 00 00 00 00   001122334455....
00 00 00 00 00 00 00 00 54 24 9E 1D 08 F8 00 08   ........T$...Ø..
```

Information collected by the malware

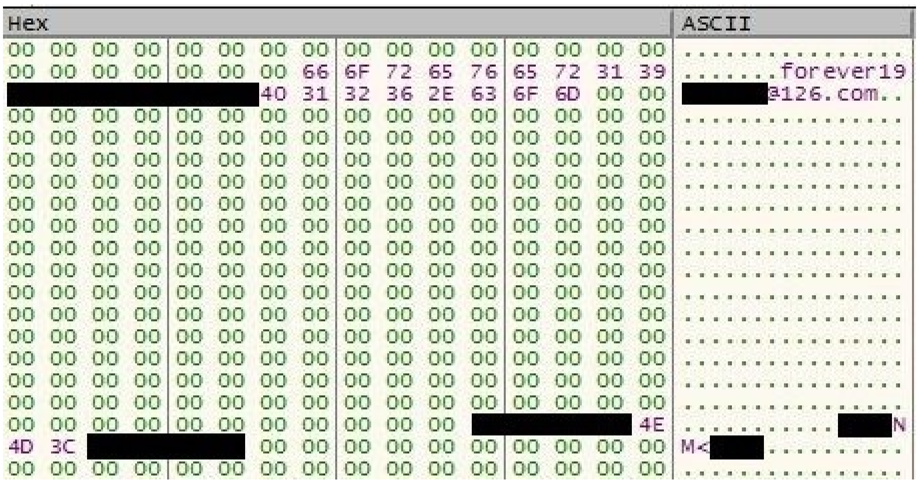
```
POST / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: [redacted]
Content-Length: 112
Connection: Keep-Alive
Cache-Control: no-cache

AAAAAIiIAAAAgAAAAAAAAGM3MmJjOGIxMmVmZTdmMDAwMAAAAAAAAAAAAAAAAAAAMC4wLjAuMAAAAAAAAAAAAAADAwMTEyMjMzNDQ1NQAAAAAAAAAAA
```

Actual Traffic

Figure 6. Taikite traffic

SiyBot

This backdoor has yet to be reported, likely because we observed this tool as being deployed less and only in few attack incidences. SiyBot abuses earlier versions of public services such as Gubb and 30 Boxes to perform C&C communication, wherein the necessary credential or token can be found in the malware configuration. We observed this backdoor to support only a few functions based on the commands we found.



```
Hex                                                ASCII
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 66 6F 72 65 76 65 72 31 39   .......forever19
[redacted]      40 31 32 36 2E 63 6F 6D 00 00   [redacted]@126.com..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 [redacted]      4E   ..........[redacted]N
4D 3C [redacted]      00 00 00 00 00 00 00 00 00 00   M<[redacted].........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

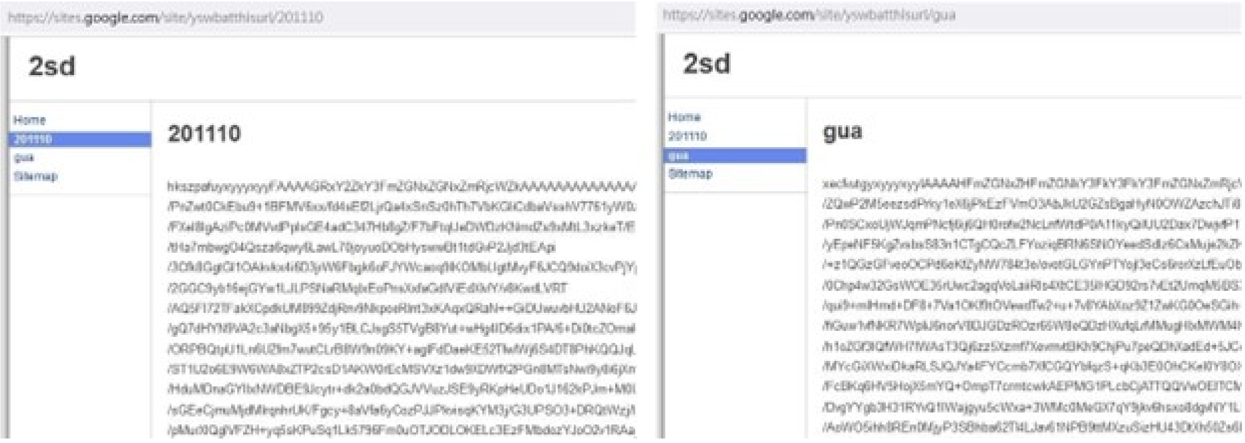
Figure 7. Embedded 30 Boxes credential in the malware

Connections

We feature some of the overlaps and connections we found with Earth Aughisky's malware and tools.

Roudan and SiyBot

We found the same website being used to host Roudan and SiyBot, as well as ASRWEC downloader (a tool we also attribute to Earth Aughisky) payload in the same repository.



https://sites.google.com/site/ywbatthisurl/201110

2sd

201110

[illegible]

https://sites.google.com/site/ywbatthisurl/gua

2sd

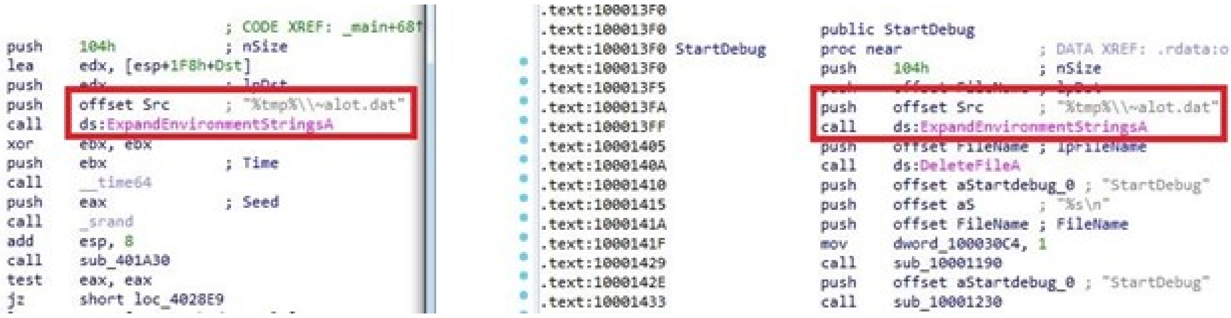
gua

[illegible]

Figure 8. Roudan (left) and SiyBot (right) payload in the same repository

Roudan, Taleret, and Taikite

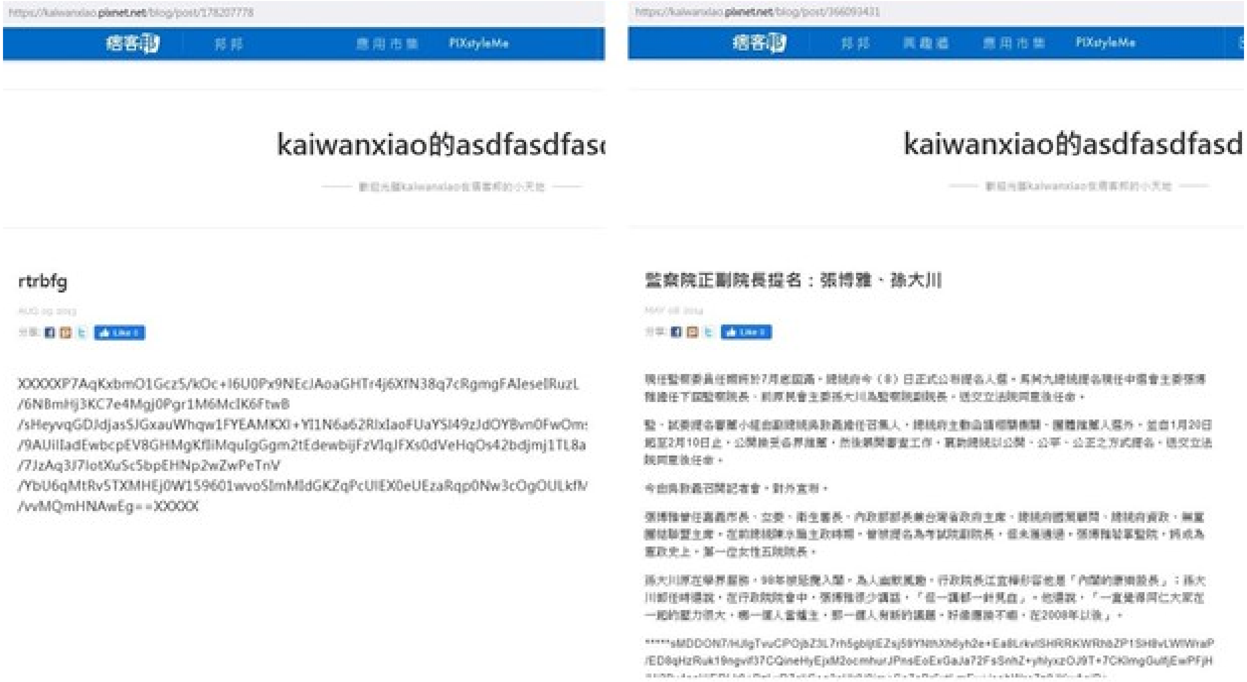
Taleret is another malware family that has been identified or suspected with Earth Aughisky for years. We found overlaps in the C&C servers being used by these malware families, as well as the same hashes, logging mechanisms, and blog hosts between Taleret and earlier versions of Roudan payload.



```
                              ; CODE XREF: _main+68↑
push    104h                  ; nSize
lea     edx, [esp+1F8h+Dst]
push    edx                   ; lpDst
push    offset Src            ; "%tmp%\\~alot.dat"
call    ds:ExpandEnvironmentStringsA
xor     ebx, ebx
push    ebx                   ; Time
call    __time64
push    eax                   ; Seed
call    _srand
add     esp, 8
call    sub_401A30
test    eax, eax
jz      short loc_4028E9
```

```
.text:100013F0
.text:100013F0                 public StartDebug
.text:100013F0 StartDebug      proc near               ; DATA XREF: .rdata:o
.text:100013F0                 push    104h            ; nSize
.text:100013F5                 push    offset FileName ; lpDst
.text:100013FA                 push    offset Src      ; "%tmp%\\~alot.dat"
.text:100013FF                 call    ds:ExpandEnvironmentStringsA
.text:10001405                 push    offset FileName ; lpFileName
.text:1000140A                 call    ds:DeleteFileA
.text:10001410                 push    offset aStartdebug_0 ; "StartDebug"
.text:10001415                 push    offset aS       ; "%s\n"
.text:1000141A                 push    offset FileName ; FileName
.text:1000141F                 mov     dword_100030C4, 1
.text:10001429                 call    sub_10001190
.text:1000142E                 push    offset aStartdebug_0 ; "StartDebug"
.text:10001433                 call    sub_10001230
```

Figure 9. Taleret's special log file (left) compared with Roudan's earlier version (right)



https://kaiwanxiao.pixnet.net/blog/post/178207778

kaiwanxiao的asdfasdfas

rtrbfg

AUG 09 2013

```
XXXXXP7AqKxbmO1Gcz5/kOc+I6U0Px9NEcJAoaGHTr4j6XfN38q7cRgmgFAleselRuzL
/6NBmHj3KC7e4Mgj0Pgr1M6McIK6FtwB
/sHeyvqGDJdjasSJGxauWhqw1FYEAMKXI+YI1N6a62RIxIaoFUaYSI49zJdOYBvn0FwOm:
/9AUiIIadEwbcpEV8GHMgKfIiMquIgGgm2tEdewbijFzVIqJFXs0dVeHqOs42bdjmj1TL8a
/7JzAq3J7IotXuSc5bpEHNp2wZwPeTnV
/YbU6qMtRv5TXMHEj0W159601wvoSImMIdGKZqPcUIEX0eUEzaRqp0Nw3cOgOULkfV
/vvMQmHNAwEg==XXXXX
```

https://kaiwanxiao.pixnet.net/blog/post/366093431

kaiwanxiao的asdfasdfasd

監察院正副院長提名：張博雅、孫大川

MAY 08 2014

[illegible]

*****sMDDONT/HJlgTvuCPOjbZ3L7rh5gbljtEZsj59YNthXh6yh2e+Ea8LrkvlSHRRKWRhbZP1SH8vLWlWraP
/ED8qHzRuk19ngvlf37CQineHyEjxM2ocmhurJPnsEoExGaJa72FsSnhZ+yhlyxzOJ9T+7CKlmgGuIfjEwPFjH

Figure 10. Taleret configuration (left) and Comeon downloader payload (Roudan, right) on the same blog

Insights

As Earth Aughisky is one of the few APT groups that has exercised longevity in cyberespionage, security analysts and teams have collected and continue to gather data to evaluate the group's skills, developments, relations with other APT groups, and their activities. Samples of their malware families and tools allow security teams to gain an understanding of the level of sophistication – or lack of it – of the group's operations, connection, and even changes possibly affecting them from the real-world complexities such as politics and geographic objectives.

To find the complete details of our malware analyses, insights, and attribution connections, download our research paper, "The Rise of Earth Aughisky: Tracking the Campaigns Taidoor Started."

Indicators of Compromise (IOCs)

For a full list of the IOCs, find them here.