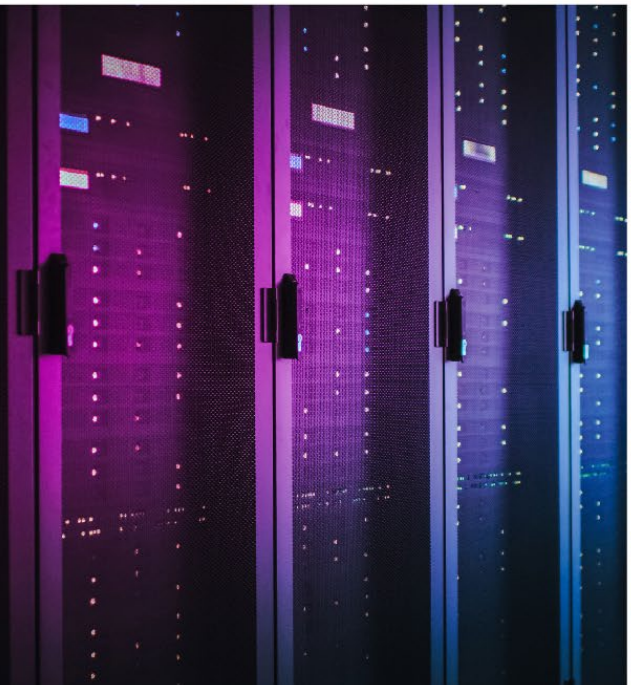





The Rise of Earth Aughisky

Tracking the Campaigns Taidoor Started

CH Lei

TREND MICRO™ | research

Published by

Trend Micro Research

Written by

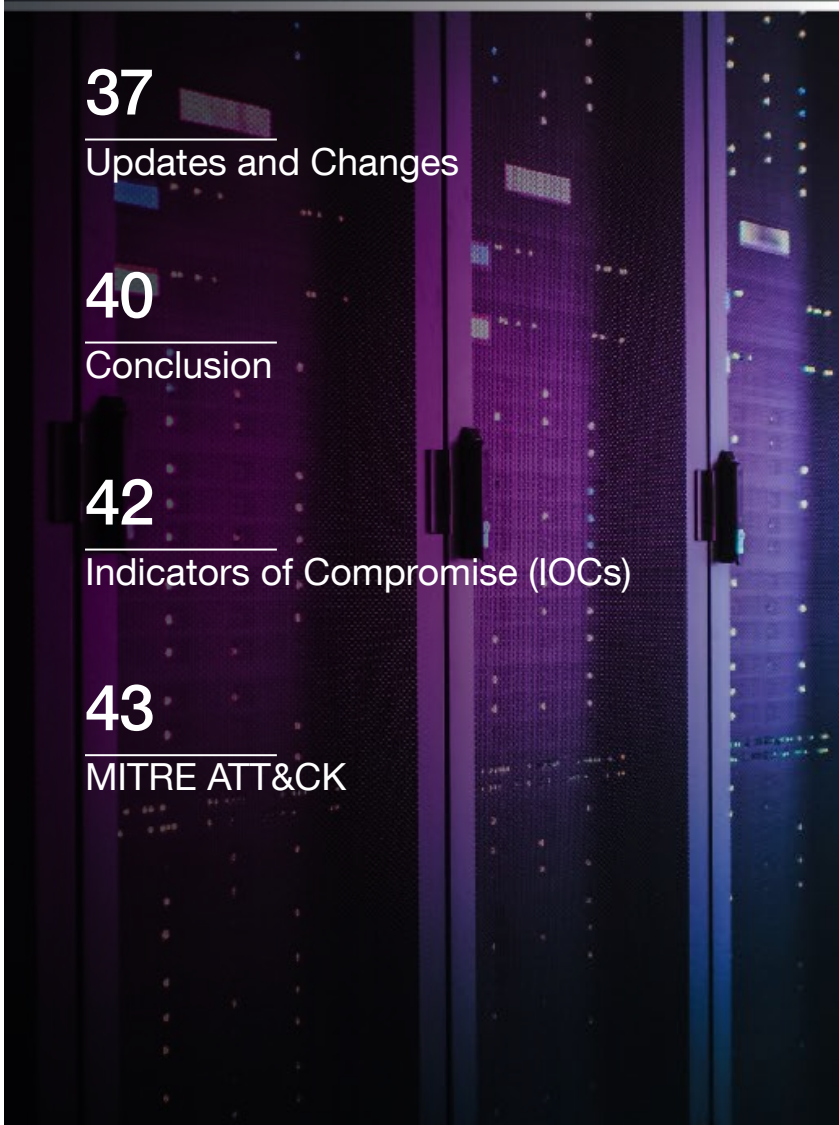
CH Lei

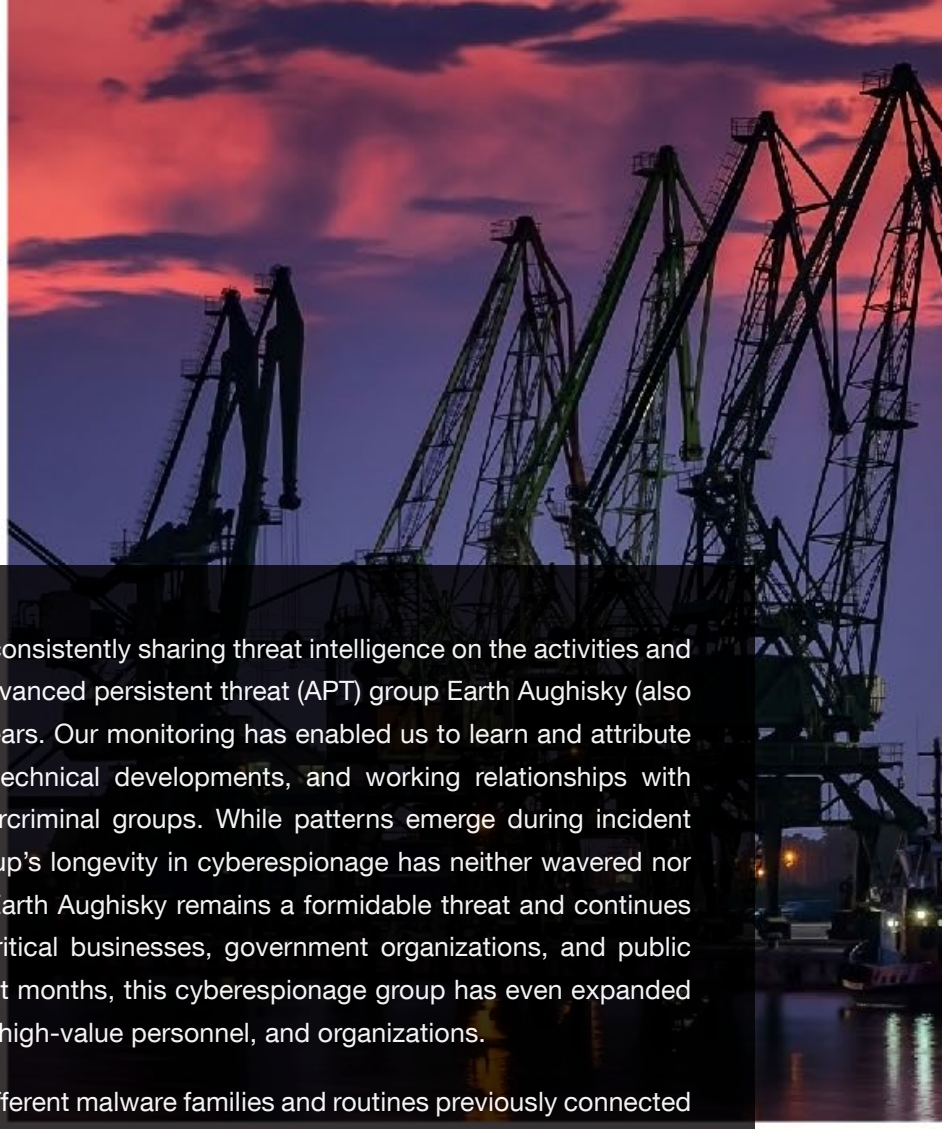
Trend Micro

Stock images used under license from Shutterstock.com and Envato.com

For Raimund Genes (1963-2017)

Contents

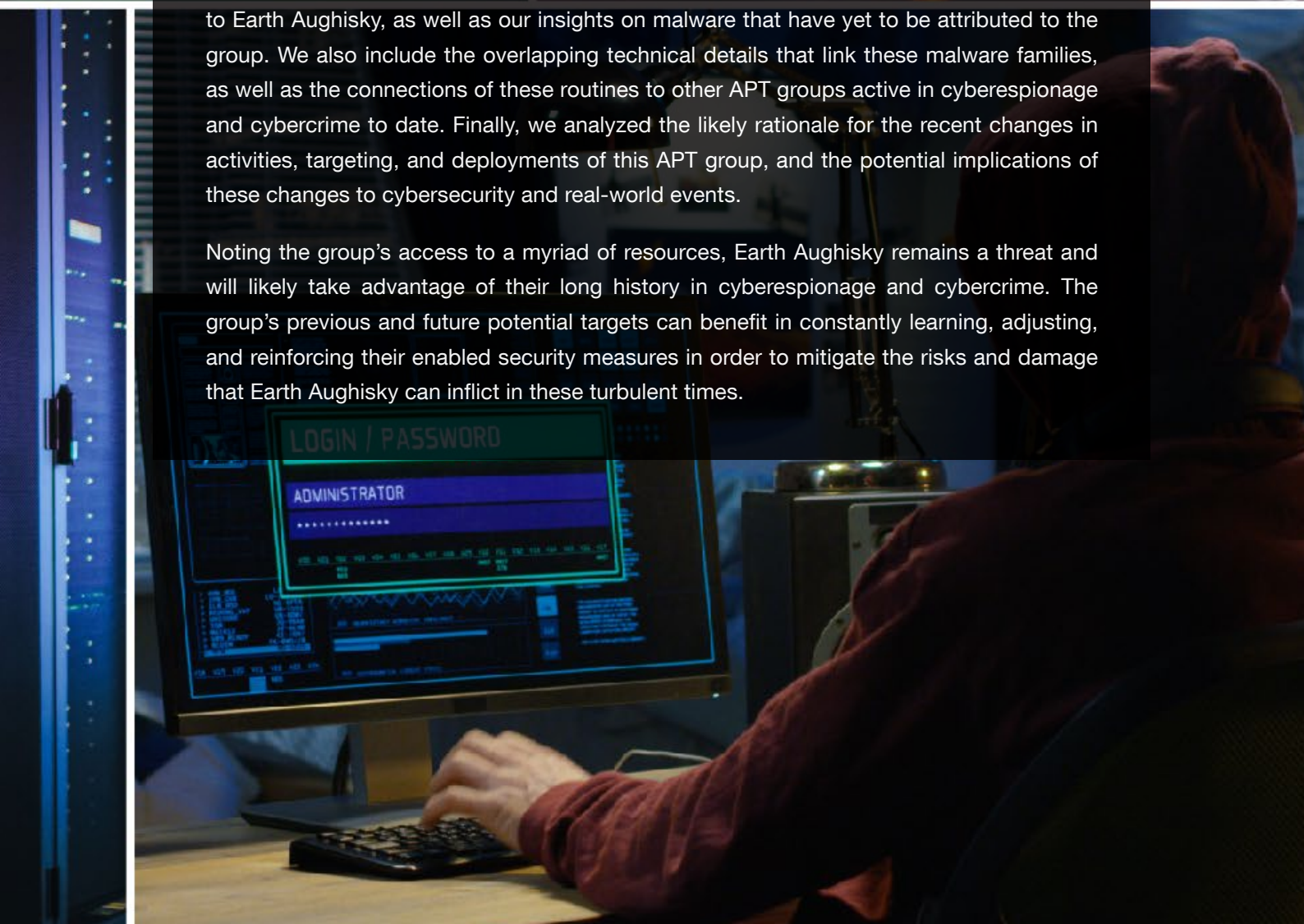




Security researchers have been consistently sharing threat intelligence on the activities and malware families deployed by advanced persistent threat (APT) group Earth Aughisky (also known as Taidoor) for over 10 years. Our monitoring has enabled us to learn and attribute this APT group's movements, technical developments, and working relationships with other cyberespionage and cybercriminal groups. While patterns emerge during incident responses and analysis, the group's longevity in cyberespionage has neither wavered nor become predictable over time. Earth Aughisky remains a formidable threat and continues to disrupt daily operations of critical businesses, government organizations, and public services, among others. In recent months, this cyberespionage group has even expanded operations to target more areas, high-value personnel, and organizations.

In this research, we look at the different malware families and routines previously connected to Earth Aughisky, as well as our insights on malware that have yet to be attributed to the group. We also include the overlapping technical details that link these malware families, as well as the connections of these routines to other APT groups active in cyberespionage and cybercrime to date. Finally, we analyzed the likely rationale for the recent changes in activities, targeting, and deployments of this APT group, and the potential implications of these changes to cybersecurity and real-world events.

Noting the group's access to a myriad of resources, Earth Aughisky remains a threat and will likely take advantage of their long history in cyberespionage and cybercrime. The group's previous and future potential targets can benefit in constantly learning, adjusting, and reinforcing their enabled security measures in order to mitigate the risks and damage that Earth Aughisky can inflict in these turbulent times.



Introduction

While remote access trojan (RAT) Taidoor was disclosed[1] over a decade ago, reports[2] on advanced persistent threat (APT) group Earth Aughisky's campaigns and activities continued[3] to surface[4] as victim organizations come clean on operation disruptions. The group constantly updates[5] malware routines to manage security solutions' developments and remain a formidable threat as the group improves[6] its tactics. In the last decade, Earth Aughisky has deployed a number of associated malware to facilitate their attacks, noted in their varying levels of sophistication.

The group's targets[7] are primarily entities found in Taiwan,[8] with our solutions' sensors detecting 95% of their targeted victims located in the country. In recent years, however, we noticed Earth Aughisky's activities extending to Japan beginning in late 2017 and 2018.[9]

Our sensors caught the first activities targeting Japan towards the end of 2017, matching public reports of observed deployments in 2018. This additional targeting can also be seen to support the organizational changes discussed in the latter part of this research. Earth Aughisky mostly targets government institutions, followed by a significant number of enterprise victims[10] in critical industries.[11]

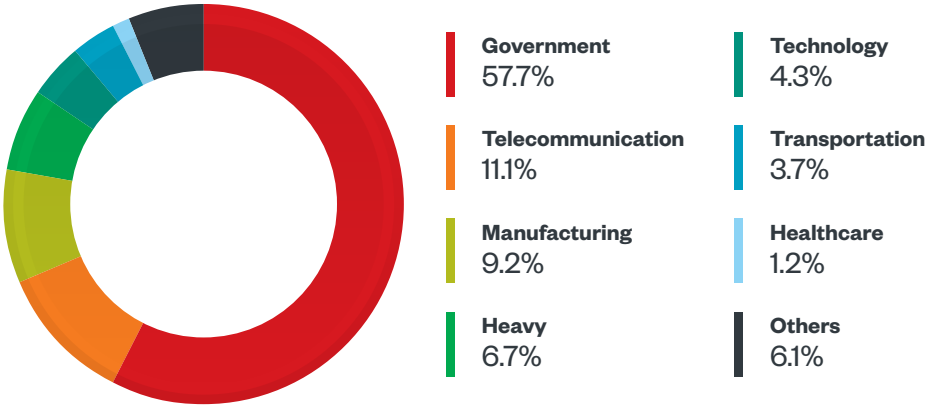


Figure 1. Earth Aughisky's targets distributed by industry

Similar to other APT groups, Earth Aughisky's cyberespionage activities have been closely monitored and tracked. The group uses spear phishing as a common means of entry. Once inside their target's systems, we observed varied efforts at evading detection, such as abusing legitimate user accounts and functions, leveraging weak network architecture designs, and deploying later-stage backdoors, to stay for as long as possible. While some agencies discuss the sensitivities and types of information the group exfiltrates,[12] others have kept these details confidential.

Since then, a number of malware families associated with Earth Aughisky have been disclosed or discussed by different sources, while some have yet to be attributed, documented, or noticed. The following table summarizes the malware families we attribute to Earth Aughisky:

Name	Brief
Roudan (also known as Taidoor)	Earth Aughisky's first attributed backdoor[13]
Taleret (also known as Dalgan)	Backdoor capable of searching for configurations on blogs or other repositories using the following formats:[14, 15] • XXXXX[encrypted configuration]XXXXX • ARTEMIS[encrypted configuration]ARTEMIS
Serkdes (also known as Yalink)	Backdoor identified in incidents involving Japanese organizations
DropNetClient/Buxzop	Abuses DropBox API to perform command and control (C&C) communication[16]
Kuangdao (also known as KD)	Backdoor disclosed in 2020 by the name "Taidoor" loaded by a custom loader, MemoryLoad[17, 18]
Taikite (also known as Svcmondr)	Mentioned in a report on CVE-2015-2545, this backdoor is dropped in the system by an executable file named *svcmondr.exe*.[19]
Specas	Backdoor sometimes identified as Taleret or Roudan
LuckDLL	We found this new backdoor and observed it as active since 2020.
GrubbyRAT	Backdoor with a separate configuration file, often observed in attacks involving critical industries
K4RAT	Backdoor that only contains some basic functions
ASRWEC Downloader	Downloads the final malware payload from a blog (*hxxp://sites[.]google[.]com/site/yswbatthisurl/gua*) or other repositories, and the encrypted payload follows the format *yxyyyxyy[encrypted payload]yxyyyxyy*
Illitat Downloader	Calls back to control server with path fc.asp and dw.html to download actual payload
Comeon downloader	Downloads actual payload from blog (*kaiwanxiao[.]pixnet[.]net/blog/post/366093431*) or other repositories following the format *****[encrypted payload]*****
SiyBot	We discovered this backdoor abusing legitimate applications, such as Gubb or 30 Boxes, to perform C&C communication.

Name	Brief
TWTRAT	We discovered this backdoor abusing social media Twitter's direct message feature to perform C&C communication.
GOORAT	We analyzed this backdoor searching for a command on blog or other repositories, with the format *XXXXX[encrypted command]XXXXX*.

Table 1. Summary of malware associated with Earth Aughisky's campaigns

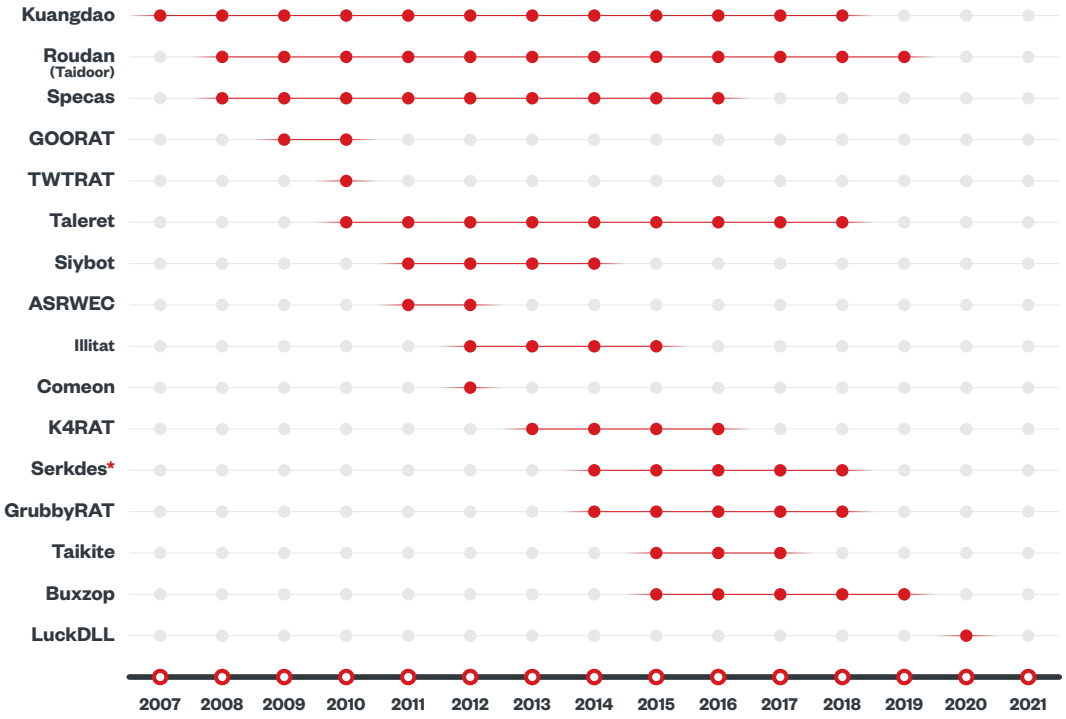


Figure 2. Observed malware activity timeline

(Note: Serkdes might have been shared by different cybercriminal groups, detailed in the Serkdes section)

Each malware serves a different purpose for every Earth Aughisky operation. Some of them are used for initial intrusion, which are usually bundled with spear phishing emails or exploits, where samples can be relatively easy to source. On the other hand, some malware families are used to maintain long-term footprints, activated through more sophisticated techniques, and sometimes wrapped with an extra loader.

Among the backdoors used in later stages, few are hidden more and most of the time can only be observed in routines deployed to high-value targets. The variations in approaches based on the number of factors reduce the chance that important operations get disrupted and make important tools less likely to be disclosed. Our observations showed that among the targets categorized as "Important"

include industries such as critical infrastructure, government agencies, and military-related organizations. Meanwhile, “General” targets include vulnerable systems or offices in other industries like the healthcare sector.

Categorization	Malware Families Used
Initial intrusion	Roudan, Taikite, ASRWEC / Comeon / Illitat Downloader
Later stage payloads	Taleret, Kuangdao, Specas, Serkdes
Later stage payloads: High-value targets	Buxzop, GrubbyRAT
Short-lived / Not widely used	TWTRAT, SiyBot, GOORAT
Not enough data to categorize	LuckDLL, K4RAT

Table 2. Observed malware usage per campaign target

Malware

This section details our analysis for every malware, including their routines and significant characteristics.

Roudan (Taidoor)

Roudan is the classic Earth Aughisky malware that was disclosed over 10 years ago. Over the years, different formats have been used for callback traffic, which basically contains an encoded MAC address and some random data. Detailed malware analysis are available in previous reports.

```
GET /index.jsp?bx=yynjvl121212121212 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 /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 /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 3. Roudan network traffic, wherein *121212121212* is the encoded MAC address for *010101010101*. *INTERNET_FLAG_SECURE* is sometimes enabled since April 2018

Although the name “Taidoor” has been adopted widely for years, threat actors actually name this malware “Roudan.” The term can be observed in looking at both backdoor and backdoor builder. A few samples contain a simplified Chinese version of Roudan, which is “肉弹” or “肉蛋” (although not exactly the same, “肉弹” has a meaning similar to “cannon fodder”).

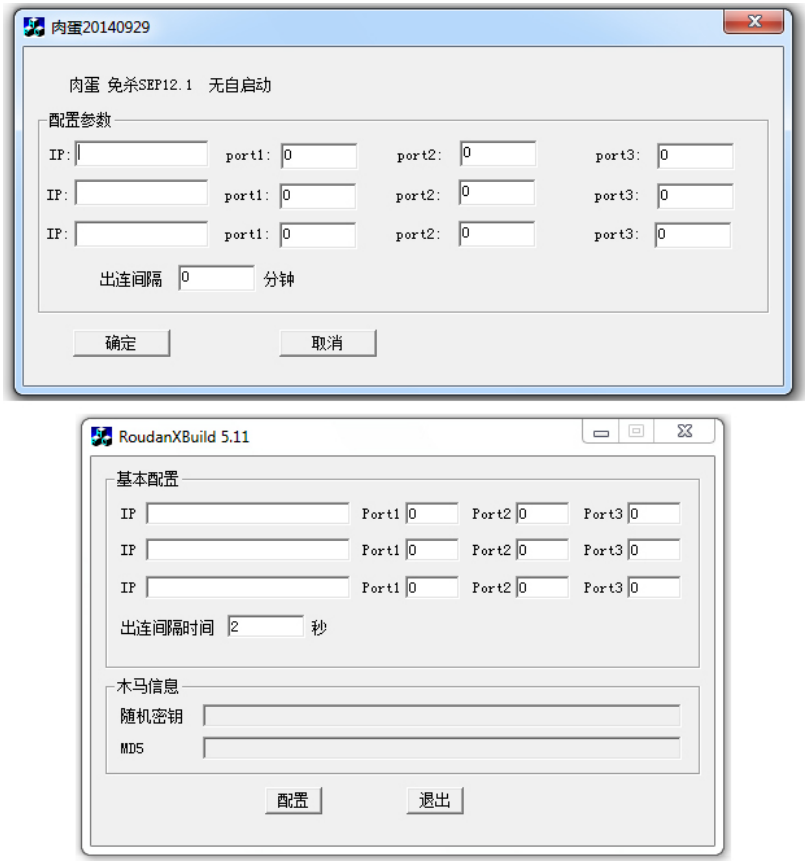


Figure 4. Roudan builders

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/    cmdgetfileask    run
%s  wetdx0  cmdrunexe  set time %d to sleep %d s   connected  aaaaaaaa    connect
http://%s:%d/%s.jsp?%c%c=%s nSleepTime:%d   %d  %s  EXPLORER.EXE    while  system  real
service   aa  %c%c%d   x00   %s.lz   %s %%temp%%\%u thread  GET HTTP/1.1    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) fInternetOpen 0x%08x, %s %d %s %d   E:\ziliao\roudan
\rd-get-addc-format\rd-get\MsgHandleDll\MsgHandleDll.cpp    enter getdata   Content-
Type: application/x-www-form-urlencoded POST    %02X-%02X-%02X-%02X-%02X-%02X   01-01-
01-01-01-01   w+b Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) %temp%\ %c%c
%c%c%c%c.exe            瑾 □    .?AVtype_info@@
```

Figure 5. The Roudan project name (*Hash: 18c67331716ae672e46583700c4a3eb2abdaa61c*), “ziliao,” is written as “資料,” which simply means “data”

Taleret (Dalgan)

Taleret malware was disclosed in 2013[20] and has been repeatedly mentioned[21] with Roudan/Taidoor in different reports.[22,23], [24] The malware searches for C&C configurations on public blogs or other repositories and uses “XXXXX” or “ARTEMIS” as maker to locate the configuration. The configuration can be decrypted using Rivest Cipher 4 (RC4) key “C3 7F 12 A0”.[25]

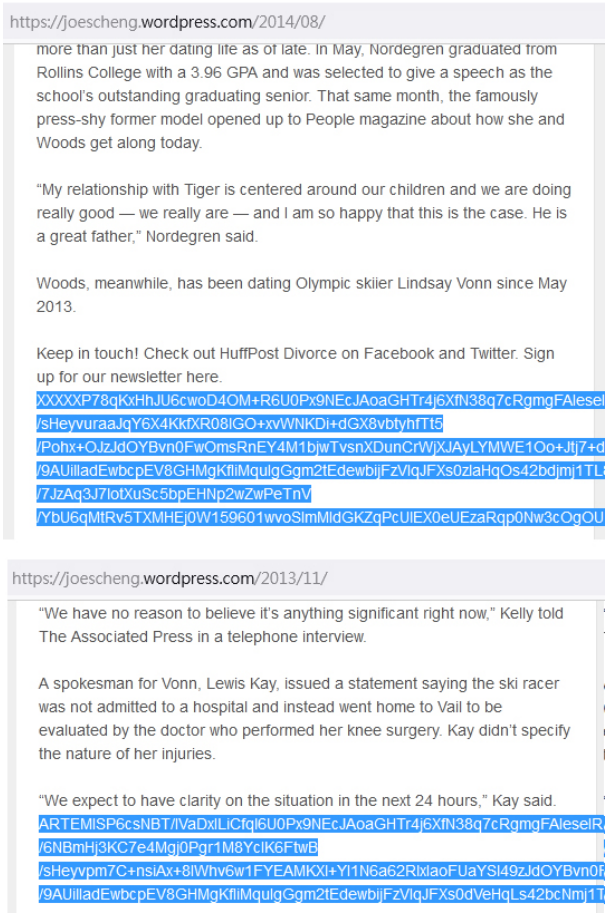


Figure 6. Two different types of configurations found on the same blog

Technically, any service that serves configurable content can be abused to host the malware configuration. From our observations, there are also other web services embedded inside the malware.

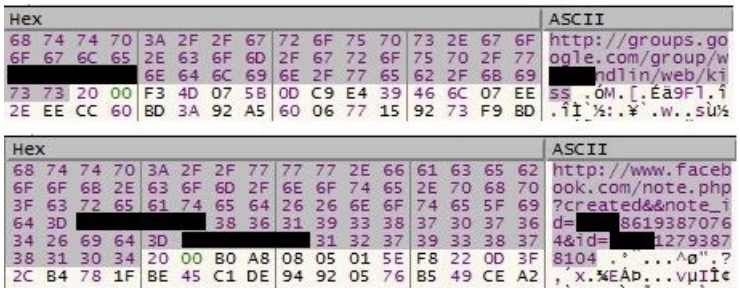


Figure 7. A special configuration host setting in Taleret capable of retrieving data from the blog and C&C server. In this example, Google groups (*Hash: f2dfd3910017cd9b3798e9b9dce8ddcace5c6af6*) and Facebook (*Hash: 0dfd5669f67a3a992817ca6db096a4cbeadc3257*) are abused to host malware configurations.

There are two different Taleret implementations. A simpler one uses “XXXXX” as a marker, while another uses “ARTEMIS” as a marker, which has more accompanying functions.

XXXXX Implementation

Once the backdoor retrieves the actual C&C server, it proceeds to save the configuration to the registry *<Software\Microsoft\SysInternal>* in case the configuration is not available next time. The implementation then calls back to the C&C server with Cookie MCI and MUID.

While MCI contains an encoded MAC address and IP Address with a corresponding logic, MUID is a random string generated based on CoCreateGuid or GetTickCount.

MAC and IP Address Original Characters	Encoding Logic
'0'~'9'	<ASCII Code> + 0x18
'.'	Transfer to 'R'
'A' ~ 'F'	<ASCII Code> + 0x1

Table 3. MAC and IP address encoding in the MCI

```
GET / 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
Cookie: MCI=HHIIJJKKLLMMIQJRINPRIIIRIII; MUID=8fd7513a40d502402e7b0000
```

Figure 8. XXXXX implementation traffic

Security teams and analysts can note that some samples drop the special log file at *%tmp%\~l.dat*, which contains the execution history.

```
File  Edit  Format  View  Help
09/13/17 19:24:22 - fail url: http://tw.myblog.yahoo.com/jw!tDHYEqOfHxIzJUO_fpKyMEs-
09/13/17 19:24:51 - fail url: http://blog.yam.com/tradegover/article/31069985
09/13/17 19:24:52 - fail url: http://tw.myblog.yahoo.com/jw!8PlorjKfHxI_lhNlDk_FeAU-
```

Figure 9. The ~alot.dat log file

ARTEMIS Implementation

Studying the ARTEMIS implementation, the traffic contains information similar to MCI and MUID. But instead of using a Cookie, it sends the information to the C&C server using an HTTPS post. The traffic starts with "SVc5" followed by a hardcoded "1", the size of both MCI and MUID feedback information, and the encoded information itself. Studying the samples, we noticed that after 2015, the header changed to "SSSS" from "SVc5", suggesting two different malware protocols in place, but analysis on the feedback information showed that it remained largely the same.

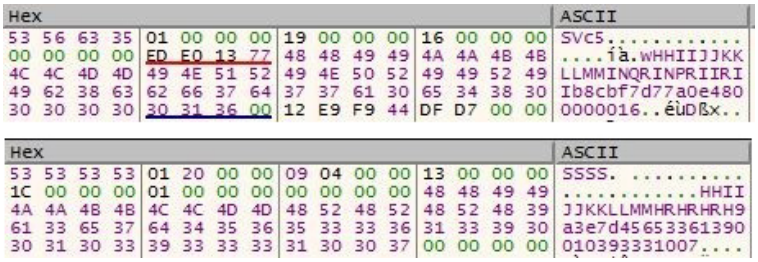


Figure 10. ARTEMIS implementation traffic before 2015 (top), and after 2015 (bottom)

Although it's disabled in most samples, this implementation is capable of dropping the log file under *%tmp%\~ah[4 random number].dat*, which contains information likely designed for debugging.

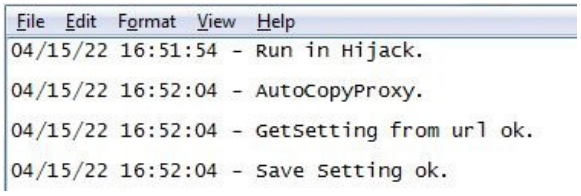


Figure 11. The ~ah[four random numbers].dat log file

Serkdes (Yalink)

In 2018, security researchers NTT[26] and Macnica[27] reported malware Serkdes found in Taidoor-related incidents. In some versions, Serkdes is capable of loading the configuration from a separate file, sysconf.dll, via the executable GetPrivateProfileStruct.[28]

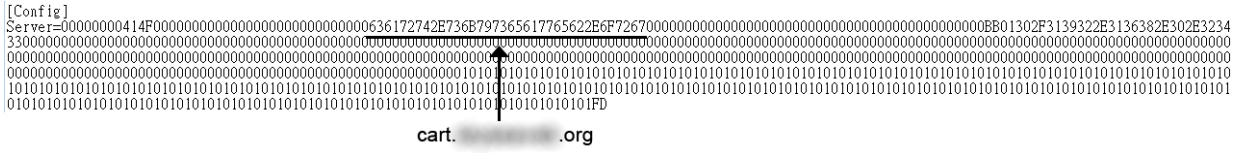


Figure 12. Extra configuration file sysconf.dll (*Hash: 4dc73b64f25c96d9bd58f9bc84aa9efa413620ed*)

The malware has a hardcoded version of itself inside used as a mutex. We have identified V1.0, V1.2, V1.3, V1.5, V1.7, and V2.0 from the samples we have collected. While comparing Serkdes versions with sample compile time, we found some conflicting details that suggests this backdoor is being used by, and shared with, different related groups.

There are two batches of V1.0: one was compiled on March 2016, while the other batch was compiled from November 2017 to June 2018. However, before the 2016 version, there were already a lot of V1.X samples observed in attacks, and may have been deployed by more than one cybercriminal group. Moreover, between the 2016 V1.0 and 2017 V1.0, there was V2.0, which was compiled in September 2017.

Another interesting finding is that some Serkdes samples call back to a subdomain under sslvps[.]top, which is believed[29] to be one of APT group DragonOK's domains. This could indicate that Serkdes is not exclusively used by only one group in East Asia, and all the groups using the backdoor actively have the region in their sights as a target.

Version	Compilation Period
1.3	July 2014
1.2	Sept 2014
1.5	Nov2014
1.7	Aug 2015 / Oct 2015
1.0	Mar 2016
2.0	Sept 2017
1.0	Nov 2017 / June 2018
1.2	Aug 2018

Table 4. Summary of the compilation periods of Serkdes' versions

Buxzop/DropNetClient

DropNetClient was first disclosed in HITCON 2015,[30] reportedly found abusing a DropBox API to perform C&C communication. Later the same year, the malware was reimplemented, with the new version now called "Buxzop." As DropNetClient, the malware embeds a DropBox secret to perform C&C communication and encodes it with a customized algorithm.

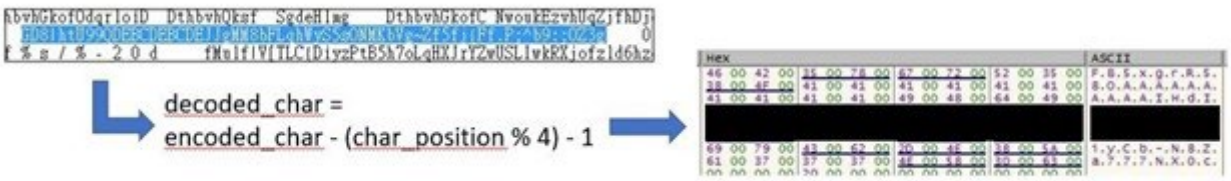


Figure 13. Buxzop string decoding

Once activated, the malware creates a folder, */1/001*, which serves to store uploaded victim information.

```
POST /1/fileops/create_folder HTTP/1.1
Authorization: Bearer FB5xgrR58OAAAAAAAAAAIH[redacted]a777NX0c
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: api.dropbox.com:443
Content-Length: 17
Cache-Control: no-cache

root=auto&path=/1
```

Figure 14. Buxzop callback to create a folder (the actual traffic is in https)

The uploaded information is in the format *<<host-name>(<IP>[MAC Address])>* such as *win-123(0.0.0.0[00-01-02-03-04-05])*. The information is encrypted with a modified version of RC4, which is basically an additional extra bit operation before and after the regular RC4 stream.

```
for i = 0 to data_length:
   data[i] = enc_flag ? (data[i] - i) : (data[i] ^ i)
   regular_rc4(data[i])
   data[i] = enc_flag ? (data[i] ^ i) : (data[i] + i)
```

Figure 15. Buxzop RC4

K4RAT

Looking at the call back traffic of K4RAT, “MP” is the campaign code embedded inside the malware configuration. “M10” contains MAC address, which is encrypted by RC4 with key “a1 a2 a3 a4”. “M11” is the IP address with same encryption procedure.

```
POST /index.asp?M00=0 HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (Compatible; MSIE 6.0;)
Host: fourk-asptree.qc.to
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: MP=novirusnodangerous; M10=gyPvXAEEnK2Q7aT3rv33ZQw%3D; M11=gz3yQwAHng%3D%3D
```

Figure 16. K4RAT callback traffic

LuckDLL

LuckDLL is a relatively new backdoor that became active after 2020. Some samples contain a program database (.pdb) string <*C:\Users\user\Desktop\luckDll\x64\Release\luckDll.pdb*> or <*C:\Users\user\Desktop\luckDll\Release\luckDll.pdb*>.

Figure 17. LuckDLL pdb string

LuckDLL embeds a public key inside the configuration before communicating with the C&C server. It then generates a random session key and initialization vector (IV) to encrypt actual traffic.

```
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 18. Public key (top) and session key (bottom)

During the initial communication, the public key encrypts the session key and IV, and shared with the C&C server. The hash-like value after parameter *api_key* is also embedded in the malware configuration, likely used to identify which private key should be used to decrypt the traffic.

Figure 19. LuckDLL traffic using the shared encrypted session key (while the actual traffic is in HTTPS)

GrubbyRAT

Based on our sensors and observation, GrubbyRAT is a rarely deployed backdoor. The threat actor only deploys it mostly to important targets, depending on the APT group's evaluation of the company, personnel, or industry's sensitivity level. The malware has a separate configuration file, which is encrypted with a simple algorithm.

The configuration file is sometimes installed under an existing application folder or general system folders, and uses a similar file name as the application component. This technique indicates that GrubbyRAT is installed manually, likely after the actor has investigated the environment and gained an administrative level of control in the system.

Every time GrubbyRAT tries to read the configuration, it first reads the encrypted file and write the decrypted configuration to a temporary folder with the prefix 123. The temp configuration then sets the file time as *C:\windows\system32\c_20000.nls* and deletes the temporary file after reading.

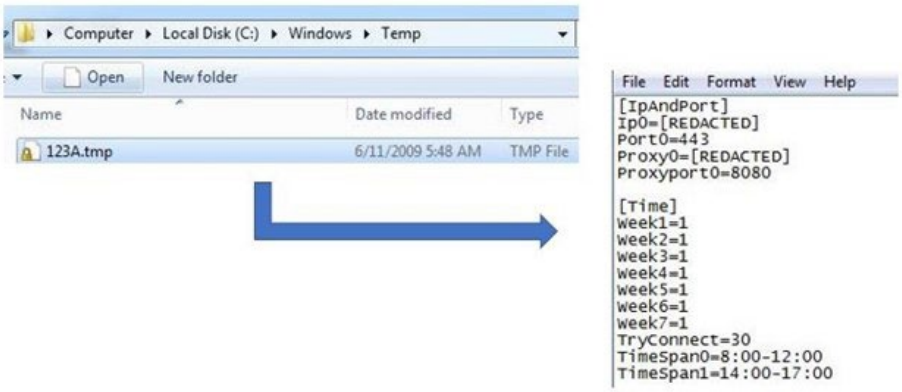


Figure 20. Decrypted GrubbyRAT configuration

The callback traffic is set in the format *<hardcoded 0x33><OSVERSIONINFOEXA result><Is Admin or not><getsockname result><machine name>*.

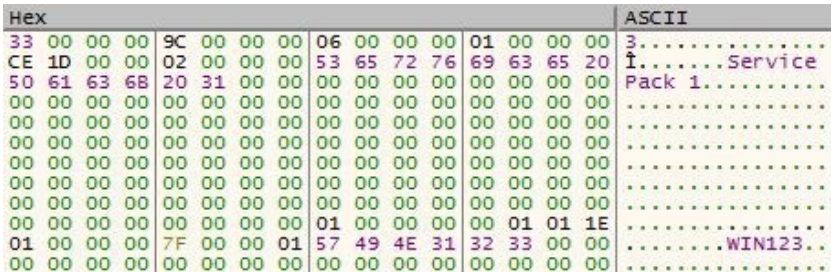


Figure 21. GrubbyRAT callback information

A random key is generated from GetTickCount and uses it to encrypt the callback information, resulting in traffic with length *0xee*, where the first *0xe* is the random key, and the remaining is the encrypted information.

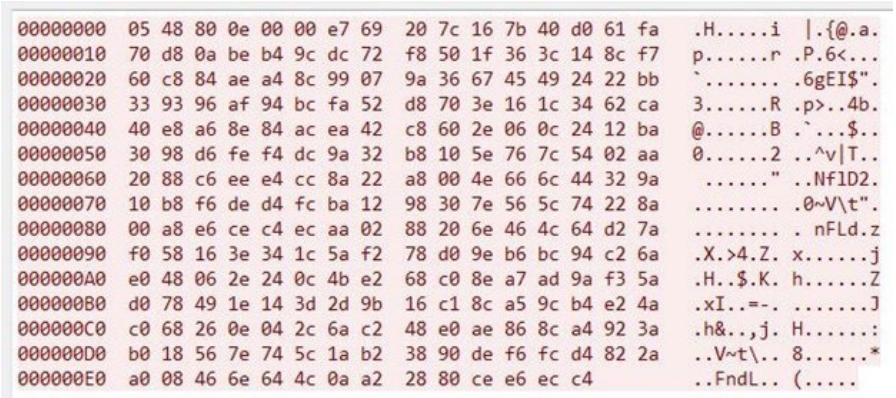


Figure 22. GrubbyRAT callback's actual traffic

Kuangdao (KD)

Kuangdao malware was disclosed on 2020[31] and as far back as 2008[32] or even earlier, as previous reports provide detailed malware analysis that can be matched. As reported, there is a special string “KD” in .pdb.

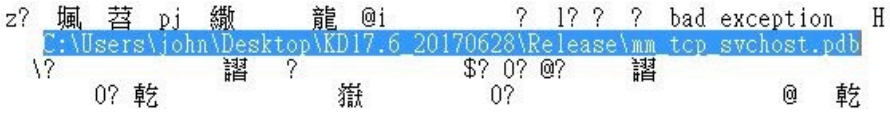


Figure 23. Kuangdao .pdb string

Interestingly, Earth Aughisky previously named the C&C domain using the real malware name. For example, in certain Roudan samples, the C&C domain is named “*roudan[.]serveftp[.]com*”. With Kuangdao, we found a special string in the C&C domain named “kuangd” or “kuangdao” (狂刀, meaning “madness blade”). This string could be observed in multiple backdoor configurations and matches the .pdb string “KD”, figuring in how actors named this malware.

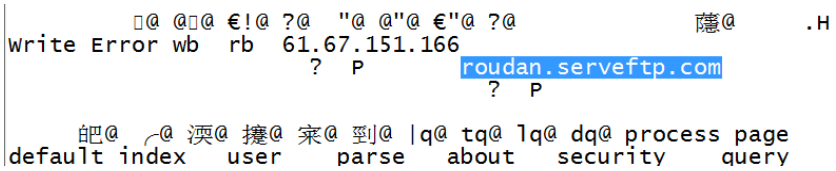


Figure 24. The Roudan C&C domain (*Hash: a9982fede417d96b0a8604b485c548ad1c5f845b*)

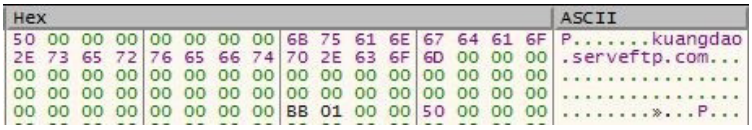


Figure 25. The Kuangdao C&C domain

Taikite (SVCMONDR)

The malware was first disclosed in a report[33] identifying CVE-2015-2545, using the dropped file name as malware name “SVCMONDR.” Given the .pdb in some samples and that the malware was mainly observed in Taiwan, we named this malware “Taikite.” The first C&C callback traffic is encoded in Base64, with detailed feedback data structure and behavior analysis.

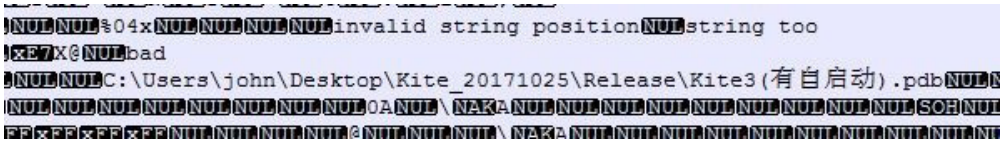


Figure 26. The Taikite .pdb string (*Hash: 44673e28e03d642e937eb5d6fed9fc6535e4b872*)

Figure 27. Taikite traffic

Specas

This malware family was categorized as Taidoor in an earlier report,[34] but is also sometimes identified as "Taleret." As other communities have used the name Taleret to identify another malware[35] and the protocol is slightly different than regular Roudan, we will use the name "Specas" to describe this malware in this report.

On the first C&C callback, it generates a random URL by template "http://%s:%d%s0%u%u" and "/%c%c%c%c%c.asp?". Looking at the GET request line, *mhbvi* is composed simply of five random characters, with one hardcoded "0" after a question mark. For the remaining numbers on the line "100287525376", GetTickCount "287525376" is the derived result. "100" before "287525376" is calculated as (*287525376 & 0X1FF*) + *100*, which is likely used as the checksum in the traffic.

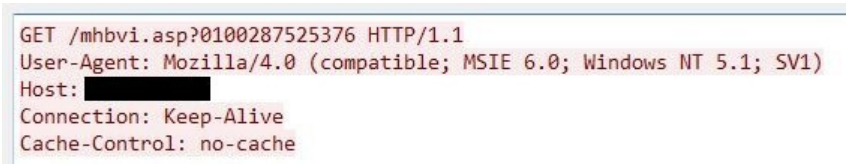


Figure 28. Specas traffic

The malware also drops a log file at [current module name].xxt, which contains the execution history.

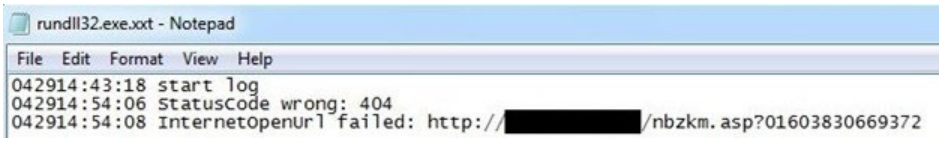


Figure 29. Specas .xxt log

Based on analysis, Specas malware is also capable of reading extra proxy settings from *%systemroot%\system32\sprxx.dll*, with the format being *<IP>:<Port>*.

```
mov     [esp+334h+nSize], 104h ; nSize
push    eax             ; lpDst
push    offset Src      ; "%systemroot%\\system32\\sprxx.dll"
mov     dword ptr [esi+10h], 2000h
mov     [esi+60h], ebx
call    ds:ExpandEnvironmentStringsA
lea     eax, [ebp+Dst]
push    offset aR       ; "r"
push    eax             ; FileName
call    ds:fopen
```

Figure 30. Specas sprxx.dll proxy setting

SiyBot

SiyBot is a backdoor we observed to be deployed less and only in few instances of an attack. Similar to Buxzop, SiyBot abuses public services to perform C&C communication. The malware mainly leverages Gubb and 30 Boxes in its earlier version.

```
.data:10022488  00000028  C  %s/list/create.xml?name=%s%d&api_key=%s
.data:10022530  00000015  C  %s/list/delete?id=%s
.data:100224CC  0000001F  C  %s/list/get_all.xml?api_key=%s
.data:10022450  00000027  C  %s/list_comment/create.xml?id=%s&note=
.data:10022424  00000029  C  %s/list_comment/create.xml?id=%s&note=%s
.data:1002256C  0000002C  C  %s/list_comment/delete.xml?api_key=%s&id=%s
.data:100225B0  0000002D  C  %s/list_comment/get_all.xml?api_key=%s&id=%s
.data:10022124  0000004C  C  %sevents.AddByElements&apiKey=%s&authorizedUserToken=%s&summary=%d%s&notes=
.data:100220CC  00000058  C  %sevents.AddByElements&apiKey=%s&authorizedUserToken=%s&summary=%d%s&notes=
.data:100221A8  0000003C  C  %sevents.Delete&apiKey=%s&authorizedUserToken=%s&eventId=%s
.data:10022294  0000003D  C  %sevents.Get&apiKey=%s&authorizedUserToken=%s&start=%d-%d-00
.data:1002222C  0000003D  C  %sevents.TagSearch&apiKey=%s&authorizedUserToken=%s&tag=%s%c
.data:100223C0  0000002E  C  %suser.Authorize&apiKey=%s&applicationName=%s
```

Figure 31. Service API

Like most other malware that abuse public web service, the necessary credential or token can be found in the malware configuration.

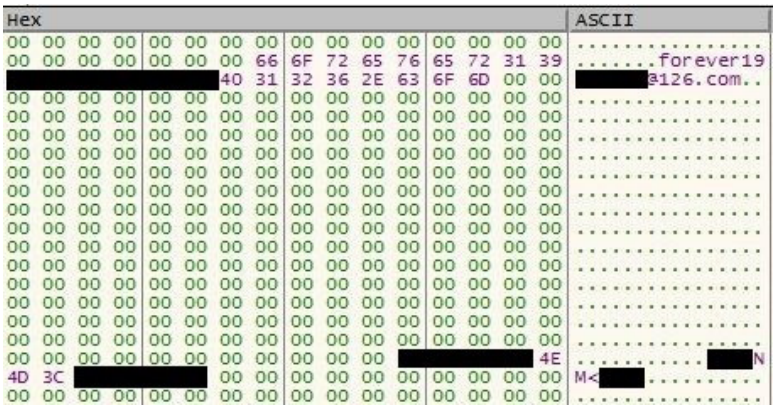


Figure 32. Embedded 30 Boxes credential in the malware

SiyBot supports few basic functions such as chconf, run, download run, and download.

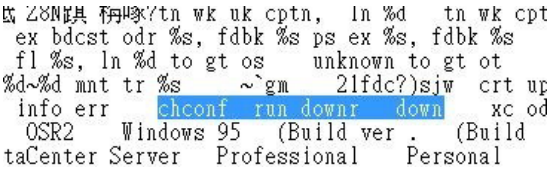


Figure 33. Backdoor command

TWTRAT

TWTRAT is an old backdoor compiled around 2010 based on analysis of the malware binary, first observed as abusing Twitter direct messages to perform C&C communication. TWTRAT only supports some basic functions, specifically “down,” “run,” and “downr”; the commands are very similar to SiyBot. Given that there are new backdoors abusing different public services since the year of compilation and that we have not observed activities of TWTRAT afterward, this backdoor was only used for a limited period.

Figure 34. TWTRAT invokes direct_message

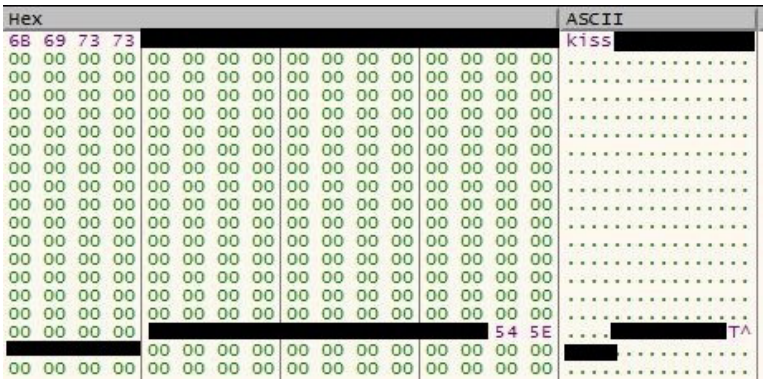


Figure 35. Twitter account embedded in the malware configuration

GOORAT

GOORAT is a possible precedent to Taleret, observed active around 2009 to 2010 based on the samples submitted in repositories and analysis of the malware binary. Like Taleret, the malware searches for content between “XXXXX”, but the content inside is a command rather than a configuration. Most samples were configured to retrieve data from Google groups, while the rest of the samples we observed would search for data from different blogs. Eventually, it appears that the group has apparently abandoned this branch and turned to using Taleret instead.

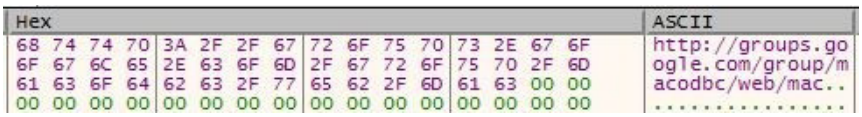


Figure 36. Embedded site in GOORAT

ASRWEC Downloader

ASRWEC is a downloader capable of searching for the actual payload on blogs or other repositories that was first disclosed in 2012[36] and subsequently reported on. This downloader first locates the actual payload between a special marker, “yxyyyxyy”, with actual decryption procedures documented in detail. The payload we observed includes both Roudan and SiyBot.

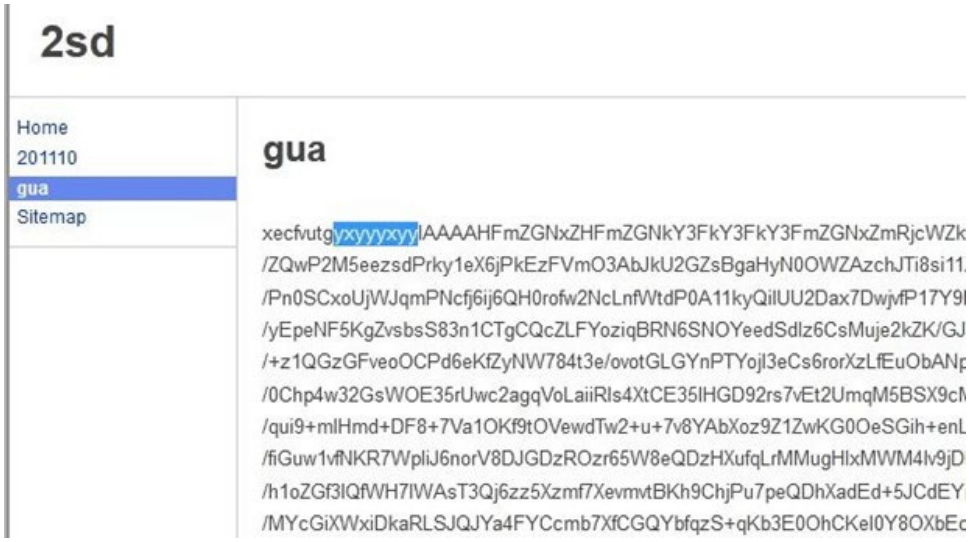


Figure 37. ASRWEC payload found from the blog (the characters after “yxyyyxyy”)

Comeon Downloader

Similar to ASRWEC, Comeon is another type of downloader from Earth Aughisky capable of searching for payload between *****. We call this Comeon because of the export function name we observed during analysis. Aside from using a different maker, most Comeon payload were hosted on private servers rather than a public blog such as *210[.]240[.]26[.]2/java.txt* or *TheoreticalModel[.]onmypc[.]us/u.txt*.

The actual payload could be decrypted by:

1. Skipping the first character
2. Decoding using Base64
3. Decrypting with RC4, using key “A1 A2 A3 A4 A5”

Based on our observations of samples, the payload of Comeon downloader is Roudan, such as the one hosted on *kaiwanxiao[.]pixnet[.]net/blog/post/366093431*.

Figure 38. Comeon downloader payload on blog

The malware is capable of dropping the log file at *%temp%\iod.zp*, with the content likely designed for debugging purposes.

```
04/20/22 14:44:41 - lpURL[3] = 0, dwBase64_len = 0
04/20/22 14:44:41 - lpURL[2] = 0, dwBase64_len = 0
04/20/22 14:44:41 - lpURL[1] = 0, dwBase64_len = 0
04/20/22 14:44:41 - lpURL[0] = 64, dwBase64_len = 100
04/20/22 14:44:41 - DecodeURL BaseLen 100, i= -1
04/20/22 14:44:41 - The Decode URL http://210.240.26.2/java.txt  http://Th
```

Figure 39. The iod.zp log file

Illitat Downloader

Illitat was first disclosed on 2012[37] and again observed in 2015.[38] This downloader calls back to *fc.asp* using the local environment information it collects such as the machine name and IP address, and then calls *dw.html* to download the actual payload. Based on the reports, all the samples' payloads are Roudan.

```
jnz     loc_4015DA
push    offset Name     ; "efcc ilitat"
push    eax             ; bInitialOwner
push    eax             ; lpMutexAttributes
call    ds:CreateMutexA
```

Figure 40. Special mutex in some samples used to name this malware

Attribution

While some of the listed malware families here were previously documented and attributed to Earth Aughisky, we list the other malware families we analyzed (that have yet to be reported) in this section to complete the APT group's technical profile. We also identify and connect a number of these unreported malware families based on analysis of the sourced samples over the years, such as similarities in codes, domains, and naming conventions.

Connections Between Families

We describe the links between the different malware and how our observations have led us to tie them together as being employed by Earth Aughisky.

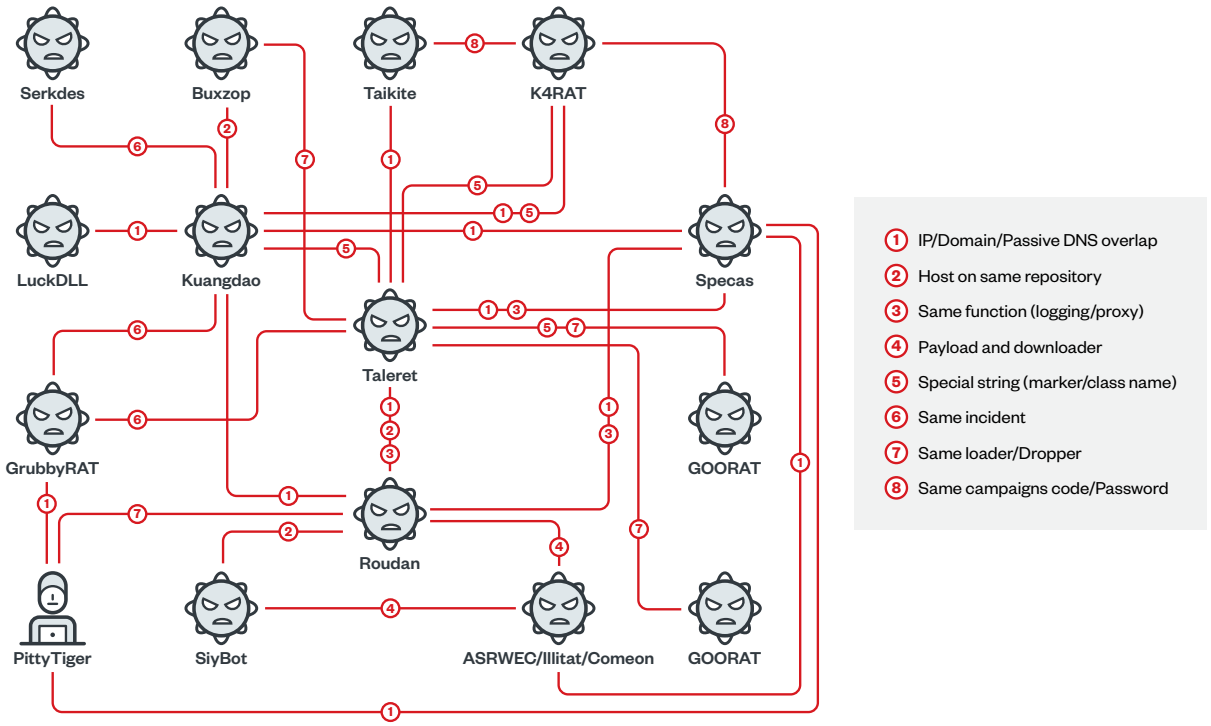


Figure 41. Connections between the different families

Roudan, ASRWEC, Comeon, and Illitat

Different sources have reported that ASRWEC, Comeon, and Illitat download Roudan malware in different ways.

Roudan, Taleret, and Taikite

Taleret has been suspected or identified to be related to Earth Aughisky for years, while Taikite (Svcmondr) was not previously attributed. Among these families, we could observe some C&C overlaps.

IP addresses	Taleret URLs	Roudan hashes	Taikite hashes	Months observed
61[.]216[.]128[.]129	mini2016blog[.]wordpress[.]com/2016/11/03/mini2016/ mini2016[.]pixnet[.]net/blog/post/8382313	de7a4946cd2e0d60bd0a1e1c758b6753965f7fb9		• July 2018
211[.]22[.]7[.]237	saism2010[.]wordpress[.]com/2010/12/29/februa/	a28dbea98d424a2bb5b645f20773d6c4c6dce393		• Jan 2012 • April 2012
193[.]170[.]111[.]210	saism2010[.]wordpress[.]com/2011/01/19/pdvd/	d329936d870afc888e58b843823d7136de00ac6e		• Jan 2010 • March 2011
121[.]241[.]81[.]116	tasklili[.]pixnet[.]net/blog/post/128497913		a01be1ff3ec69cad31b1880cb5e304d920f3ccd4	

Table 5. Overlapping C&Cs of Taleret, Roudan, and Taikite

In some earlier versions of Roudan, it adopts the same logging mechanism as Taleret.

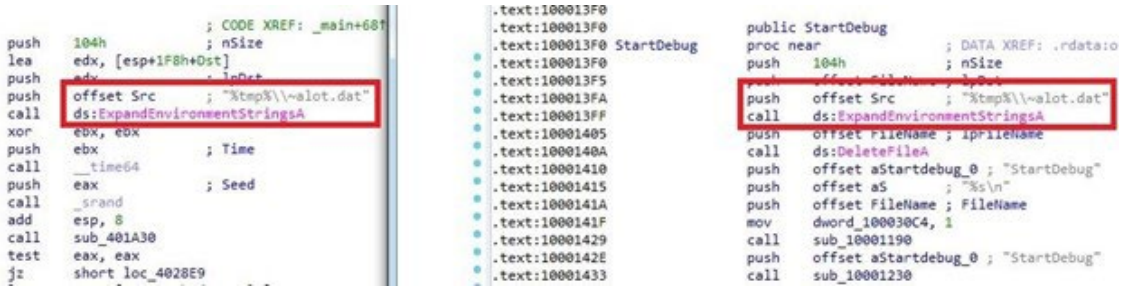


Figure 42. Taleret's special log file (left) compared with Roudan's earlier version (right)

We can also see the same blog hosts both a Taleret configuration and Roudan payload.

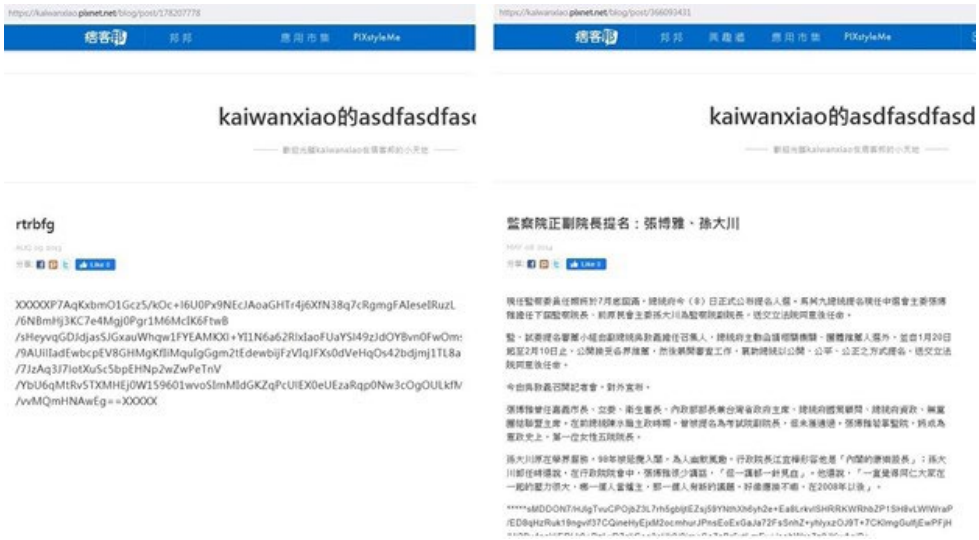


Figure 43. Taleret configuration (left, *Hash: 13d0961daf1166d95795f2c7e2ee88f32037ea1b*) and Comeon payload (Roudan *hash: 3c55249b6512e1b1f7e721c2fd9faa5d30e56fe6*, right) on the same blog

Roudan, Specas, Kuangdao, and Buxzop

The Cybersecurity and Infrastructure Security Agency (CISA) has attributed Kuangdao to Earth Aughisky.[39] DropNetClient, which shares similarities with Buxzop, has also been attributed to the group. We observed C&C, hosting domain, or IP address overlaps among Roudan, Specas, and Kuangdao routines.

IP / Domain	Roudan / ASRWEC / Comeon hashes	Specas hashes	Kuangdao hashes	Months observed
abianshabi[.]myddns[.]com	006cc46b85b791bc26a865ccc6950993901cd597 4a9f99627ef76f8a382f11513a2853cddf6cd31d	ed53ed2c554055986b2257774f6aa00ccdd52bba		• Jan 2011 • Mar 2012
yahoofacebook[.]345[.]pl	0cbb05ee07c2fca207e4835496ac6fe0e319e4e0	3be0ad0bf20d0b6d160a44676146e9ae789c6933		• May 2010 • Nov 2010
118[.]175[.]7[.]74	8b566291d127c11213f0d378b5cf3292d9df2031	a4e52877d5666f265775f50b6d6993ecbbab70bd 557e177295ebd1c6597eba23b5234f1943161484		• May 2012 • July 2012 • Sept 2012

IP / Domain	Roudan / ASRWEC / Comeon hashes	Specas hashes	Kuangdao hashes	Months observed
78[.]39[.]236[.]6	9f9206046652ac3d33b126b91779065c61d5571e e6ae1562f2222758de4d9adb7509bb8884a7e18d		00425add8d8b24fb4c15af484a8fcc7db22ffa55	• June 2011 • Aug 2011
www[.]google[.]dynssl[.]com	da581523a0b203e3e5e5f072cf82f6883afea35e		2e948663610d8224a9bf5216b686d6f9eb3d1981	• Nov 2013 • Jan 2014
www[.]ourfriends[.]sexxxy[.]biz		c135eefb021ffecfa991c523e41c43ad87d769fc	27d61d9e379c5fc4fb09e57f50fef24b30d06acc	• Nov 2015 • Aug 2016

Table 6. Overlapping C&Cs and hashes of Roudan/ASRWEC/Comeon, Specas, and Kuangdao

From the middle towards the end of 2018, we found IP address 103[.]110[.]80[.]48 used to host both Buxzop and Kuangdao simultaneously.

URL	Family	Hash
103[.]110[.]80[.]48/123.dll	Kuangdao	663fb74f33dde51b6ca3c0faf5bfd5b1431a43b2b1650e83f14ba11a35a2c326
103[.]110[.]80[.]48/task.zip	Kuangdao	4d55d8e4354501207affb7aaa2d79108e6596fe6c3d753c32aa22e075853ba6e c11a9d7c06130fc05430bcca32f7c3e4621e838efb888ebddc52985f5cd17d0e
103[.]110[.]80[.]48/1102/x64-1102.dll	Buxzop	73846ec3f92b723ee6b5648ca957b5d9a518974d9358569ab6f23bf611938659
103[.]110[.]80[.]48/1102/x86-1102.dll	Buxzop	93e1c51d0c0c01673187d40f4b41a8fd461f4bb46572c2c6dee5077d9dff4a97
103[.]110[.]80[.]48/x64.dll	Buxzop	8b4e42a2abbcd47f3fd8e9b75913d05633efb610d646565ef43e3f9daaabaeaf
103[.]110[.]80[.]48/x86.dll	Buxzop	4e6c21ccab81af36e58da66347a301240a005044ca2bd7521a79f56373356ed2

Table 7. Buxzop's and Kuangdao's host overlap

Taleret, Specas, and Taikite

We observed overlaps with the hashes and IP addresses among Taleret, Specas, and Taikite malware families.

IP	Taleret	Specas	Taikite	Time
202[.]54[.]49[.]5	tasklili[.]pixnet[.]net/blog/post/128966213	5c9050d6cb94e64ccb4f4a542b28201d81d09855		• Dec 2015 • April 2016
202[.]55[.]92[.]56		c135eefb021ffecfa991c523e41c43ad87d769fc	a43ebe4e931eaf5c801635d9091f2fb78c8bd26d	• May 2016 • Aug 2016
121[.]241[.]81[.]116	tasklili[.]pixnet[.]net/blog/post/128497913		a01be1ff3ec69cad31b1880cb5e304d920f3ccd4	• June 2016

Table 8. Overlapping C&Cs and hashes of Taleret, Specas, and Taikite

Kuangdao, K4RAT, and Taleret

We observed a passive domain name system (DNS) overlap with Kuangdao and K4RAT in 2013.

Passive DNS	Kuangdao	K4RAT	Time
190[.]143[.]87[.]148	73bade5f565bf5ea157772a93d4e2378540260e1 5e81a8fdef0baabfb7f65e46625bbe6d1f79328f fsc-kd[.]ns01[.]info moeas[.]agent[.]tw	34d0b9b09d807fed44ed3467cbb85c6687157c22 fourk-asptree[.]qc[.]to	• July 2013 • Nov 2013

Table 9. DNS overlap of Kuangdao and K4RAT

We also observed Kuangdao, K4RAT, and Taleret sharing a special window class name, “wxxxd.”

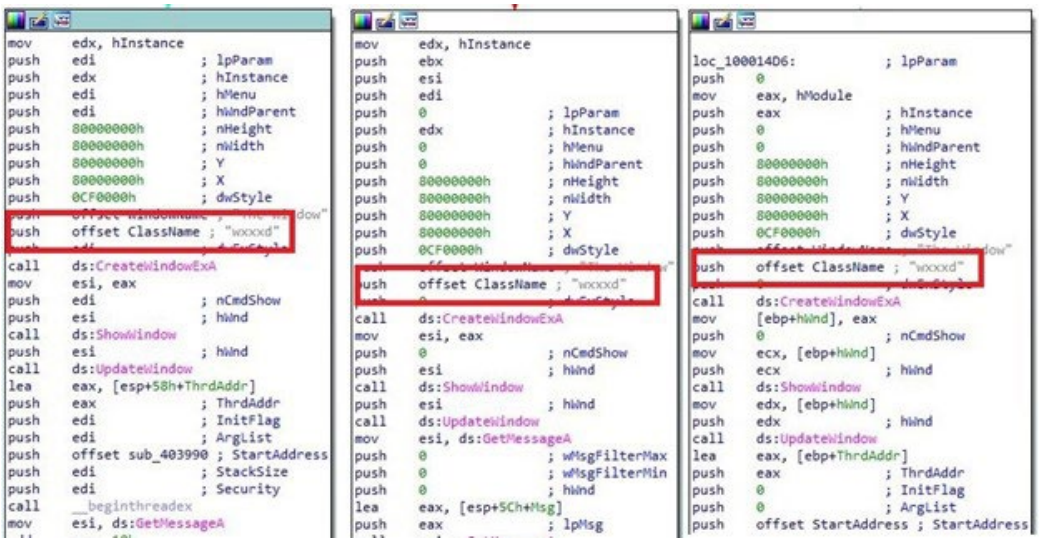


Figure 44. The wxxxd class name of K4RAT (left, *hash: 26b8faaf301c2b6bc180f179d0d68f3f0fd419ab*), Taleret (middle, *hash: 775eac7787a351fed43a0150484b9870ecbc4ec9*), and Kuangdao (right, *hash: f3987d5629dfb61c518528cb8314e60f1bb2dd5c*)

Roudan, Specas, and Taleret

We found a lot of Specas samples that would load a proxy setting from a special file *%systemroot%\\system32\\sprxx.dll*. The same behavior could also be found in some Roudan or Taleret samples.

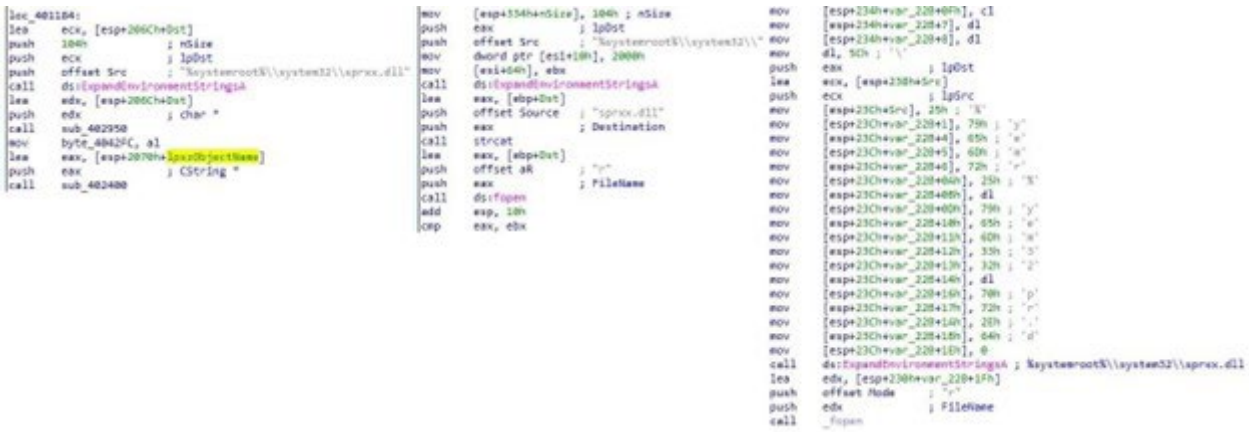


Figure 45. The sprxx.dll proxy setting of Roudan (left, *hash: 0a5895e0c360a25d5abb7fbd7959da044c2c6c93*), Specas (middle, *hash: 341cbeb81e6cba15442ee5f9544b7d7593686a2e*), and Taleret (right, *hash: 789614db37fb2302957028fd6c30cea492636f3e*)

Specas, Taikite, and K4RAT

Some of Earth Aughisky's malware have special embedded codes inside the configurations for different purposes, such as password[40] or campaign codes. Upon analysis, we also observed the same codes being used across these three families.

Code	Specas	Taikite	K4RAT
cherry	fbedc622d5b611714468 e98ca1b2e07c1229c66d	a4b8d9d166c9aa94e139 dbc124fce0c6cc6dbd9a bb580239c3f5f2bd57c18 90e94e46c0ea5a2565b	967c89d78eed2f519744 6414342a79fe5a76a868 a85a2b07588701ba6059 a638b664905371ac3202
fuck@123	ec6fcf1435b13d9b4037b 1839bdbaaf13b65244b	66f47d13455a34043beb b83fe99a700e10ddd4e7	
itsmy / itsmy!	264e962f51535b1ec79c 375947f142ce782cab89		c1ae8ab849624c16597f a7c5bd4396dad01390e5

Table 10. Hashes of the embedded codes found in configurations of Specas, Taikite, and K4RAT

Kuangdao and Serkdes

Previous reports have attributed Serkdes to Earth Aughisky in 2018.[41, 42] Some samples also indicated that these two families were found in the same incident.

Hash	Family	Time	Proxy setting
c377923108a2bdae1c06819eea9db49ea7883537a31d92a904405f6d813ab4b6	Serkdes	Nov 2014	[REDACTED].15.167
e5f3c3053da3707274b8e958a4b498f70f8a92e1beae74da5ea49174e255f898	Kuangdao	July 2014	

Table 11. Overlapping incidents of Serkdes and Kuangdao

Kuangdao and LuckDLL

We found different domains under lily[.]onmypc[.]net set as the C&C servers for Kuangdao and LuckDLL.

Domain	Kuangdao	LuckDLL
lily[.]onmypc[.]net	7c5841f19740350d36a0644205dcb558 003a58739d420d344e2a78221663fac4 www[.]lily[.]onmypc[.]net	51f15ca72ff1afa8b8615d426dc634d6e 853de82a3b127c95f3473efdb3094a9 ftp[.]lily[.]onmypc[.]net

Table 12. Same domain as C&C servers for Kuangdao and LuckDLL

Kuangdao, Taleret, and GrubbyRAT

During an investigation of an incident, we observed an organization being attacked by GrubbyRAT, Kuangdao, and Taleret continuously.

Months observed	Malware observed
May 2013	Specas
August 2013	Kuangdao
June 2014	Taleret
December 2014	GrubbyRAT
January 2015	GrubbyRAT
January 2015	GrubbyRAT
March 2015	GrubbyRAT
September 2015	Kuangdao
November 2015	Kuangdao

Table 13. Recorded incidents attacking one organization from 2013 to 2015

Moreover, we found some GrubbyRAT and PittyTiger samples sharing the same domain in their configurations, such as *davy[.]myddns[.]com* or *yourdomainnames[.]myddns[.]com*. Unfortunately, due to the sensitivities surrounding the incidents, we will not disclose more details on this but will continue monitoring these threats.

Taleret and GOORAT

Both malware use "XXXXX" as a marker to locate the information they need. In addition, the same dropper was used to deliver both GOORAT and Taleret, which functions to decrypt the payload from the resource and execute it.

```
mov     esi, ds:ExpandEnvironmentStringsA
push    104h            ; nSize
push    eax             ; lpDst
push    offset Src      ; "xxxxxxxxxxxx"
call    esi ; ExpandEnvironmentStringsA
lea     ecx, [esp+61Ch+FileName]
push    104h            ; nSize
push    ecx             ; lpDst
push    offset aCWindowsSystem ; "c:\\windows\\system32\\Google.dll"
call    esi ; ExpandEnvironmentStringsA
lea     edx, [esp+61Ch+CmdLine]
push    208h            ; nSize
push    edx             ; lpDst
push    offset a1111111111 ; "1111111111"
call    esi ; ExpandEnvironmentStringsA
lea     eax, [esp+61Ch+var_208]
push    208h            ; nSize
push    eax             ; lpDst
push    offset aRundll32CWindo ; "rundll32 c:\\windows\\system32\\Google."...
call    esi ; ExpandEnvironmentStringsA
lea     ecx, [esp+61Ch+Dst]
push    ecx             ; lpFileName
push    offset Type     ; "RT_RCDATA"
push    65h ; 'e'       ; lpName
push    0               ; hModule
call    sub_4010D0
mov     esi, ds:WinExec
```

```
mov     esi, ds:ExpandEnvironmentStringsA
push    104h            ; nSize
push    eax             ; lpDst
push    offset Src      ; "xxxxxxxxxxxx"
call    esi ; ExpandEnvironmentStringsA
lea     ecx, [esp+61Ch+FileName]
push    104h            ; nSize
push    ecx             ; lpDst
push    offset aCDocume1Alluse ; "c:\\docume~1\\alluse~1\\applic~1\\regsr"...
call    esi ; ExpandEnvironmentStringsA
lea     edx, [esp+61Ch+CmdLine]
push    208h            ; nSize
push    edx             ; lpDst
push    offset a1111111111 ; "1111111111"
call    esi ; ExpandEnvironmentStringsA
lea     eax, [esp+61Ch+var_208]
push    208h            ; nSize
push    eax             ; lpDst
push    offset aRundll32CDocum ; "rundll32 c:\\docume~1\\alluse~1\\applic"...
call    esi ; ExpandEnvironmentStringsA
lea     ecx, [esp+61Ch+Dst]
push    ecx             ; lpFileName
push    offset Type     ; "RT_RCDATA"
push    65h ; 'e'       ; lpName
push    0               ; hModule
call    sub_4010D0
mov     esi, ds:WinExec
```

Figure 46. GOORAT dropper (left, *hash: 1a30a00b394aa4443f44d7645b67d22c82875ad7*) and Taleret dropper (right, *hash: c6f2d78b5f89d522306f74426e4b0d8e00841c46*)

Roudan and SiyBot

We found the same site used to host both Roudan and SiyBot.

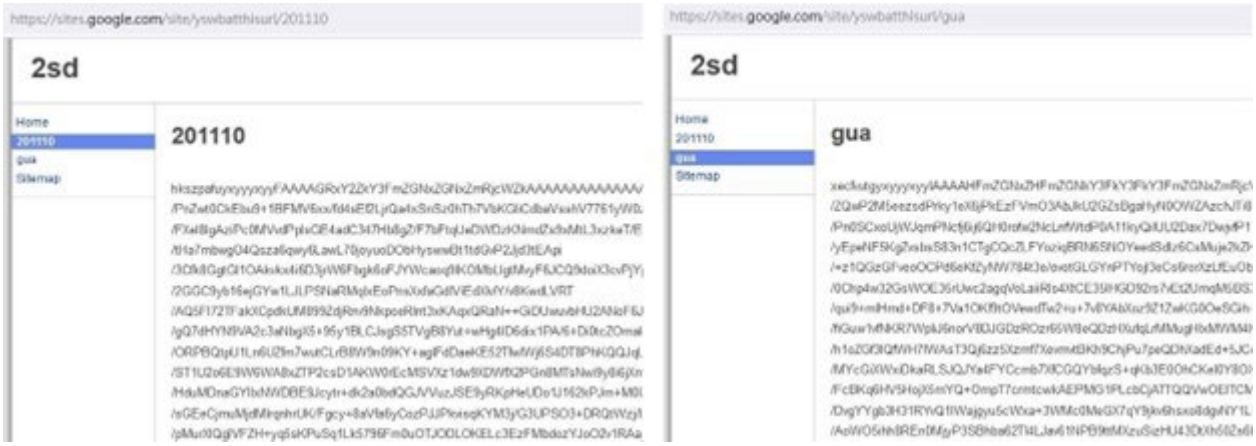


Figure 47. ASRWEC downloader payload on same repository, Roudan (left) and SiyBot (right)

Taleret and TWTRAT

We observed the same dropper being used to deliver both TWTRAT and Taleret. In 2011, two samples of a special dropper were submitted to a public repository, *c67db6af5873a558145452341e34de74eda78cec7ef33921d2885038a1e6aaaa* and *a1054e8b5336ead42c1a43947bbd50a896f5fe551c5994aa7414e44c14339e29*. Analysis of the samples revealed that one of them dropped TWTRAT while the other dropped Taleret. Since there is no evidence that either of the droppers is leveraged by more groups, we believe TWTRAT is also one of Earth Aughisky's malware.

Taleret and Buxzop

Earth Aughisky has been using a special loader for several years posing as one of the different system DLLs such as *version.dll* or *cryptbase.dll*. Once activated, it loads an encrypted payload from a separate file and decrypts it with RC4. Based on the samples we collected, most of the payloads are located at one of the five files: *[Same Folder]\master_patch.dat, master_update.dat, crypt_base.dat*, *Extensions.xml*, or *ipatch.dat*.

After loading the payload into the memory, it searches for "MyThread" or "MyBegin" export function and transfers the control to the in-memory executable. Based on the samples we collected, most payloads are Taleret and a few instances had Buxzop.

Links to PittyTiger

Airbus Cybersecurity published a report[43] on the APT group PittyTiger[44] disclosing a detailed analysis of the threat actor, including Rerol malware (MD5: *b6380439ff9ed0c6d45759da0f3b05b8*). But researchers from Mandiant also connected Earth Aughisky to PittyTiger via Roudan.[45]

According to the disclosure, PittyTiger has been active since 2011 and attacked targets in Europe. Rerol[46] was used for initial intrusion and was reportedly capable of downloading a second payload from the controller. The dropper of Rerol mentioned is a specially crafted dropper widely observed in other Earth Aughisky attacks. Based on analysis of the sample of the dropper we collected, majority of the payloads were the different Earth Aughisky malware, but a few of them also noticeably dropped PittyTiger artifacts (such as Rerol, trojan MMRAT,[47] and a decoy document used to deceive victims).

MMRAT	Rerol	Earth Aughisky
May 2014 June 2014 Jul 2014 Aug 2014	April 2014	April 2010 June 2010 March 2011 June 2011 Aug 2011 March 2012 Aug 2012 Sept 2012 Jan 2013 March 2013 April 2013 May 2013 June 2013 July 2013 Aug 2013 Sept 2013 Jan 2014 May 2014 June 2014 July 2014 Dec 2014 April 2015 Nov 2015 March 2017

Table 14. Months of documented PittyTiger and Earth Aughisky incidents wherein payloads were dropped by the same dropper

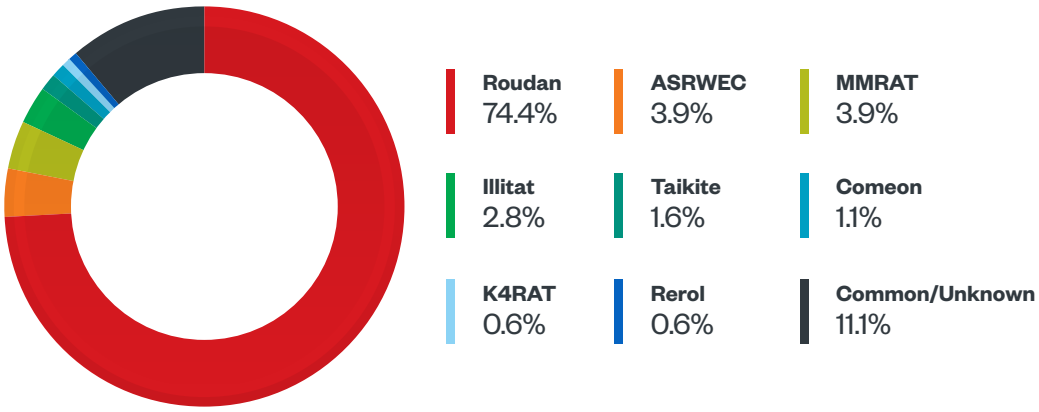


Figure 48. PittyTiger payload distribution

Figure 49. Decoy document compiled by PittyTiger actor known as "Toot"[48]

In 2014, we found a few Specas samples calling back to subdomains under *avstore[.]com[.]tw, seed01[.]com[.]tw*, and *lightening[.]com[.]tw*, all believed to be domains belonging to PittyTiger.

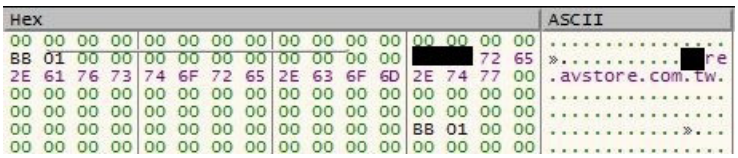


Figure 50. "avstore" Specas sample (*Hash: 90ca82604d29a87da95f68aaca7d2b0748b1504b*)

Based on these observations, we think that Earth Aughisky and PittyTiger are closely related to each other.

Origins

Law enforcement agencies[49] and other security researchers believe Earth Aughisky and Taidoor malware originated and operates from China.[50, 51, 52] Analyzing samples of the malware have consistently contained Simplified Chinese and Pinyin among the group's artifacts.

Figure 51. Roudan builder with Simplified Chinese user interface

During incident response (IR) investigations, we observed different IP addresses get involved in Earth Aughisky's activities from the logs. For those we confirmed not using proxies or virtual private networks (VPNs), most of them were tracked as originating and located in Fuzhou, Fujian. Considering some connections made between Earth Aughisky and PittyTiger, these observations also match the Airbus Cybersecurity PittyTiger report described.[53]

Updates and Changes

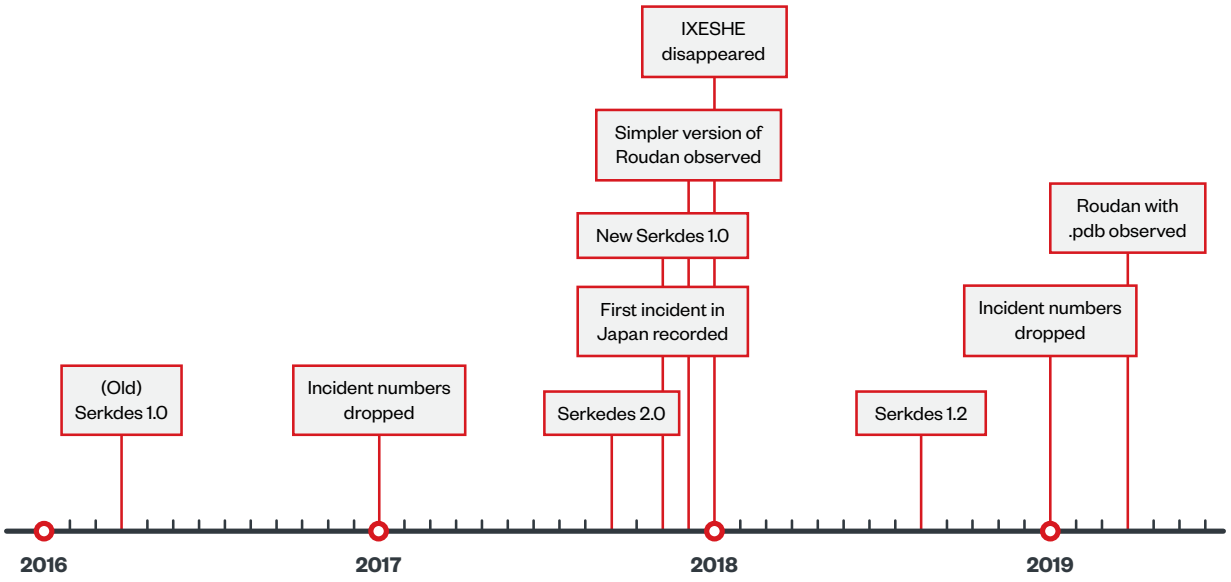


Figure 52. Special events timeline between 2017 to 2019

Earth Aughisky has been active for a long time. However, our continuous tracking of the group showed something interesting that has been happening since 2017. In this section, we describe our observations, specifically on potential changes in Earth Aughisky as an organization.

Level of Activity

The first landscape change is the noticeable drop of attack incidents in Taiwan. In a nutshell, Earth Aughisky was active before 2017, but activities significantly dropped during the said year and dropped further after 2019. Meanwhile, other APT groups previously documented as targeting Taiwan also had notable shifts in targets and activities in Japan and Southeast Asia, pointing to a likelihood of related internal changes in organization and objectives.[54, 55, 56, 57, 58, 59]

Figure 53. Trend of incidents observed (top) and trend of sample compilation time (bottom)

Group Overlap

For the incidents in Japan wherein Serkdes malware was observed and identified, it seems that there are interesting overlaps between different groups. Certain Upheart samples (Hash: a7b7a6a9b4aafe2ac1f792c901a21906df3c09adea6549446da1ed72f90b9194) we identified, which was initially reported as belonging to DragonOK based on a report by Macnica,[60] were submitted to a public repository by the same source around the same time a Serkdes sample (Hash: 5888b026ab7df42ed32d53038e9b8541cf272f0010385694e2ba28e0454f14c2) was also uploaded. This suggests a possibility that both samples are employed in an attack. In addition, as mentioned in Serkdes section, some Serkdes samples call back to a subdomain under *sslvps[.]top*, which is also believed to be one of DragonOK's domains.

The NTT report presented another overlap with PoshC2, but the evidence was not strong enough to make the connection. We have never seen Earth Aughisky utilize PoshC2 before. While it might be a coincidence that they adopted a new open-source tool, other researchers reported that PoshC2 was adopted[61] by DragonOK and BlackTech[62] for activities in Japan around the same time. We continue to monitor and study these instances for better threat intelligence and knowledge on these connections.

Special Roudan Sample

NTT pointed out that they acquired a Roudan sample that seemingly contained only two functions, which is less than the older samples of the malware. Based on the samples we collected, Roudan seems to have been developed into a simpler version between 2016 and 2017, potentially indicating a new malware developer team operating within the group.

In some samples compiled in 2019, the .pdb string *C:\Users\user\Desktop\MsgHandleDll0304\Release\MsgHandleDll.pdb* was observed in some samples, which is something that we have not observed in the last decade.

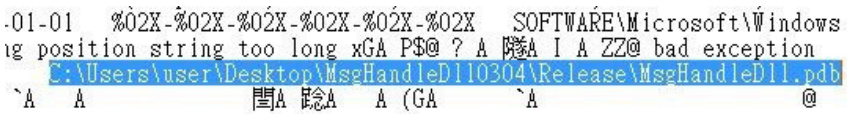


Figure 54. Roudan .pdb string (*Hash: 071e0693b5b6219e6cf02621e02c09f36ddee5e3*)

Conclusion

Earth Aughisky has demonstrated a long history in cyberespionage. Since its first disclosure, there have been continuous reports about its activities for over a decade. Tracking this group and their longevity in cyber espionage have given security teams and analysts time to gather information and technical data on their knowledge and skill development as a group, as well as look into the group's relations and potential links to other groups and activities.

Examples of these are GOORAT and TWTRAT's short period of use. Studying a small number of samples of TWTRAT backdoor and not seeing this malware family used after 2010 suggests that the group's exploration of their technical skills had to yet reach maturity. The coding was too complex and contained unnecessary data that was not required to abuse the services it needed, which was a strong indicator that the operation and the developers' skills for malware implementation were still in development.

In GOORAT's case, the subsequent choice of using Taleret over this earlier backdoor reduced the resources needed to operate the malware: Taleret hosts the malware configuration on web services, while GOORAT hosts the command itself. While not an exhaustive list of their development, and even as newer and more developed security technologies (such as behavior analysis and monitoring) can detect and block these threats especially in public services, Earth Aughisky choosing Taleret allowed the group to:

- Change the C&C server being used faster and easier.
- Avoid in-depth analysis from security teams and researchers.
- Minimize the coding complexity needed in communicating by web service.

Moreover, while relatively inactive compared to a number of APT groups, studying links such as this group's potential connection to PittyTiger allow security practitioners and researchers a general understanding of APT groups via closer analyses of previous deployments. These groups can be connected to actual organizations or considered an extension of certain government agencies, and having the background of these connections allow security teams and (potential) targets to make ample preparations in dealing with attacks from such threat actors working in tandem or individually.

In addition, the changes from and in the activities of the group can be matched with real-world organizational changes such as political shifts and transitions. For Earth Aughisky, changes in routines, frequency, or level of activity, and overlaps in the organization can imply:

- A change in their focus or objectives, making their target countries, regions, industries, and/or companies different.
- A change in their tool arsenal, which means they might begin using malware previously documented and attributed to other groups and vice versa.
- A change in their current malware and infrastructure.

Groups such as Earth Aughisky have plenty of resources to develop varied custom tools for their operations and will likely take advantage of their long cybercriminal and cyberespionage history. After a decade, this level of consistency and even this observed break from activity can be looked as either a period of respite from attacks for victims or a period for a higher level of vigilance for when the threat actor decides to become active again.

Indicators of Compromise (IOCs)

Find the full list of the IOCs related to Earth Aughisky in the Reference section.[63]

MITRE ATT&CK

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
T1598 Phishing for Information	**T1583** Acquire Infrastructure	**T1566** Phishing	**T1059** Command and Scripting Interpreter	**T1546** Event Triggered Execution	**T1546** Event Triggered Execution	**T1140** Deobfuscate/ Decode Files or Information
	T1586 Compromise Accounts	**T1078** Valid Accounts	**T1203** Exploitation for Client Execution	**T1574** Hijack Execution Flow	**T1574** Hijack Execution Flow	**T1480** Execution Guardrails
	T1584 Compromise Infrastructure		**T1129** Shared Modules	**T1205** Traffic Signaling	**T1055** Process Injection	**T1211** Exploitation for Defense Evasion
	T1587 Develop Capabilities		**T1072** Software Deployment Tools	**T1078** Valid Accounts	**T1078** Valid Accounts	**T1564** Hide Artifacts
	T1588 Obtain Capabilities		**T1569** System Services		**T1068** Exploitation for Privilege Escalation	**T1574** Hijack Execution Flow
	T1608 Stage Capabilities		**T1204** User Execution			**T1070** Indicator Removal on Host
						T1036 Masquerading
						T1112 Modify Registry
						T1027 Obfuscated Files or Information
						T1055 Process Injection
						T1620 Reflective Code Loading
						T1205 Traffic Signaling
						T1078 Valid Accounts

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
T1003 OS Credential Dumping	**T1135** Network Share Discovery	**T1570** Lateral Tool Transfer	**T1560** Archive Collected Data	**T1132** Data Encoding	**T1041** Exfiltration Over C2 Channel
T1056 Input Capture	**T1016** System Network Configuration Discovery	**T1072** Software Deployment Tools	**T1005** Data from Local System	**T1001** Data Obfuscation	**T1567** Exfiltration Over Web Service
T1110 Brute Force	**T1201** Password Policy Discovery		**T1114** Email Collection	**T1573** Encrypted Channel	
T1555 Credentials from Password Stores	**T1007** System Service Discovery		**T1056** Input Capture	**T1008** Fallback Channels	
	T1049 System Network Connections Discovery		**T1113** Screen Capture	**T1105** Ingress Tool Transfer	
	T1057 Process Discovery			**T1095** Non-Application Layer Protocol	
	T1083 File and Directory Discovery			**T1571** Non-Standard Port	
	T1087 Account Discovery			**T1090** Proxy	
				T1205 Traffic Signaling	
				T1102 Web Service	

References

1 Mila. (March 1, 2011). *Contagio*. “Feb 25 CVE-2010-3333 DOC China’s Military Build-up from a compromised IBEW-NECA Joint Trust Funds account.” Accessed on July 22, 2022 at http://contagiodump.blogspot.com/2011/03/cve-2010-3333-doc-chinas-military-build.html.

2 Karlo Zanki. (Sept. 22, 2020). *Reversing Labs*. “Taidoor – a truly persistent threat.” Accessed on July 22, 2022 at https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat.

3 Luo Zenghan. (Aug. 19, 2020). “調查局首度揭露國內政府委外廠商成資安破口的現況，近期至少10個公家單位與4家資訊服務供應商遇害.” Accessed on July 22, 2022 at https://www.ithome.com.tw/news/139504.

4 Cybersecurity & Infrastructure Security Agency. (Aug. 3, 2020). “Malware Analysis Report (AR20-216A).” Accessed on July 22, 2022 at https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-216a.

5 Yoshihiro Ishikawa. (April 24, 2020). Lac Watch. “標的型攻撃の新たな手口判明。診断ツール「PoshC2」を悪用する攻撃の流れを解説.” Accessed on July 22, 2022 at https://www.lac.co.jp/lacwatch/people/20200424_002177.html.

6 Nart Villeneuve, Thoufique Haq, and Ned Moran. (Sept. 6, 2013). *Mandiant*. “Evasive Tactics: Taidoor.” Accessed on July 22, 2022 at https://www.mandiant.com/resources/evasive-tactics-taidoor-3.

7 A L Johnson. (Mar. 27, 2012). *Broadcom*. “Trojan.Taidoor takes aim at policy think tanks.” Accessed on July 22, 2022 at https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=910b21d2-9e54-42a7-8a47-7c2d26bd54d8&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

8 Trend Micro. (Aug. 18, 2012). “Taidoor Campaign Targets Government Agencies in Taiwan.” Accessed on July 22, 2022 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/taidoor-campaign-targets-government-agencies-in-taiwan.

9 Cyber Threat Research Team. (Jan. 26, 2018). Trend Micro. “標的型攻撃キャンペーン「Taidoor」の活動が日本で活発化.”Accessed on July 22, 2022 at https://blog.trendmicro.co.jp/archives/16893.

10 A L Johnson. (Mar. 27, 2012). *Broadcom*. “Trojan.Taidoor takes aim at policy think tanks.” Accessed on July 22, 2022 at https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=910b21d2-9e54-42a7-8a47-7c2d26bd54d8&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

11 Macnica. (n.d.). “日本を狙うサイバーエスピオナージ（標的型攻撃）の動向 2018年上半期.” Accessed on July 22, 2022 at https://www.macnica.co.jp/business/security/manufacturers/mpressioncss/report.html.

12 Luo Zenghan. (Aug. 19, 2020). “調查局首度揭露國內政府委外廠商成資安破口的現況，近期至少10個公家單位與4家資訊服務供應商遇害.” Accessed on July 22, 2022 at https://www.ithome.com.tw/news/139504.

13 Trend Micro. (Aug. 18, 2012). “Taidoor Campaign Targets Government Agencies in Taiwan.” Accessed on July 22, 2022 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/taidoor-campaign-targets-government-agencies-in-taiwan.

14 Security of Things: HITCON 2015. (n.d.). *CHROOT Security Group*. “Lets Play Hide and Seek in the Cloud- The APT Malware Favored in Cloud Services.” Accessed on July 22, 2022 at https://hitcon.org/2015/CMT/agenda/#day2-h-r2.

15 Nart Villeneuve, Thoufique Haq, and Ned Moran. (Sept. 6, 2013). *Mandiant*. “Evasive Tactics: Taidoor.” Accessed on July 22, 2022 at https://www.mandiant.com/resources/evasive-tactics-taidoor-3.

16 Ashley X Belinda. (n.d.). *HitCon 2015*. “Let’s Play Hide and Seek in the Cloud: The APT Malwares Favored in Cloud Service.” Accessed on July 22, 2022 at https://hitcon.org/2015/CMT/download/day2-h-r2.pdf.

17 Cybersecurity & Infrastructure Security Agency. (Aug. 3, 2020). “Malware Analysis Report (AR20-216A).” Accessed on July 22, 2022 at https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-216a.

18 Karlo Zanki. (Sept. 22, 2020). *Reversing Labs*. “Taidoor – a truly persistent threat.” Accessed on July 22, 2022 at https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat.

19 Global Research and Analysis Team. (May 25, 2016). *Kaspersky Labs*. “CVE-2015-2545: Overview of Current Threats.” Accessed on July 22, 2022 at https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/.

20 Nart Villeneuve, Thoufique Haq, and Ned Moran. (Sept. 6, 2013). *Mandiant*. “Evasive Tactics: Taidoor.” Accessed on July 22, 2022 at https://www.mandiant.com/resources/evasive-tactics-taidoor-3.

21 Cyber Threat Research Team. (Jan. 26, 2018). *Trend Micro*. “標的型攻撃キャンペーン「Taidoor」の活動が日本で活発化.”Accessed on July 22, 2022 at https://blog.trendmicro.co.jp/archives/16893.

22 Ashley X Belinda. (n.d.). *HitCon 2015*. “Let’s Play Hide and Seek in the Cloud: The APT Malwares Favored in Cloud Service.” Accessed on July 22, 2022 at https://hitcon.org/2015/CMT/download/day2-h-r2.pdf.

23 RSAAdmin. (Nov. 25, 2015). *RSA*. “Detecting GlassRAT using Security Analytics and ECAT.” Accessed on Sept. 19, 2022 at https://community.netwitness.com/t5/netwitness-community-blog/detecting-glassrat-using-security-analytics-and-ecat/bap/518585.

24 Eduard Kovacs. (Nov. 24, 2015). *Security Week*. “GlassRAT Malware Stayed Under Radar For Years: RSA.” Acessed on Sept. 19, 2022 at https://www.securityweek.com/glassrat-malware-stayed-under-radar-years-rsa.

25 Nart Villeneuve, Thoufique Haq, and Ned Moran. (Sept. 6, 2013). *Mandiant*. “Evasive Tactics: Taidoor.” Accessed on July 22, 2022 at https://www.mandiant.com/resources/evasive-tactics-taidoor-3.

26 Unit Canary. (March 6, 2019). NTT Security Holdings. “Taidoor を用いた標的型攻撃 解析レポート” Accessed on July 22, 2022 at https://jp.security.ntt/resources/taidoor.pdf.

27 Macnica. (n.d.). “日本を狙うサイバーエスピオナージ（標的型攻撃）の動向 2018年上半期.” Accessed on July 22, 2022 at https://www.macnica.co.jp/business/security/manufacturers/mpressioncss/report.html.

28 Unit Canary. (March 6, 2019). *NTT Security Holdings*. “Taidoor を用いた標的型攻撃 解析レポート” Accessed on July 22, 2022 at https://jp.security.ntt/resources/taidoor.pdf.

29 Macnica Networks Corp. (April 1, 2019). “標的型攻撃の実態と 対策アプローチ: 日本を狙うサイバーエスピオナージの動向 2018年度下期.” Accessed on July 22, 2022 at https://files.macnica.co.jp/mnc/mpressioncss_ta_report_2019.pdf.

30 Security of Things: HITCON 2015. (n.d.). *CHROOT Security Group*. “Lets Play Hide and Seek in the Cloud- The APT Malware Favored in Cloud Services.” Accessed on July 22, 2022 at https://hitcon.org/2015/CMT/agenda/#day2-h-r2.

31 Cybersecurity & Infrastructure Security Agency. (Aug. 3, 2020). “Malware Analysis Report (AR20-216A).” Accessed on July 22, 2022 at https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-216a.

32 Karlo Zanki. (Sept. 22, 2020). *Reversing Labs*. “Taidoor – a truly persistent threat.” Accessed on July 22, 2022 at https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat.

33 Global Research and Analysis Team. (May 25, 2016). *Kaspersky Labs*. “CVE-2015-2545: Overview of Current Threats.” Accessed on July 22, 2022 at https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/.

34 Nart Villeneuve, Thoufique Haq, and Ned Moran. (Sept. 6, 2013). *Mandiant*. “Evasive Tactics: Taidoor.” Accessed on July 22, 2022 at https://www.mandiant.com/resources/evasive-tactics-taidoor-3.

35 Security of Things: HITCON 2015. (n.d.). *CHROOT Security Group*. “Lets Play Hide and Seek in the Cloud- The APT Malware Favored in Cloud Services.” Accessed on July 22, 2022 at https://hitcon.org/2015/CMT/agenda/#day2-h-r2.

36 Jessa De La Torre. (Dec. 3, 2012). *Trend Micro*. “Taidoor Update: Taidoor Gang Tags Its Victims.” Accessed on July 25, 2022 at https://blog.trendmicro.com/trendlabs-security-intelligence/taidoor-update-taidoor-gang-tags-its-victims/.

37 Jessa De La Torre. (Dec. 3, 2012). *Trend Micro*. “Taidoor Update: Taidoor Gang Tags Its Victims.” Accessed on July 25, 2022 at https://blog.trendmicro.com/trendlabs-security-intelligence/taidoor-update-taidoor-gang-tags-its-victims/.

38 Ashley X Belinda. (n.d.). *HitCon 2015*. “Let’s Play Hide and Seek in the Cloud: The APT Malwares Favored in Cloud Service.” Accessed on July 22, 2022 at https://hitcon.org/2015/CMT/download/day2-h-r2.pdf.

39 Cybersecurity & Infrastructure Security Agency. (Aug. 3, 2020). “Malware Analysis Report (AR20-216A).” Accessed on July 22, 2022 at https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-216a.

40 Global Research and Analysis Team. (May 25, 2016). *Kaspersky Labs*. “CVE-2015-2545: Overview of Current Threats.” Accessed on July 22, 2022 at https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/.

41 Macnica. (n.d.). “日本を狙うサイバーエスピオナージ（標的型攻撃）の動向 2018年上半期.” Accessed on July 22, 2022 at https://www.macnica.co.jp/business/security/manufacturers/mpressioncss/report.html.

42 Unit Canary. (March 6, 2019). NTT Security Holdings. “Taidoor を用いた標的型攻撃 解析レポート” Accessed on July 22, 2022 at https://jp.security.ntt/resources/taidoor.pdf.

43 David Bizeul. (Nov. 7, 2014). *Airbus*. “The Eye of the Tiger.” Accessed on July 25, 2022 at https://airbus-cyber-security.com/the-eye-of-the-tiger/.

44 Mitre. (May 31, 2017). “PittyTiger.” Accessed on July 25, 2022 at https://attack.mitre.org/groups/G0011/.

45 Mandiant. (n.d.). “Advanced Persistent Threats.” Accessed on July 25, 2022 at https://www.mandiant.com/resources/insights/apt-groups#apt24:~:text=been%20made%20public.-,APT24,-AKA%3A%20PittyTiger.

46 Sophos. (Apr. 29, 2014). “Troj/Rerol-A.” Accessed on July 25, 2022 at https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Rerol-A/detailed-analysis.

47 Sophos. (May 29, 2014). “Troj/Goldsun-B.” Accessed on July 22, 2022 at https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Goldsun-B/detailed-analysis.

48 David Bizeul. (Nov. 7, 2014). *Airbus*. “The Eye of the Tiger.” Accessed on July 25, 2022 at https://airbus-cyber-security.com/the-eye-of-the-tiger/#:~:text=ROLES%20AND%20ORGANIZATION.

49 Cybersecurity & Infrastructure Security Agency. (Aug. 3, 2020). “Malware Analysis Report (AR20-216A).” Accessed on July 22, 2022 at https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-216a.

50 Electronic Transactions Development Agency. (Feb. 3, 2022). *Electronic Transactions Development Agency*. “APT group: Taidoor.” Accessed on July 25, 2022 at https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Taidoor&n=1.

51 Mitre. (May 31, 2017). *Mitre*. “Taidoor.” Accessed on July 25, 2022 at https://attack.mitre.org/software/S0011/.

52 Karlo Zanki. (Sept. 22, 2020). *Reversing Labs*. “Taidoor – a truly persistent threat.” Accessed on July 22, 2022 at https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat.

53 David Bizeul. (Nov. 7, 2014). *Airbus*. “The Eye of the Tiger.” Accessed on July 25, 2022 at https://airbus-cyber-security.com/the-eye-of-the-tiger/.

54 Electronic Transactions Development Agency. (Jan. 7, 2021). *Electronic Transactions Development Agency*. “APT group: PT 12, Numbered Panda.” Accessed on July 25, 2022 at https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2012%2C%20Numbered%20Panda&n=1.

55 Hiroaki Hara. (2022). *Trend Micro*. “Ambiguously Black: The Current State of Earth Hundun’s Arsenal.” Accessed at July 25, 2022 at https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_8_hara_en.pdf.

56 Nick Dai, Ted Lee, Vickie Su. (Dec. 14, 2021). *Trend Micro*. “Collecting In The Dark: Tropic Trooper Targets Transportation and Government.” Accessed on July 25, 2022 at https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html.

57 Jaromir Horejsi, Joey Chen, and Joseph C Chen. (March 14, 2018). *Trend Micro*. “Tropic Trooper’s New Strategy.” Accessed on July 23, 2022 at https://www.trendmicro.com/en_us/research/18/c/tropic-trooper-new-strategy.html.

58 Joey Chen. (May 12, 2020). *Trend Micro*. “Tropic Tropper’s USBferry Targtes Air-Gapped Networks.” Accessed on July 23, 2022 at https://www.trendmicro.com/en_us/research/20/e/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments.html.

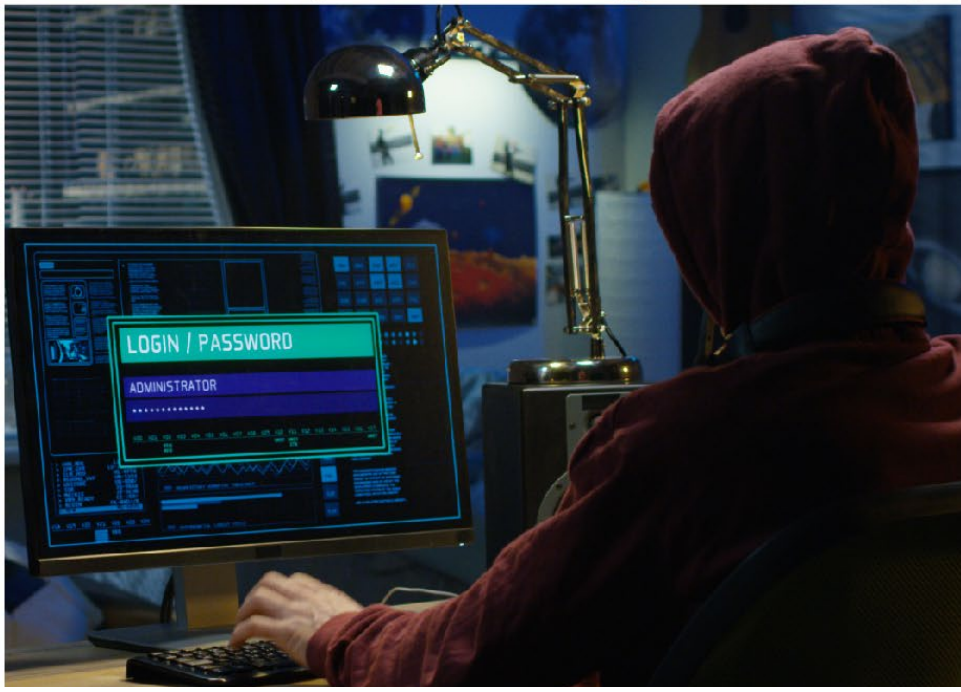
59 Hara Hiroaki and Ted Lee. (Aug. 24, 2021). “APT41 Resurfaces as Earth Baku with New Cyberespionage Campaign.” Accessed on July 24, 2022 at https://www.trendmicro.com/en_us/research/21/h/apt41-resurfaces-as-earth-baku-with-new-cyberespionage-campaign.html.

60 Macnica Networks Corp. (April 1, 2019). “標的型攻撃の実態と 対策アプローチ: 日本を狙うサイバーエスピオナージの動向 2018年度下期.” Accessed on July 22, 2022 at https://files.macnica.co.jp/mnc/mpressioncss_ta_report_2019.pdf.

61 Tim Yeh. (2021). *Code Blue 2021*. “Operation VPNOver: DragonOK’s Persistent Attacks on East Asia via VPN Flaw.” Accessed on July 24, 2022 at https://codeblue.jp/2021/en/talks/?content=talks_13.

62 Yoshihiro Ishikawa. (April 24, 2020). *Lac Watch*. “標的型攻撃の新たな手口判明。診断ツール「PoshC2」を悪用する攻撃の流れを解説.” Accessed on July 22, 2022 at https://www.lac.co.jp/lacwatch/people/20200424_002177.html.

63 CH Lei. (Oct. 2022). *Trend Micro.* “The Rise of Earth Aughisky: Tracking The Campaigns Taidoor Started.” Last accessed on Oct. 3, 2022 at https://documents.trendmicro.com/assets/txt/IOCs-the-rise-of-earth-aughisky-tracking-the-campaigns-taidoor-started.pdf.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research