

Tracking Earth Aughisky's Malware and Changes

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

Published: 2022-10-04 · Archived: 2026-04-05 12:41:06 UTC

APT & Targeted Attacks

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.



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.

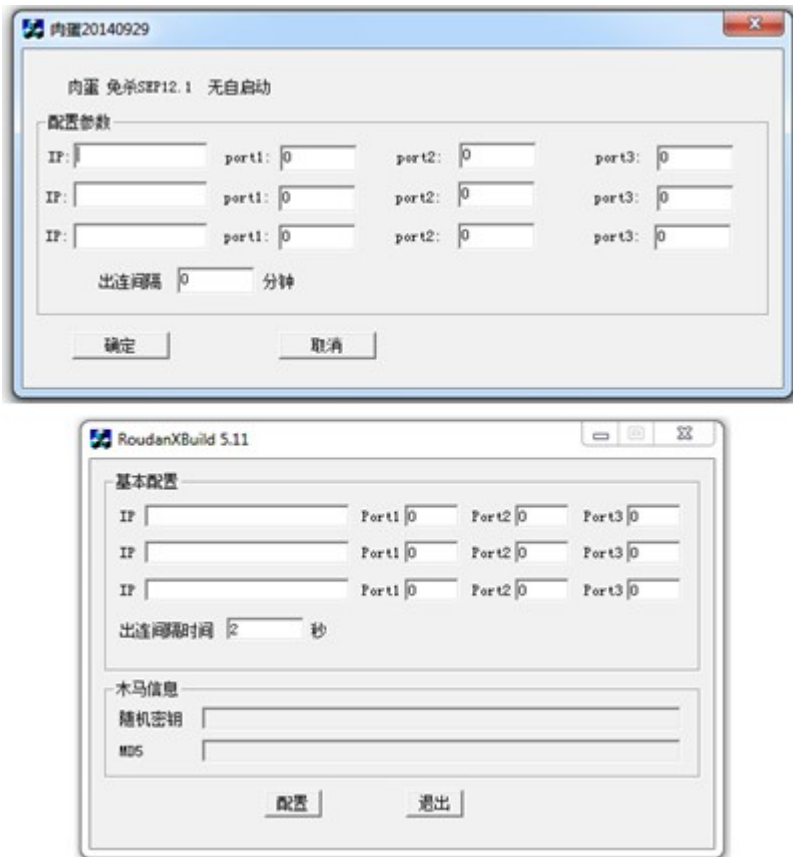


Figure 1. Some of the builders taken from different samples of Roudan

```
GET /df1=1.html?ya=muhgqh1212121212 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: ██████████
Connection: Keep-Alive
Cache-Control: no-cache

GET /Index.jsp?booyjfv112121212121212 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: ██████████
Connection: Keep-Alive
Cache-Control: no-cache

GET /cbdex.php?id=006152121212121212 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: ██████████
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: ██████████
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	38211.115.93.8
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	3532c9cfa5c75
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	48	45	59	2D	2D	2D	2D	2D	PUBLIC KEY-----
0A	4D	49	49	42	49	6A	41	4E	42	67	68	71	68	68	69	.MIIIBIjANBgkqhki
47	39	77	30	42	41	51	45	46	41	41	4F	43	41	51	38	G9w0BAQEFAAOCAQ8
41	4D	49	49	42	43	67	48	43	41	51	45	41	70	58	55	AMIIIBCgKCAQEApxU
74	76	37	71	74	76	33	48	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	68	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	9RYcZegIzcvxQ=="
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+/Os8GJ+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.

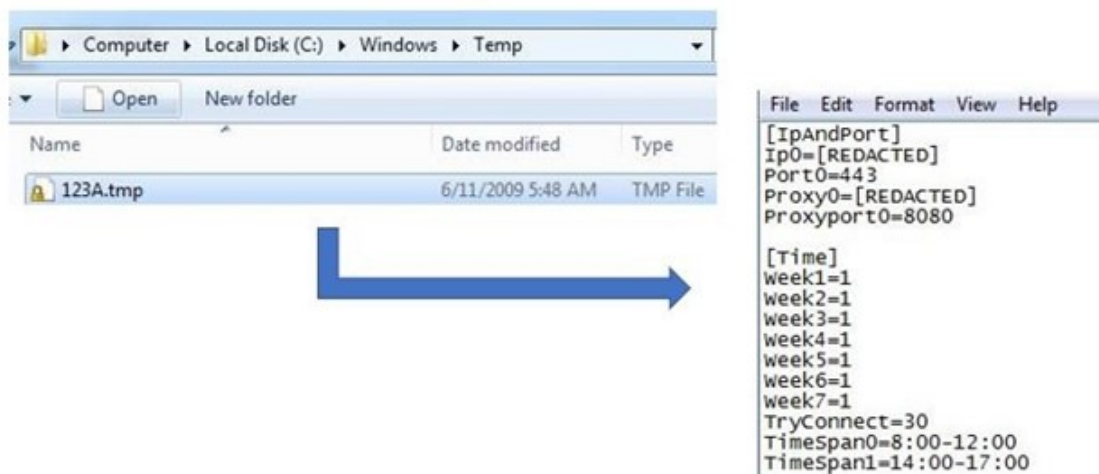


Figure 4. Decrypted GrubbyRAT configuration

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.

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.

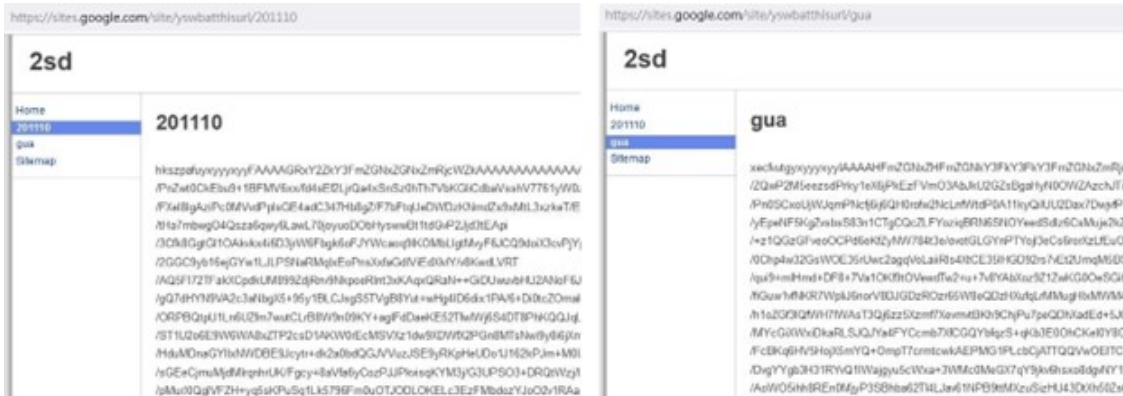


Figure 8. Roudan (left) and SiyBot (right) payload in the same repository

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 log hosts being used by Roudan and earlier versions of Taleret.



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

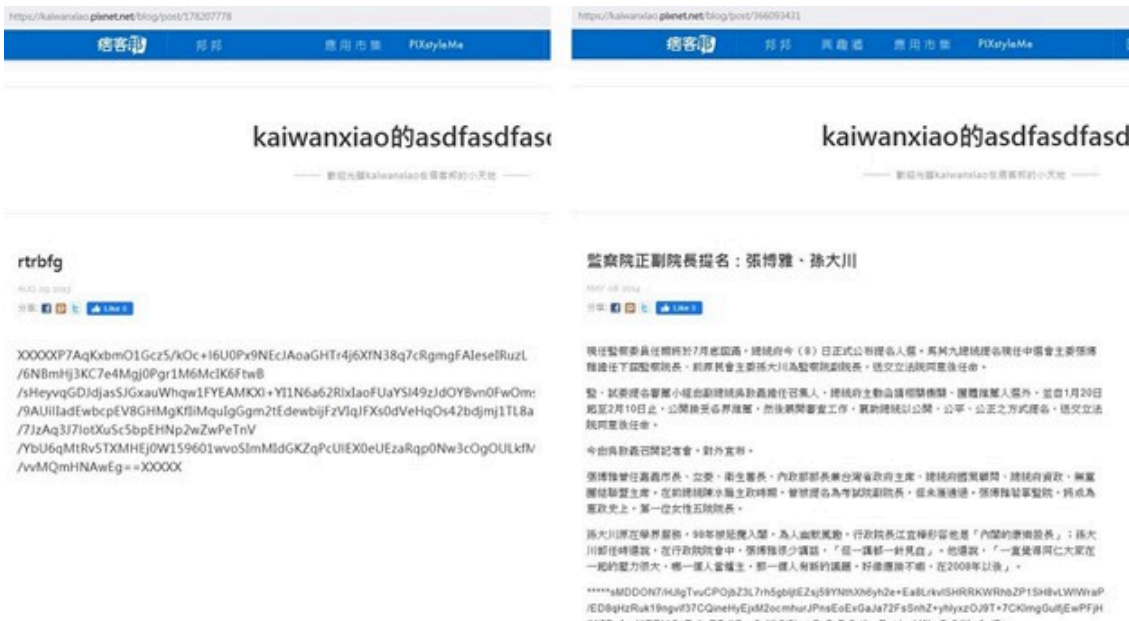


Figure 10. Taleret configuration (left) and Comeon downloader payload (Roudan, right) on the same blog

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](#).

Tags

Source: https://www.trendmicro.com/en_us/research/22/j/tracking-earth-ughiskys-malware-and-changes.html