Sequel: Gifts from Tropical Pirates - Who is the Sender? Look for the Attacker Group

Published: 2023-10-06 · Archived: 2026-04-05 21:04:38 UTC

Background

In our previous post, we investigated an attack campaign by an APT actor called Tropic Trooper (aka Pirate Panda, KeyBoy), and disclosed that they used spear phishing emails to infect victims with malware.
In addition, an infection flow and malware's behavior were disclosed too. We have continued to observe their activities since then.
This post provides how we attributed this attack campaign to Tropic Trooper based on our malware analysis.

What is Tropic Trooper?

Tropic Trooper is a cyber espionage group known for conducting cyber attacks in the Asia-Pacific region. They target government, healthcare, transportation, and high-tech industries, and have been active since 2011.
References are listed as follows.

- Tropic Trooper, Pirate Panda, KeyBoy, Group G0081 | MITRE ATT&CK®
- Operation Tropic Trooper: Relying on Tried-and-Tested Flaws to Infiltrate Secret Keepers
- Cyber Espionage (Targeted Attacks) Aimed at Japan in FY2022

We believe this attack campaign linked to the Tropic Trooper, has been targeting companies in East Asia since May 2023 until now. We estimate that semiconductor and rare metal related industries are particularly targeted.
Our analysis has confirmed that the malware EntryShell shares many similarities with the malware KeyBoy.

The Need for Attribution

Attribution is the process of identifying the threat group responsible for a targeted attack. This is often done by analyzing the malware used in the attack, as specific groups often have exclusive access to the certain malware.
By identifying the group responsible for a targeted attack, organizations can learn from the report about past attacks by that group and take steps to mitigate future attacks.
For example, understanding the threat group profile can help organizations to take more effective countermeasures, such as preventing damage escalation during an attack and taking preventive and detection measures in advance.
Additionally, obtaining the latest information on the attacker's activities can make it possible to take even more proactive measures.

Overall picture of the campaign

In our previous analysis, we discussed a malware with two functions: Installer (infection) and Loader (loading). With the loader, it loads the Cobalt Strike Beacon.
In addition to the malware, we also collected and analyzed over 200 samples and related files associated with this malware using paid intelligence services and public information.
We found that the Loader loads other malware or uses new malware. In this section, we will confirm the infection flow.

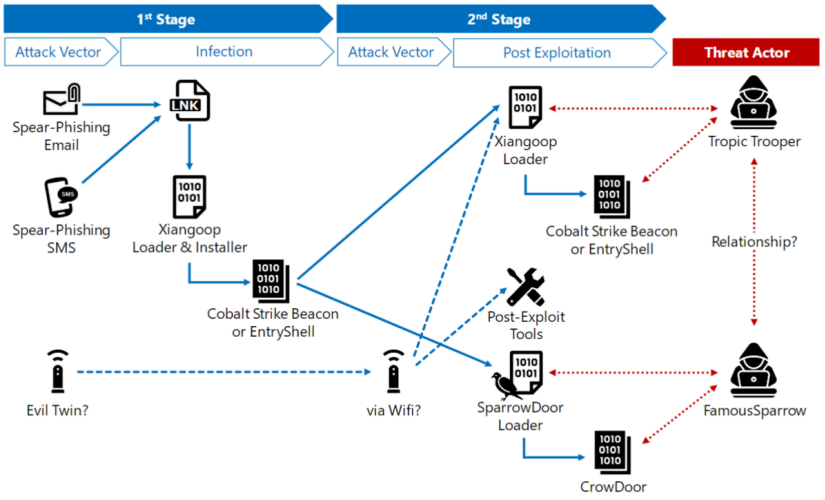

Figure 1. Overall picture of the campaign

First, the attacker attempted to break in a target device in the 1st s tage (Intrusion) by sending malware via email or SMS. The malware has two functions: Installer (infect) and Loader (load).This malware is responsible for the initial infection, and it deploys fileless malware such as Cobalt Strike Beacon and EntryShell in memory as a payload.

We named this malware Xiangoop Loader. It has two forms: Xiangoop Loader with Installer (used in the 1st stage and initial infection) and Xiangoop simple Loader (used in the 2nd stage).
After the initial infection (1st stage), in the 2nd stage, the attacker used remote access to investigate the target device further, move laterally to other devices or servers, and load Cobalt Strike Beacon or EntryShell using Xiangoop Loader.
We also found that a different type of malware called CrowDoor was loaded from an existing SparrowDoor Loader in the 2nd stage.

Malware for 1st Stage	**Malware for 2nd Stage**
Malware attached to an email and used in initial infection	Malware used in intrusion
Xiangoop Loader with Installer Has Installer and Loader function Copies itself to the Windows 'public' folder and kicks Cobalt Strike Beacon or EntryShell is used as secondary sample	**Xiangoop simple Loader** Has only Loader function Installed in any location by attacker Cobalt Strike Beacon or EntryShell is used as secondary sample
	SparrowDoor Loader + CrowDoor Has a remote control function

Similarities to previous samples

The detailed analysis of each malware is available in the VB2023 presentation materials.
Virus Bulletin :: Unveiling activities of Tropic Trooper 2023: deep analysis of Xiangoop Loader and EntryShell payload
In this section, we will discuss the similarities to previous specimens that were revealed by the analysis of these malware.
We will focus on two areas:

- Similarities between EntryShell and KeyBoy
- Relationship between the new malware CrowDoor and FamousSparrow

Similarities between EntryShell and KeyBoy

We focused on the EntryShell malware used in this attack campaign; EntryShell is the malware loaded by the Xiangoop Loader Family.
The EntryShell we discovered is decrypted and deployed in memory by the Xiangoop Loader using DLL side loading, just like the Cobalt Strike Beacon introduced in the previous post.

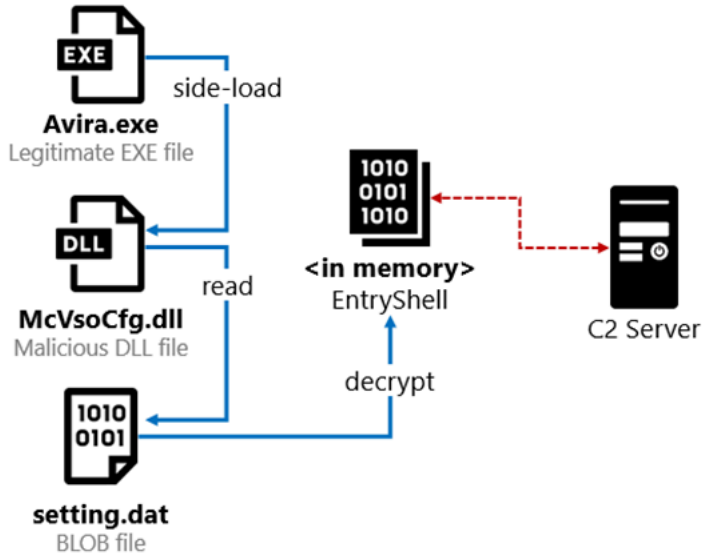

Figure 2. Sample infection flow by EntryShell

First, let's analyze the strings embedded in the EntryShell.
We noticed some characteristic strings that seemed to be error messages. The Yara rule for detecting KeyBoy that was created in 2016 detects those strings.
rules/malware/APT_KeyBoy.yar at master · Yara-Rules/rules · GitHub

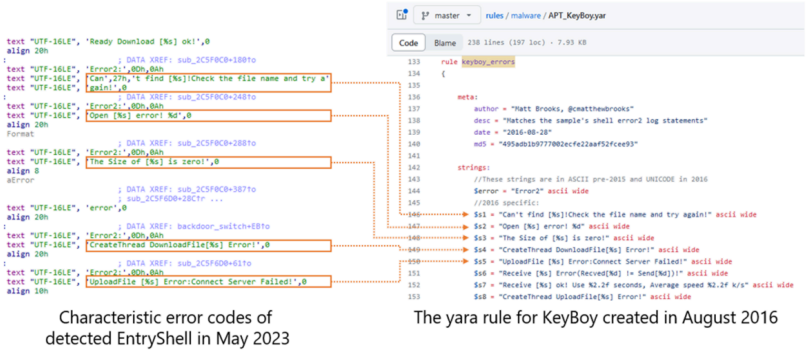

Figure 3. Compare with characteristic error codes and the Yara rule for KeyBoy

> **What is Yara**
>
> Yara is a tool that helps malware researchers identify and classify malware samples.
> It can quickly scan large amounts of files that match the patterns described in the rules. Yara rules can be flexibly written to describe patterns of text or binary and how they are combined.
>
> GitHub - VirusTotal/yara: The pattern matching swiss knife

Analysis of strings embedded EntryShell revealed that it contains hexadecimal strings represented as ASCII characters. We will investigate where these strings are used in the malware program.
The strings are first converted to binary data and then decrypted using AES ECB mode. The AES key, "afkngaikfaf" (padding is actually required), is hard-coded in another location in the sample.

Figure 4. Decrypting an encrypted string that embed in EntryShell

Checking the decrypted string, it matches the string defined in the Yara rule that detect previous versions of KeyBoy.
We also found that the encrypted string are mainly used in EntryShell backdoor function and its command ID.

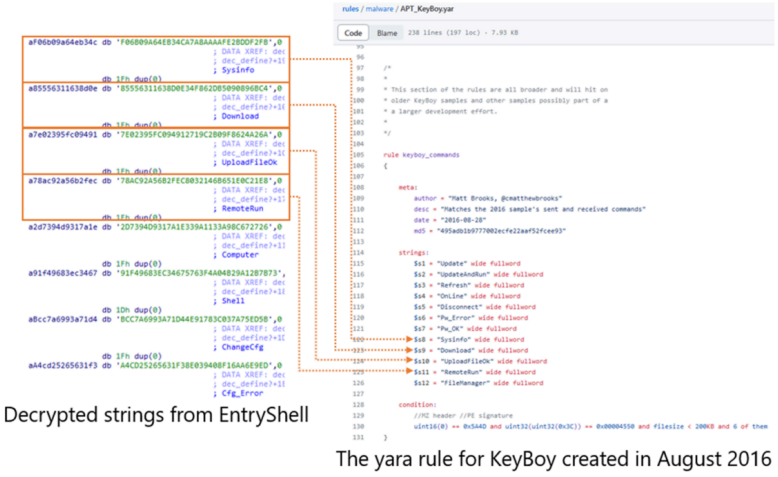

Figure 5. Compare with decrypted strings from EntryShell and the yara rule for KeyBoy

Attackers were aware of the existence of this Yara rule, and they were encrypting characteristic strings in EntryShell that are likely to be detected by that Yara rule in order not to be detected by security products.

The analysis confirmed that EntryShell is very similar to KeyBoy malware. Not only that, but we have also confirmed that compared to KeyBoy, EntryShell has updated and added functionality to its communication parts, malware configuration structure, and backdoors.
Based on this, we concluded that EntryShell is a malware upgrade from KeyBoy.

There is a report that KeyBoy was handled by Tropic Trooper, but there are no reports of KeyBoy being used by other threat actors. Therefore, KeyBoy can be said to be Tropic Trooper-specific malware.

Relationship between the new malware CrowDoor and FamousSparrow

Analysis of this attack campaign revealed a new RAT malware named CrowDoor.
The loader that loads the fileless malware CrowDoor is SparrowDoor Loader, which is used by the FamousSparrow attack group.

What is FamousSparrow?

FamousSparrow is a targeted attacker group reported by ESET in 2021. They are known to use a distinctive malware set called SparrowDoor.

FamousSparrow: A suspicious hotel guest

A new malware CrowDoor

Sample infection flow by CrowDoor is shown below.

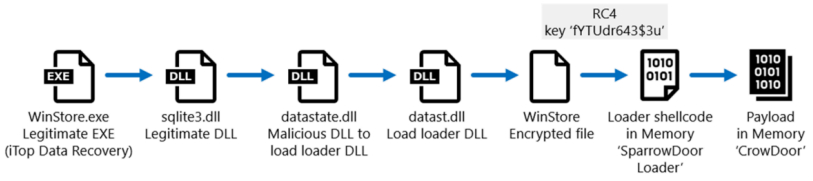

Figure 6. Sample infection flow by CrowDoor

Analysis of 2nd from the right loader shellcode in Figure 6 confirms that it matches the patterns of the Yara rules that detect the SparrowDoor Loader previously created.
Furthermore, comparison with previous samples shows that this shellcode uses the same code as the SparrowDoor Loader.

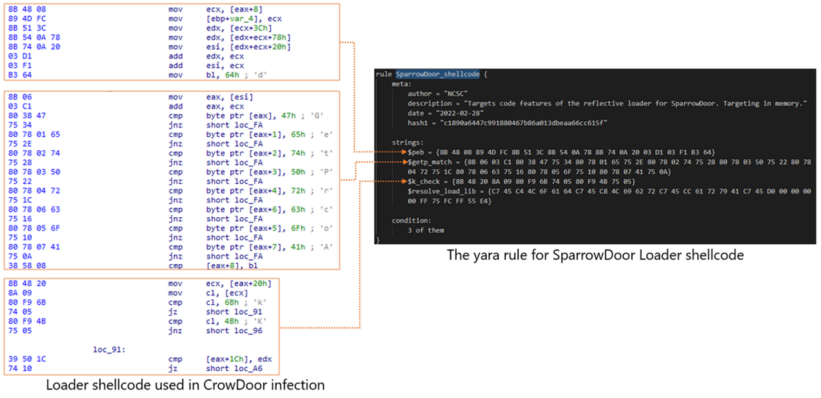

Figure 7. Comparison Loader shellcode strings in CrowDoor infection flow to Yara rules for detecting SparrowDoor Loader shellcode

The PE file of CrowDoor that is deployed in memory by the above Loader shellcode has a sequence of 0s at the beginning and lacks the magic numbers “PE”. This is very similar to SparrowDoor, as written in the ESET blog.

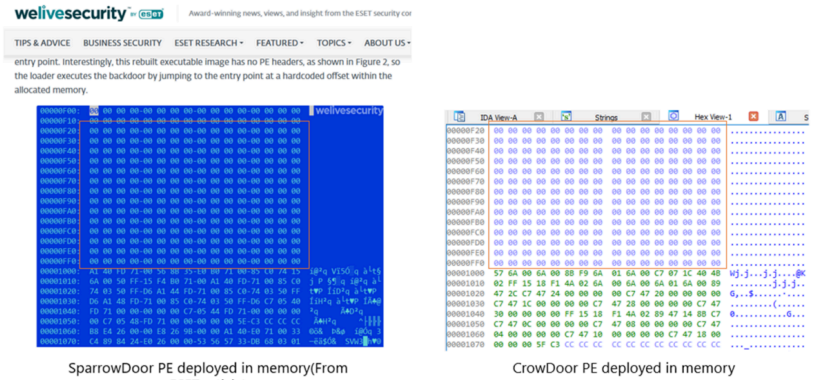

Figure 8. Similarities between Memory-deployed SparrowDoor PE and CrowDoor PE

We have also found command similarities between CrowDoor and SparrowDoor samples.

SparrowDoor

```
case 0x1A6B561Au:
  v43 = 0;
  memset(&v44, 0, 0x206u);
  MultiByteToWideChar_0(0xFDE9u, 0, v16, v15, &v43, 260);
  CreateDirectoryW(&v43, 0);
  break;
case 0x18695638u:
  My_RENAME(v16);
  break;
case 0x196A5629u:
  My_DeleteFile(v16,
  break;
```

```
v11 = 0;
v12 = 0;
v13 = 0;
v6 = 0;
v10 = 28;
v7 = FO_RENAME;
v8 = &v18;
v9 = &v20;
return SHFileOperationW(&v6);
```

```
v6 = 0;
v7 = 20;
v4 = FO_DELETE;
v5 = &v11;
return SHFileOperationW(&v3);
```

CrowDoor

```
case 0x2347148:                         // Create Directory
  memset(&v42, 0, 0x208u);
  MultiByteToWideChar_0(0xFDE9u, 0, (v4 + 16), *(v4 + 8), &v42, 260);
  if ( !CreateDirectoryW(&v42, 0) )
    GetLastError_0();
  continue;
case 0x2347149:                         // Rename File or Directory
  memset(&v46, 0, 0x104u);
  memset(&v47, 0, 0x104u);
  v21 = *(v4 + 16);
  mm(&v46, v4 + 17, v21);
  mm(&v47, v4 + v21 + 18, *(v21 + v4 + 17));
  memset(&v41, 0, 0x208u);
  memset(&v40, 0, 0x208u);
  MultiByteToWideChar = *MultiByteToWideChar_0;
  MultiByteToWideChar_0(0xFDE9u, 0, &v46, -1, &v41, 260);
  MultiByteToWideChar(65001, 0, &v47, -1, &v40, 260);
  v34 = 0;
  LOWORD(v32) = 28;
  *(&v32 + 2) = 0164;
  v30 = &v41;
  v31 = &v40;
  v28 = 0;
  v29 = FO_RENAME;
  v9 = &v51;
  if ( SHFileOperationW(&v28) )
    GetLastError_0();
  continue;
case 0x234714A:                         // // Delete File or Directory
  memset(&v39, 0, 0x208u);
  MultiByteToWideChar_0(0xFDE9u, 0, (v4 + 16), *(v4 + 8), &v39, 260);
```

Figure 9: Similarities between SparrowDoor and CrowDoor samples

We confirmed that CrowDoor was installed by the attacker after using the Xiangoop Loader Family.
Based on this, we believe that there is some connection between Tropic Trooper, which uses the Xiangoop Loader Family, and FamousSparrow, which uses the SparrowDoor.

Summary

- Xiangoop Loader Family is likely associated with Tropic Trooper based on the characteristics of the samples it calls
- A sample of the SparrowDoor Loader was used in an attack that also used the Xiangoop Loader Family. This sample is reported to be used by FamousSparrow.
- This suggests that Tropic Trooper and FamousSparrow are either the same group or are closely related.

Special thanks

The analysis of this case was conducted in cooperation with the Security Research Center of Macnica, Inc. We thank the company for its cooperation.

IoCs

file name	malware type	MD5	SHA1	SHA256
McVsoCfg.dll	Xiangoop Loader	bb01bc33b0475fb2624d906760ebe290	808f3cb47960e1b08c8b22dad780528d7fec966d	ACF4422360CA41E
NTUSER.EXE	legitimate exe	c214cc5b78616b44918ce62c8a2aa773	aa0018ef4bc398cf3e7c6b2dd9109c173d12b368	563d732c54221fcdd
setting.dat	BLOB EntryShell	cccc4cf8267815cf7ae1f924ef2d9b83	0031ddf8a700a43641ad988fb867d2c399dd6bba	da2963b338ab5324c
datast.dll	Loader of SparrowDoor Loader	a213873eb55dc092ddf3adbeb242bd44	3650899c669986e5f4363fdbd6cf5b78a6fcd484	23dea3a74e3ff6a367
datastate.dll	SparrowDoor Loader	8a900f742d0e3cd3898f37dbc3d6e054	6ddadecd10ef562fa4845794f5cba250606a366c	658e9b9947b01eaa3
sqlite3.dll	legitimate dll	2a589d796e2c4b8a47a8388471880cbb	721080c5e76aee6f0376ad122343181c1e0da61a	7d02140c3ff14cd5a0
WinStore	BLOB CrowDoor	90afb6d2dfd161ce7752226b8a52e609	e6da2bc32444d84bb1adb80ce01aa3340e5f203c	4f0cf8835d2818866
WinStore.exe	legitimate exe	5e352887630542e60eeb844a1c7ac034	b736fdda75a489e3cb8f0c1ae73adee07309ddb9	a47bf32ee0fd6b3c0