Attribution in Action

A Case Study of an Incident Involving Multiple Activity Clusters

Hiroaki Hara and Doel Santos

Speakers

Hiroaki Hara @ Palo Alto Networks

Principal Researcher

- 10+ years experience in threat research, malware analysis, and incident response
- Presented at Black Hat Asia, Virus Bulletin, HITCON, JSAC

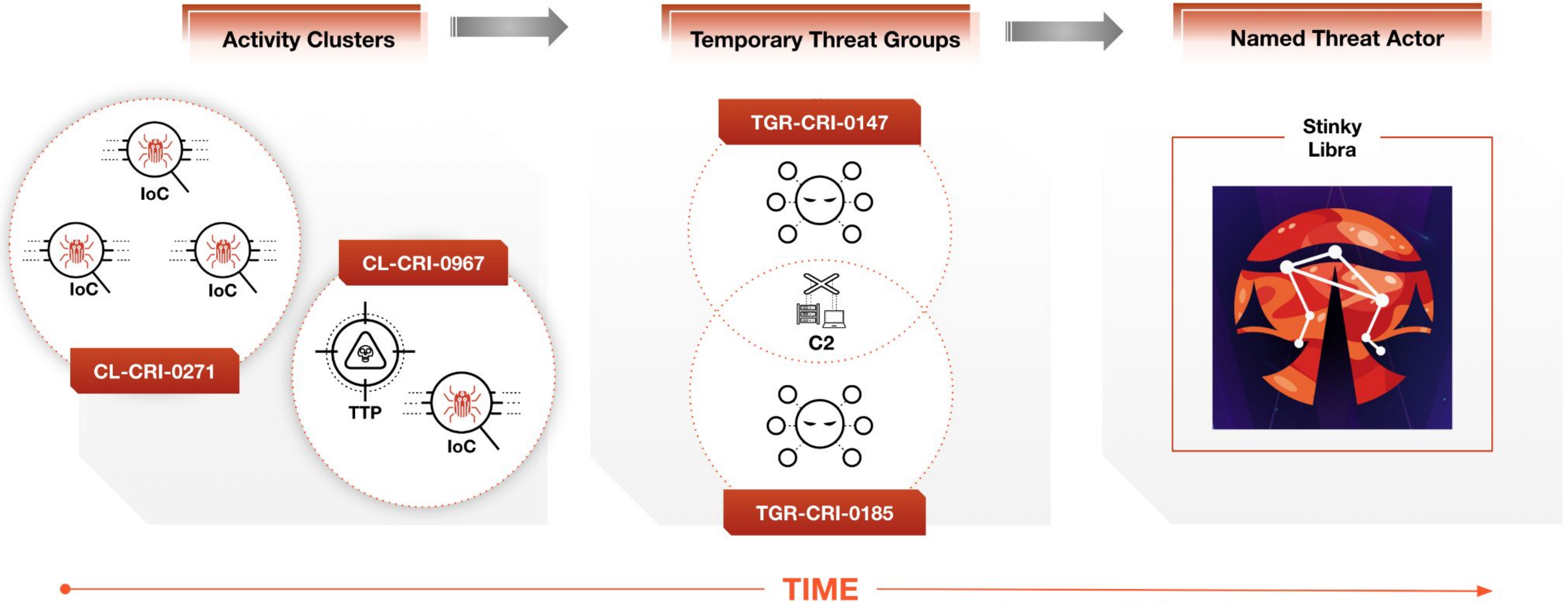
Doel Santos @ Palo Alto Networks

Principal Threat Researcher

- 8+ years of experience in threat research, and incident response
- Presented at CARO,BSIDES,OGE
- Black Hat Network Operations Center (NOC) Volunteer

Introduction of the Incident

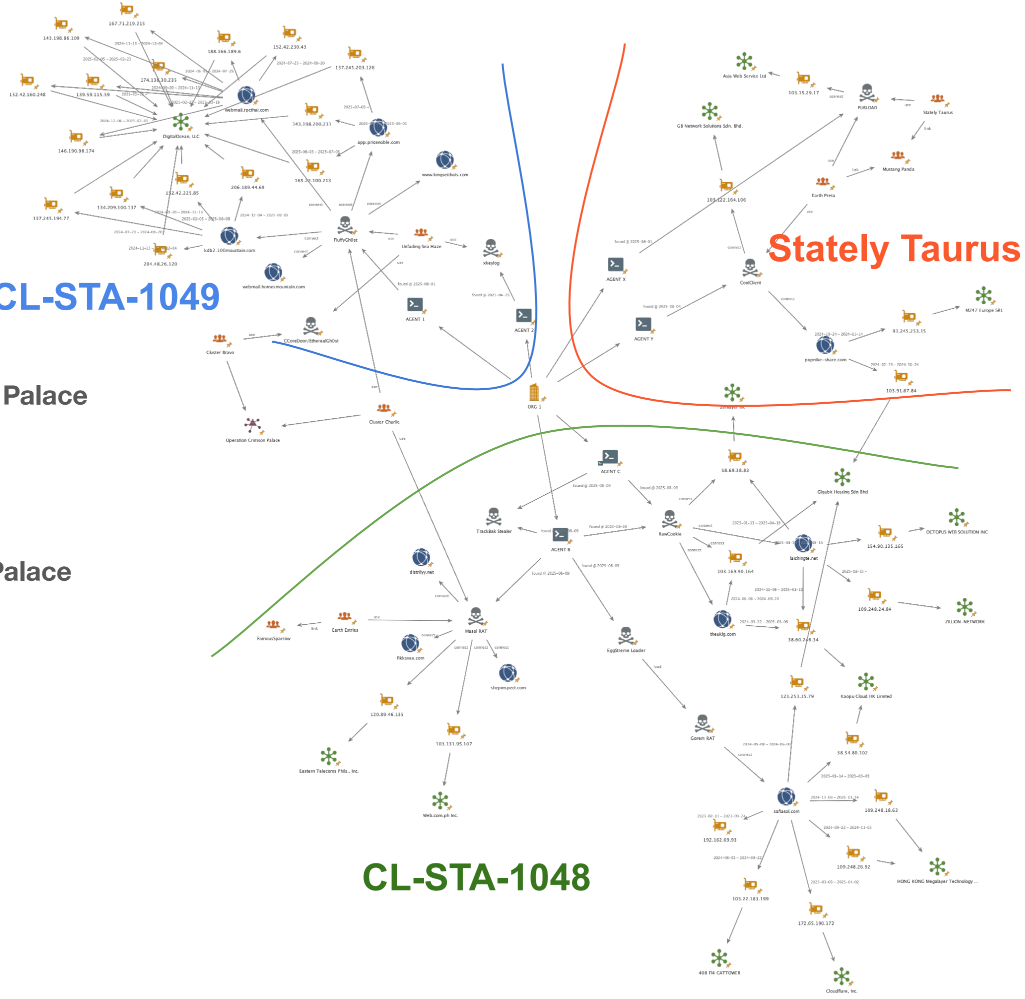
Attribution Framework



Overview of the Incident

3 activity clusters in single incident

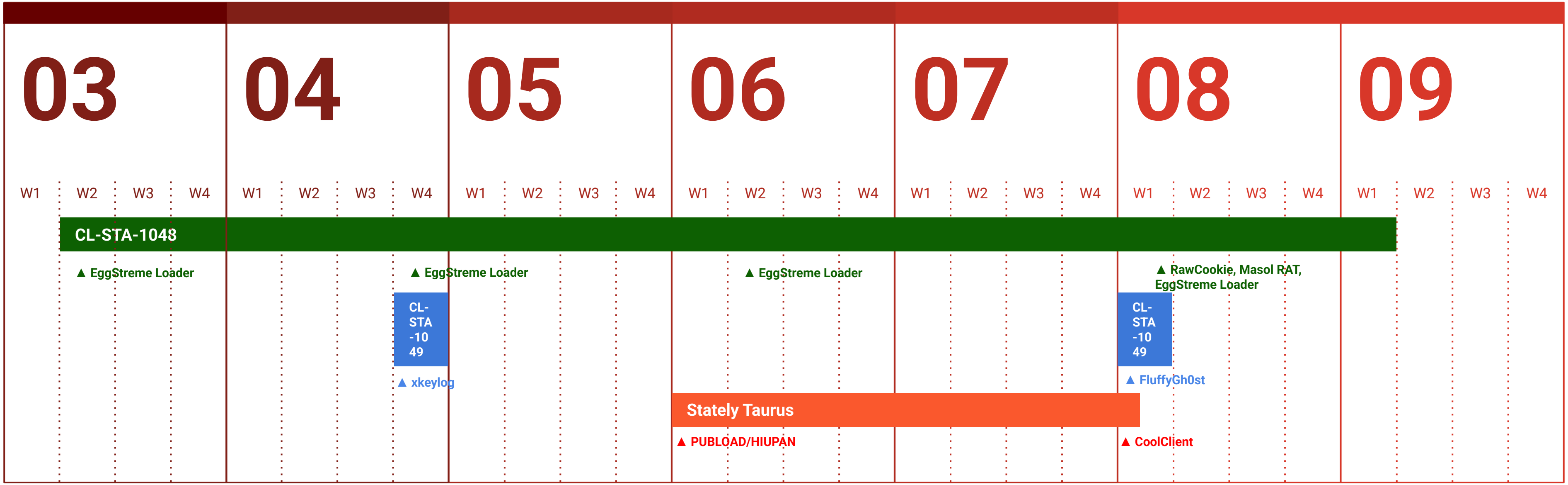
- **CL-STA-1048**
  - Possible connections with
    - **Earth Estries**
    - **Cluster Charlie** from **Operation Crimson Palace**
- **CL-STA-1049**
  - Attribute to **Unfading Sea Haze**
  - Possible connections with
    - **Cluster Bravo** from **Operation Crimson Palace**
- **Stately Taurus**
  - aka **Mustang Panda, Earth Preta**



Incident Timeline

Earliest timeline of this incident is March 2025

2025



03 04 05 06 07 08 09

W1 W2 W3 W4 W1 W2 W3 W4 W1 W2 W3 W4 W1 W2 W3 W4 W1 W2 W3 W4 W1 W2 W3 W4 W1 W2 W3 W4

CL-STA-1048

▲ EggStreme Loader

▲ EggStreme Loader

▲ EggStreme Loader

▲ RawCookie, Masol RAT, EggStreme Loader

CL-STA-1049

▲ xkeylog

CL-STA-1049

▲ FluffyGh0st

Stately Taurus

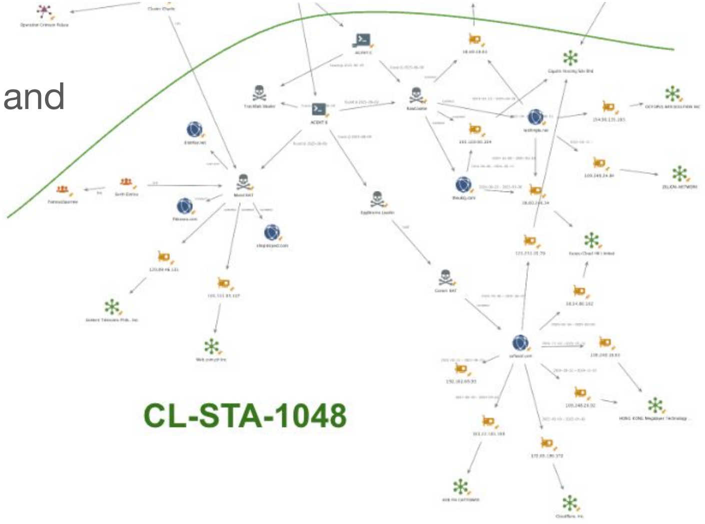
▲ PUBLOAD/HIUPAN

▲ CoolClient

Activity Cluster Analysis

CL-STA-1048

Espionage motivated activity cluster targeting Philippines, Taiwan and Malaysia, since at least June 2024



- Observed tools:
  - RawCookie (aka EggStreme Fuel)
  - EggStreme Loader
  - Gorem RAT (aka EggStreme Agent)
  - PoshRAT
  - Masol RAT
  - Original hacking tools
    - Chrome credential dumper, Signal message dumper
- Bitdefender has already mentioned EggStreme family, but no conclusion on attribution
  - https://www.bitdefender.com/en-us/blog/businessinsights/eggstreme-fileless-malware-cyberattack-apac

Mar
~

Agent A

- EggStreme Family

Aug
9

Agent B

- RawCookie
- TrackBak Stealer
- EggStreme Family
- PoshRAT
- Masol RAT

Aug
9

Agent C

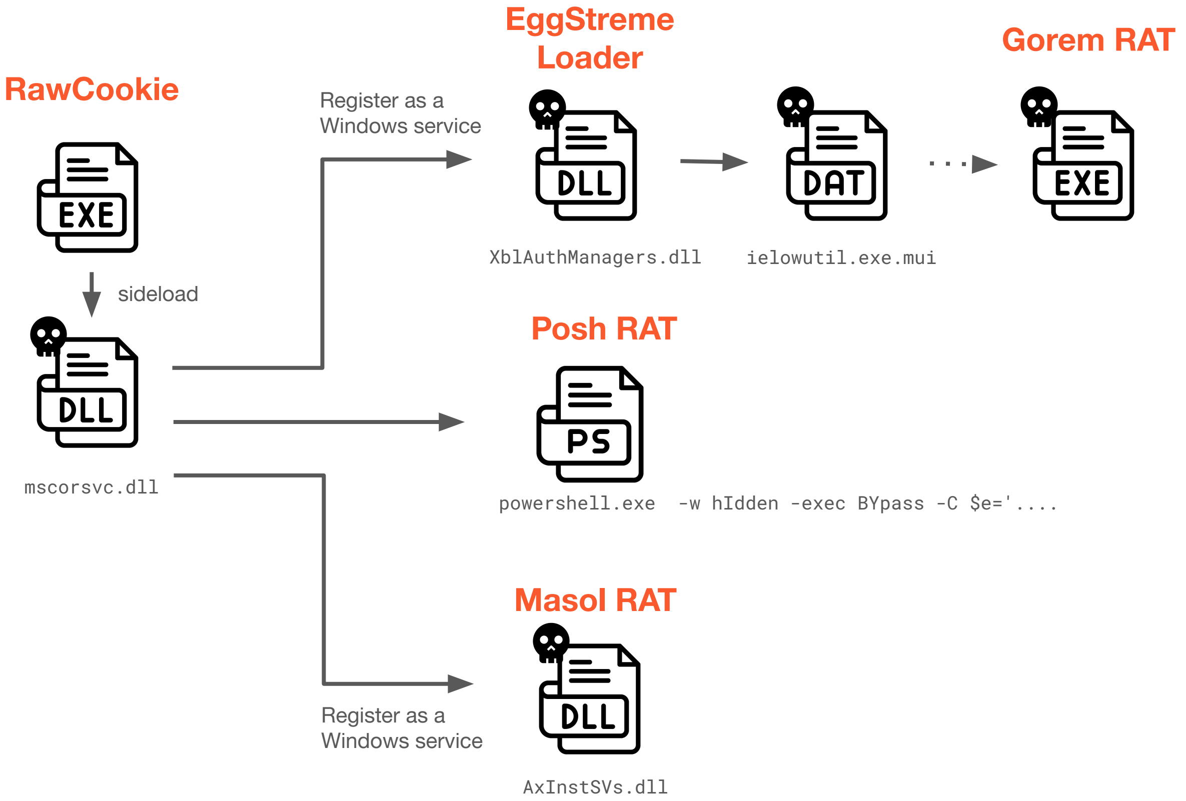
- RawCookie
- TrackBak Stealer

Sep
9

Agent D

- PoshRAT
- Signal Dumper

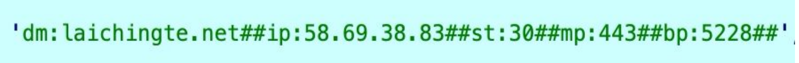
Infection Chain of CL-CRI-1048



```
powershell.exe  -w hIdden -exec BYpass -C $e='....
```

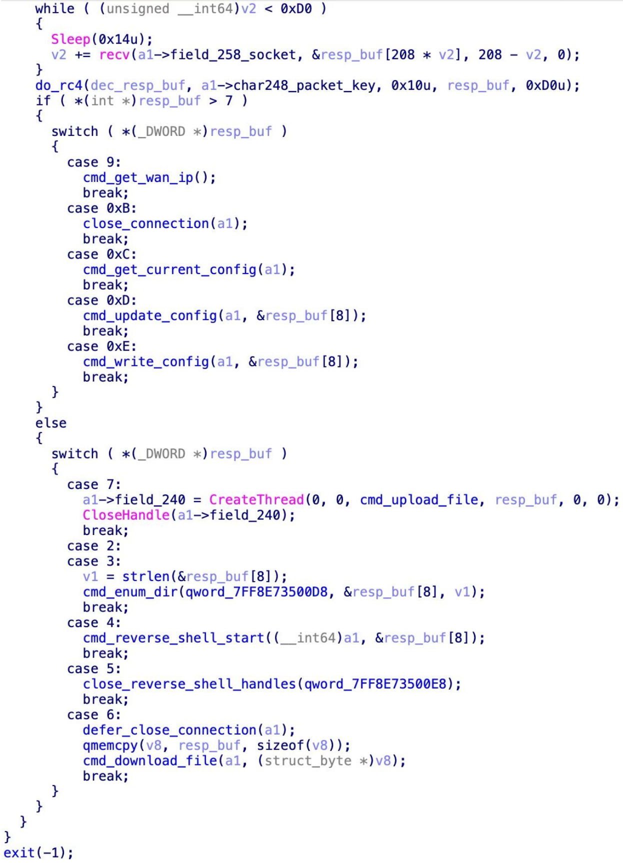
RawCookie (aka EggStreme Fuel)

Lightweight TCP-based backdoor

- Probably designed for an initial stage backdoor
- Features
  - ○ Upload/download a file
  - ○ Show a list of files/directories
  - ○ Start/terminate reverse shell
  - ○ Send the current global IP
  - ○ Get/update/overwrite C2 configuration
- C2 config is embedded but overwritable by reading it from a file
  - ○ %APPDATA%\Microsoft\Windows\Cookies\Cookies.dat
  - ○ 

```
'dm:laichingte.net##ip:58.69.38.83##st:30##mp:443##bp:5228##'
```

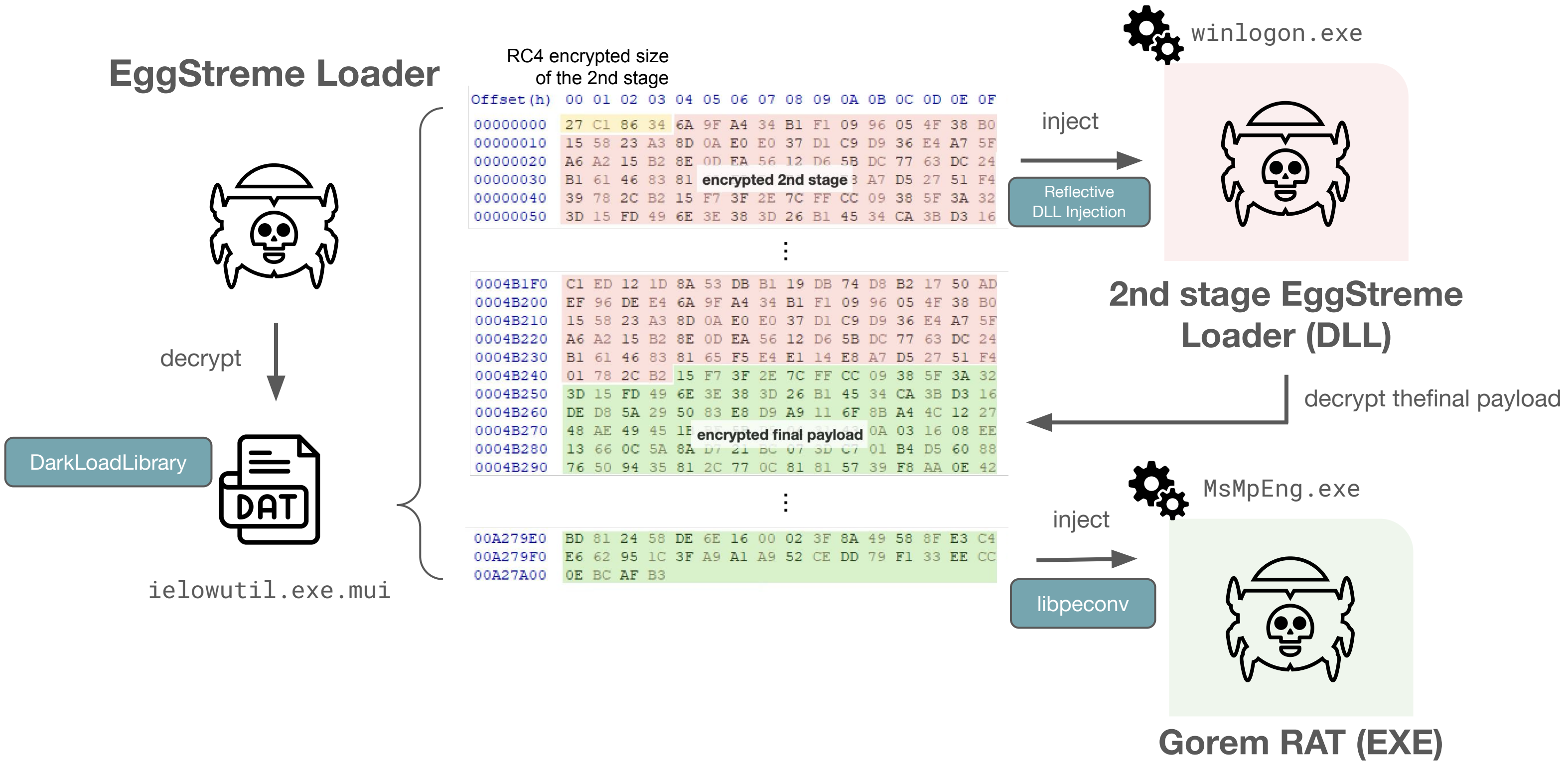
Backdoor command handler



```
    while ( (unsigned __int64)v2 < 0xD0 )
    {
      Sleep(0x14u);
      v2 += recv(a1->field_258_socket, &resp_buf[208 * v2], 208 - v2, 0);
    }
    do_rc4(dec_resp_buf, a1->char248_packet_key, 0x10u, resp_buf, 0xD0u);
    if ( *(int *)resp_buf > 7 )
    {
      switch ( *(_DWORD *)resp_buf )
      {
        case 9:
          cmd_get_wan_ip();
          break;
        case 0xB:
          close_connection(a1);
          break;
        case 0xC:
          cmd_get_current_config(a1);
          break;
        case 0xD:
          cmd_update_config(a1, &resp_buf[8]);
          break;
        case 0xE:
          cmd_write_config(a1, &resp_buf[8]);
          break;
      }
    }
    else
    {
      switch ( *(_DWORD *)resp_buf )
      {
        case 7:
          a1->field_240 = CreateThread(0, 0, cmd_upload_file, resp_buf, 0, 0);
          CloseHandle(a1->field_240);
          break;
        case 2:
        case 3:
          v1 = strlen(&resp_buf[8]);
          cmd_enum_dir(qword_7FF8E73500D8, &resp_buf[8], v1);
          break;
        case 4:
          cmd_reverse_shell_start((__int64)a1, &resp_buf[8]);
          break;
        case 5:
          close_reverse_shell_handles(qword_7FF8E73500E8);
          break;
        case 6:
          defer_close_connection(a1);
          qmemcpy(v8, resp_buf, sizeof(v8));
          cmd_download_file(a1, (struct_byte *)v8);
          break;
      }
    }
  }
}
exit(-1);
```

EggStreme Loader

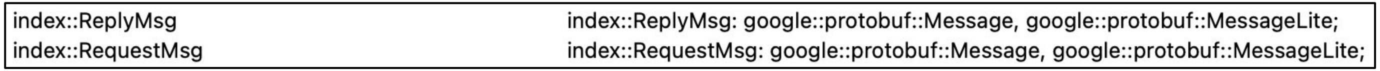
Multi-layered loader of Gorem RAT



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  27 C1 86 34 6A 9F A4 34 B1 F1 09 96 05 4F 38 B0
00000010  15 58 23 A3 8D 0A E0 E0 37 D1 C9 D9 36 E4 A7 5F
00000020  A6 A2 15 B2 8E 0D EA 56 12 D6 5B DC 77 63 DC 24
00000030  B1 61 46 83 81 encrypted 2nd stage 3 A7 D5 27 51 F4
00000040  39 78 2C B2 15 F7 3F 2E 7C FF CC 09 38 5F 3A 32
00000050  3D 15 FD 49 6E 3E 38 3D 26 B1 45 34 CA 3B D3 16

                                 ⋮

0004B1F0  C1 ED 12 1D 8A 53 DB B1 19 DB 74 D8 B2 17 50 AD
0004B200  EF 96 DE E4 6A 9F A4 34 B1 F1 09 96 05 4F 38 B0
0004B210  15 58 23 A3 8D 0A E0 E0 37 D1 C9 D9 36 E4 A7 5F
0004B220  A6 A2 15 B2 8E 0D EA 56 12 D6 5B DC 77 63 DC 24
0004B230  B1 61 46 83 81 65 F5 E4 E1 14 E8 A7 D5 27 51 F4
0004B240  01 78 2C B2 15 F7 3F 2E 7C FF CC 09 38 5F 3A 32
0004B250  3D 15 FD 49 6E 3E 38 3D 26 B1 45 34 CA 3B D3 16
0004B260  DE D8 5A 29 50 83 E8 D9 A9 11 6F 8B A4 4C 12 27
0004B270  48 AE 49 45 1E encrypted final payload 0A 03 16 08 EE
0004B280  13 66 0C 5A 8A D7 21 BC 07 3D C7 01 B4 D5 60 88
0004B290  76 50 94 35 81 2C 77 0C 81 81 57 39 F8 AA 0E 42

                                 ⋮

00A279E0  BD 81 24 58 DE 6E 16 00 02 3F 8A 49 58 8F E3 C4
00A279F0  E6 62 95 1C 3F A9 A1 A9 52 CE DD 79 F1 33 EE CC
00A27A00  0E BC AF B3
```

Gorem RAT (aka EggStreme Agent)

The most advanced backdoor in the CL-STA-1048 toolset, written in C++, using gRPC (mTLS) and Protocol Buffer



```
index::ReplyMsg        index::ReplyMsg: google::protobuf::Message, google::protobuf::MessageLite;
index::RequestMsg      index::RequestMsg: google::protobuf::Message, google::protobuf::MessageLite;
```

- Implemented 59 backdoor commands

Basic commands

- Disk (read/write/copy/move/delete file, enumerate/create/delete directory, get/set current directory, get available drive names with free spaces info, read small text file)
- Process (create new process, terminate specific process, list running process info)
- Network (enumerate established connections, get current network info, get TCP table, get ARP table)
- Services (enumerate/start/stop services, set service type)
- Registry (query/set/delete registry value)

Reconnaissance

- Get the startup command through WMI
- Get service information through WMI
- Get screenshot
- Get system uptime
- Enumerate services
- Send a ping to the remote machine
- Port scan
- Enumerate all the available network resources
- Show all the user sessions
- Get the specified remote machine host info using NTLMSSP over RCP

Command and Control

- Get current C2 server info
- Update C2 server/port info and save the current config to file
- Update sleep time and save the current config to file
- Start/terminate reverse shell session

Payload

- Run downloaded shellcode from the specified URL
- Inject the received zlib-compressed PE payload into svchost.exe

Pivot

- Execute the specified command against the specified remote machine over WMI
- Attempt to authenticate to the specified remote IP with the specified credentials over $IPC
- Register a ServiceDll in the specified remote machine
- Manipulate (list/create/delete) Scheduled Task on local/remote machine

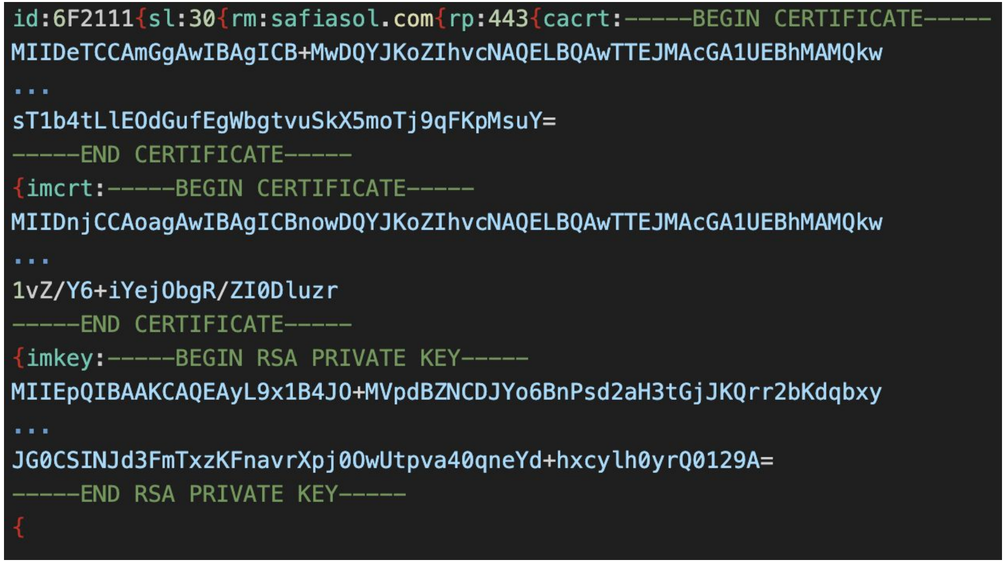
Others

- Compress specified file(s) as a GZIP archive using zlib
- Timestomping
- TCP proxy to the specified remote machine
- Set the file ownership
- Attempts to grab a file with the suffix `Network\Cookies-journal`, which is potentially a Chromium-based file containing credentials
- **Upload/download from Dropbox**

Config of Gorem RAT

Stored in `%LOCALAPPDATA%\Microsoft\Vault\Vault.dat` in key-value form with RC4 encryption

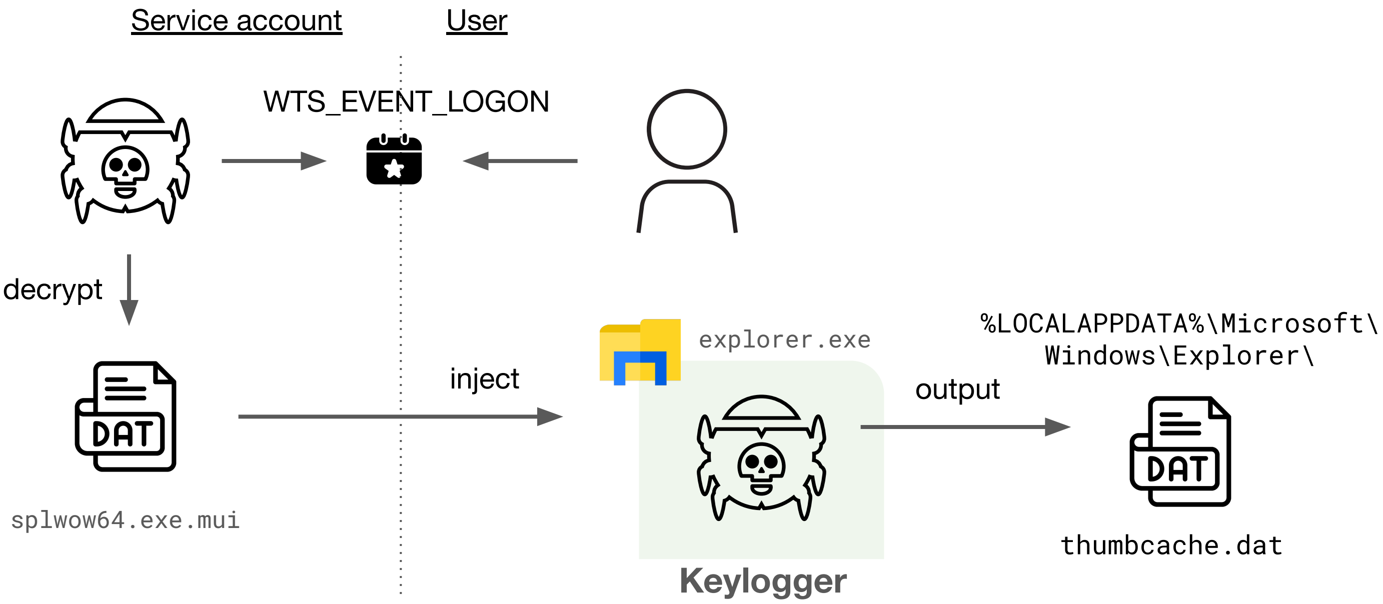
- ***id***: The victim identifier
- ***sl***: The Sleep duration time
- ***rm***: The C2 server hostname
- ***rp***: The C2 server port
- ***cacrt***: The CA certificate
- ***imcrt***: The client certificate
- ***imkey***: The client's private key



```
id:6F2111{sl:30{rm:safiasol.com{rp:443{cacrt:-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgICB+MwDQYJKoZIhvcNAQELBQAwTTEJMAcGA1UEBhMAMQkw
...
sT1b4tLlEOdGufEgWbgtvuSkX5moTj9qFKpMsuY=
-----END CERTIFICATE-----
{imcrt:-----BEGIN CERTIFICATE-----
MIIDnjCCAoagAwIBAgICBnowDQYJKoZIhvcNAQELBQAwTTEJMAcGA1UEBhMAMQkw
...
1vZ/Y6+iYejObgR/ZI0Dluzr
-----END CERTIFICATE-----
{imkey:-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAyL9x1B4JO+MVpdBZNCDJYo6BnPsd2aH3tGjJKQrr2bKdqbxy
...
JG0CSINJd3FmTxzKFnavrXpj0OwUtpva40qneYd+hxcylh0yrQ0129A=
-----END RSA PRIVATE KEY-----
{
```

Keylogger Module

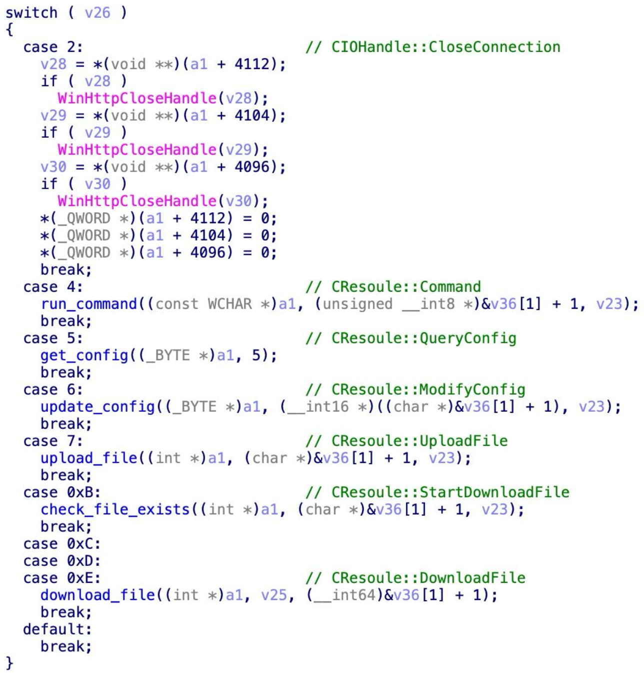
Gorem RAT monitors WTS_EVENT_LOGON event and injects user-mode keylogger module into every user session



Masol RAT (Windows)

Multi-architecture-support backdoor

- Possible earliest timeline is 2019
  - `E:\Masol_https190228\x64\Release\Masol.pdb`
- Potentially shared among multiple groups
  - Sophos reported the Linux version of Masol RAT (Backdr-NQ) in 2022
    - https://news.sophos.com/en-us/2022/10/19/covert-channels/
  - Sophos reported the Windows version of Masol RAT linked to Cluster Charlie in Crimson Palace
    - https://www.sophos.com/en-us/blog/crimson-palace-new-tools-tactics-targets
  - Trend Micro reported Earth Estries deployed Masol RAT in 2024
    - https://www.trendmicro.com/en_us/research/24/k/earth-estries.html
    - With note that Masol RAT is possibly not exclusive to Earth Estries

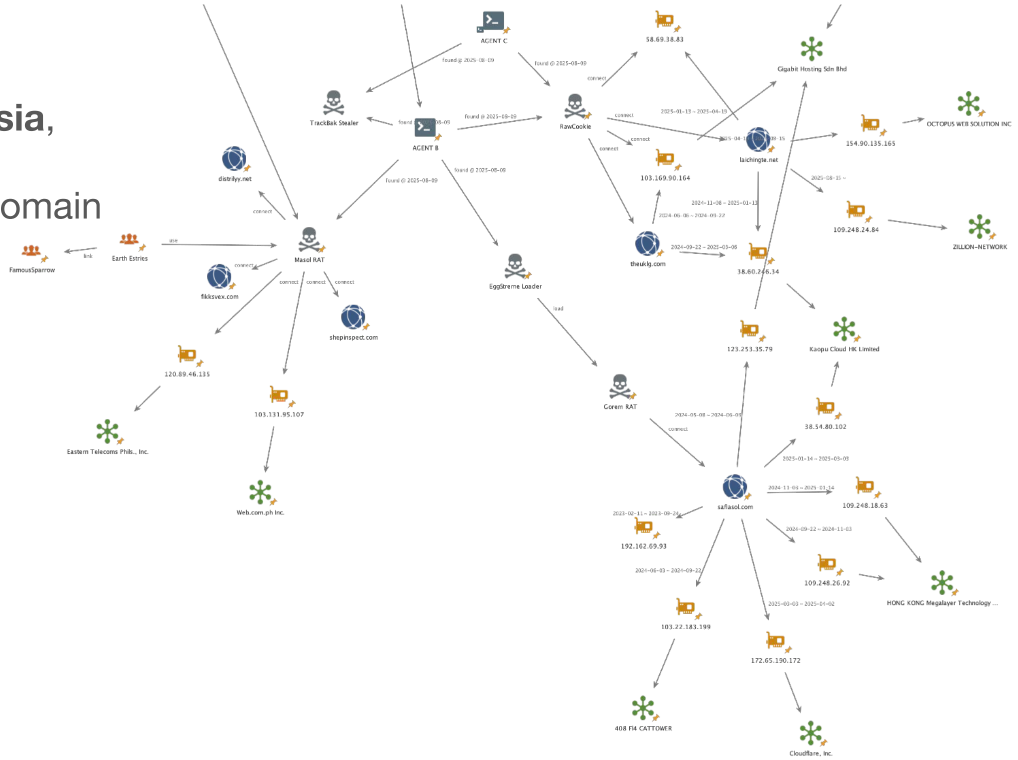


```
switch ( v26 )
{
  case 2:                          // CIOHandle::CloseConnection
    v28 = *(void **)(a1 + 4112);
    if ( v28 )
      WinHttpCloseHandle(v28);
    v29 = *(void **)(a1 + 4104);
    if ( v29 )
      WinHttpCloseHandle(v29);
    v30 = *(void **)(a1 + 4096);
    if ( v30 )
      WinHttpCloseHandle(v30);
    *(_QWORD *)(a1 + 4112) = 0;
    *(_QWORD *)(a1 + 4104) = 0;
    *(_QWORD *)(a1 + 4096) = 0;
    break;
  case 4:                          // CResoule::Command
    run_command((const WCHAR *)a1, (unsigned __int8 *)&v36[1] + 1, v23);
    break;
  case 5:                          // CResoule::QueryConfig
    get_config((_BYTE *)a1, 5);
    break;
  case 6:                          // CResoule::ModifyConfig
    update_config((_BYTE *)a1, (__int16 *)((char *)&v36[1] + 1), v23);
    break;
  case 7:                          // CResoule::UploadFile
    upload_file((int *)a1, (char *)&v36[1] + 1, v23);
    break;
  case 0xB:                        // CResoule::StartDownloadFile
    check_file_exists((int *)a1, (char *)&v36[1] + 1, v23);
    break;
  case 0xC:
  case 0xD:
  case 0xE:                        // CResoule::DownloadFile
    download_file((int *)a1, v25, (__int64)&v36[1] + 1);
    break;
  default:
    break;
}
```

Infrastructure

June 2024 ~

- No obvious overlaps with known groups
- Most of IPs locate in **Philippines** or **Malaysia**, which aligns with victim’s regions
- **Frequently changing IP** associated with domain

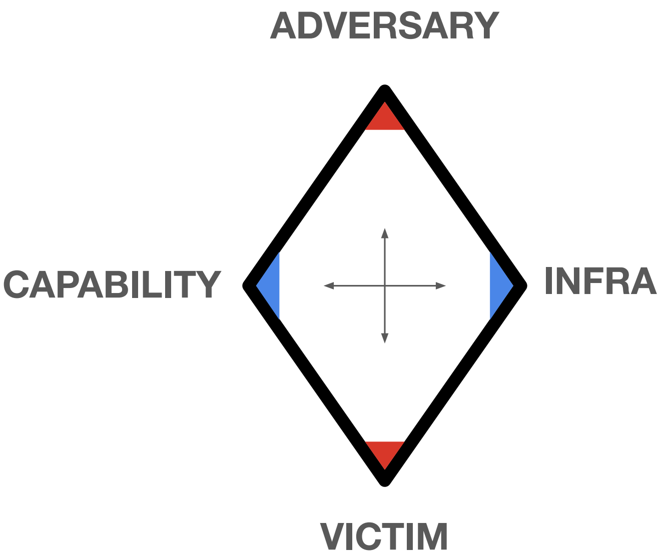


Potential Links with Known Groups

Masol RAT (Windows version) has been mentioned in reports associated with several China-linked groups in the past

- **Cluster Charlie of Crimson Palace** from the report in 2024 by Sophos
  - https://www.sophos.com/en-us/blog/crimson-palace-new-tools-tactics-targets
- **Earth Estries** from the report in 2024 by Trend Micro
  - https://www.trendmicro.com/en_us/research/24/k/earth-estries.html
  - Noted with low confidence

Diamond Model of CL-STA-1048

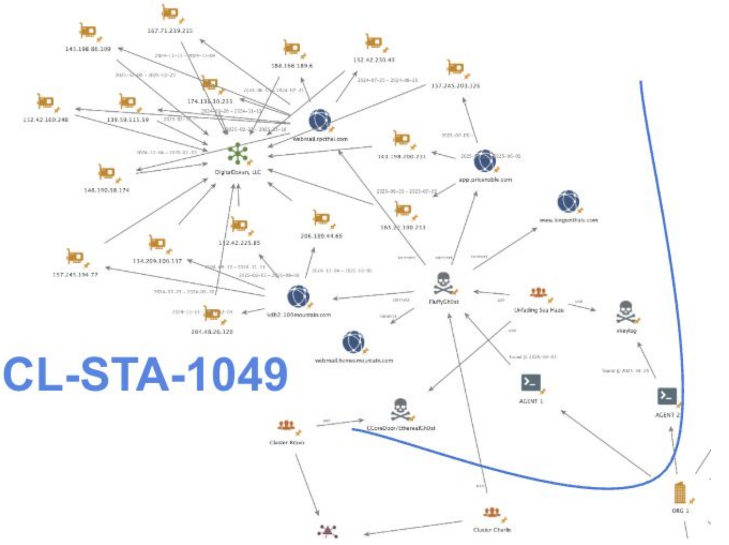


ADVERSARY	● China-aligned espionage motivated custer ● Possible link to Earth Estries and Cluster Charlie of Crimson Palace with low confidence
VICTIM	● South China Sea Area ● Philippines, Taiwan and Malaysia ● Military, Government and Research Institute
INFRASTRUCTURE	● Use domains and frequently change IP ● Various ASN ● Many IP located in Philippines and M
CAPABILITY	● DLL Sideloading ● Reuse of old samples (compiled in 2022-2023) ● Reuse of publicly available tools (libpeconv, DarkLoadLibrary, gRPC)

CL-STA-1049

Espionage motivated activity cluster targeting Philippines since at least March 2018

- Observed tools:
  - xleylog
  - Hypnosis Loader -> FluffyGh0st
  - InsidiousGh0st
- Based on the tool overlaps, we assume that this cluster links with the China-nexus group **Unfading Sea Haze** reported by Bitdefender in 2024
  - https://www.bitdefender.com/en-us/blog/businessinsights/deep-dive-into-unfading-sea-haze-a-new-threat-actor-in-the-south-china-sea

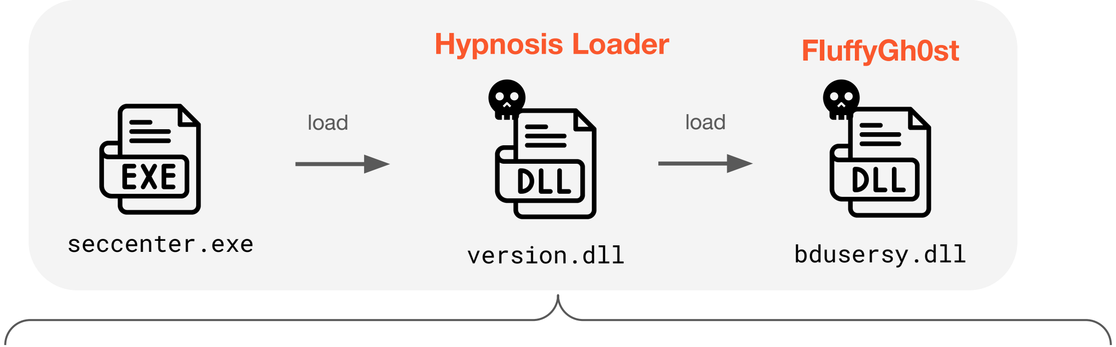


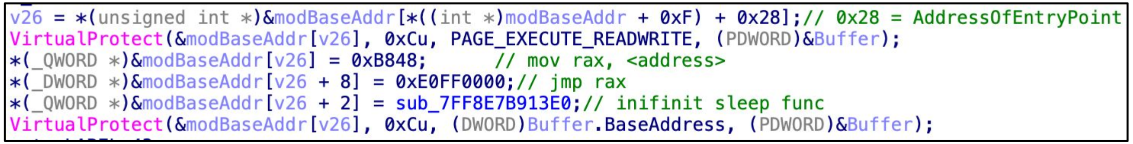
Hypnosis Loader

DLL Proxy-Sideloading leveraging adaptive DLL Sideloading technique

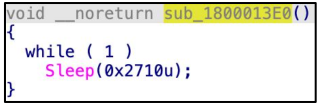
- The earliest ITW timeline is Dec 2023

C:\Program Files\Common Files\Bitdefender\SetupInformation\

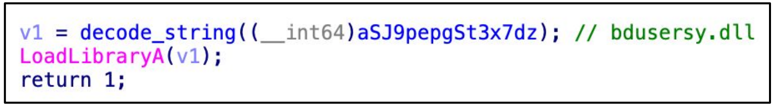




```
v26 = *(unsigned int *)&modBaseAddr[*((int *)modBaseAddr + 0xF) + 0x28];// 0x28 = AddressOfEntryPoint
VirtualProtect(&modBaseAddr[v26], 0xCu, PAGE_EXECUTE_READWRITE, (PDWORD)&Buffer);
*(_QWORD *)&modBaseAddr[v26] = 0xB848;       // mov rax, <address>
*(_DWORD *)&modBaseAddr[v26 + 8] = 0xE0FF0000;// jmp rax
*(_QWORD *)&modBaseAddr[v26 + 2] = sub_7FF8E7B913E0;// inifinit sleep func
VirtualProtect(&modBaseAddr[v26], 0xCu, (DWORD)Buffer.BaseAddress, (PDWORD)&Buffer);
```



```
void __noreturn sub_1800013E0()
{
  while ( 1 )
    Sleep(0x2710u);
}
```

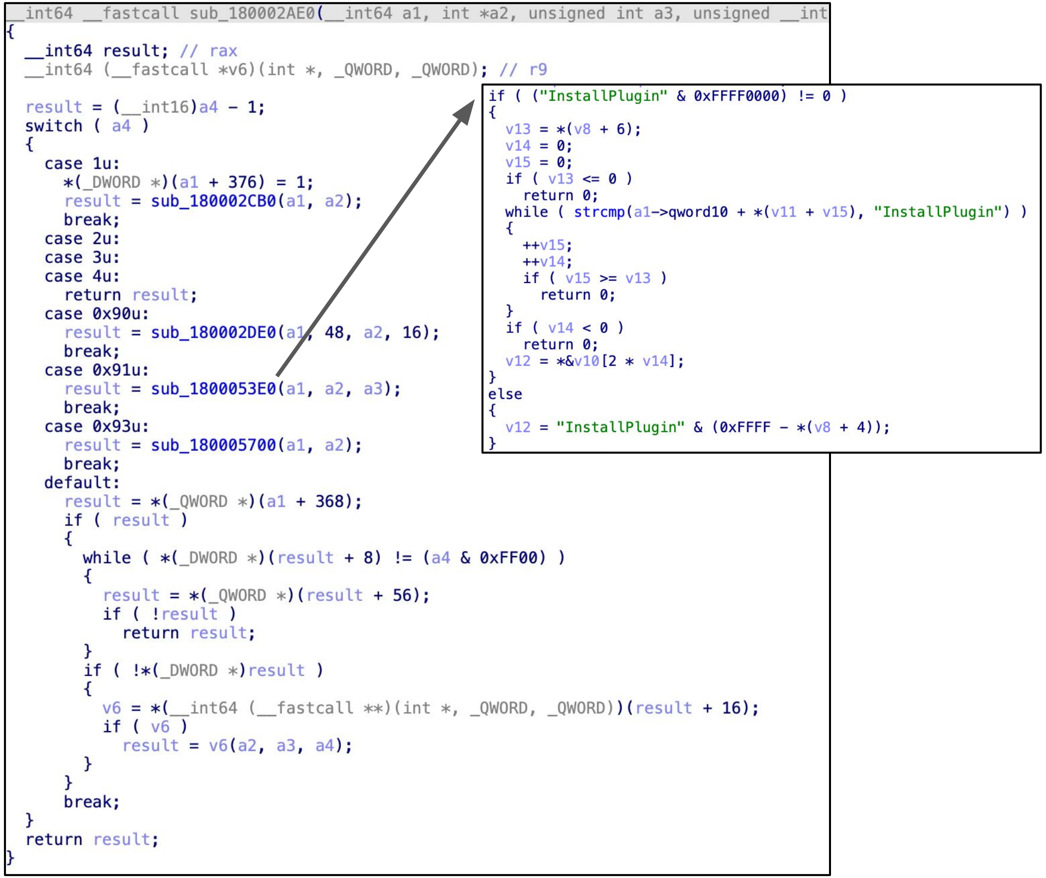


```
v1 = decode_string((__int64)aSJ9pepgSt3x7dz); // bdusersy.dll
LoadLibraryA(v1);
return 1;
```

FluffyGh0st

A variant of Gh0st RAT

- TLS over TCP for C2 communication
- Manipulating plugins received from C2
  - LZNT1 + RC4
  - “InstallPlugin” exported function



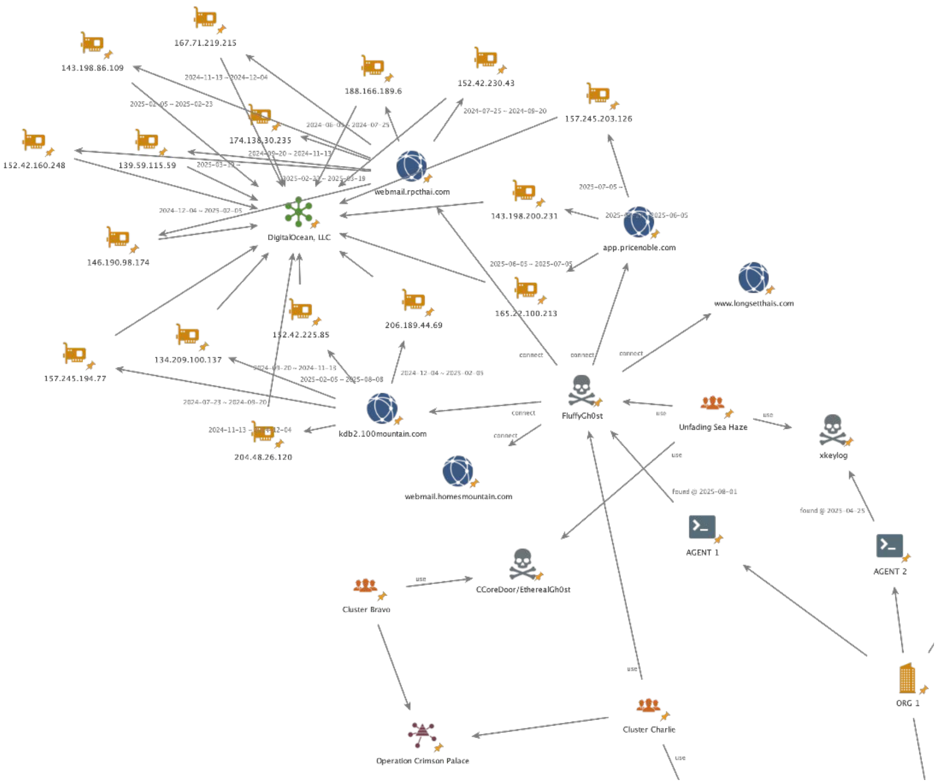
```
__int64 __fastcall sub_180002AE0(__int64 a1, int *a2, unsigned int a3, unsigned __int
{
  __int64 result; // rax
  __int64 (__fastcall *v6)(int *, _QWORD, _QWORD); // r9

  result = (__int16)a4 - 1;
  switch ( a4 )
  {
    case 1u:
      *(_DWORD *)(a1 + 376) = 1;
      result = sub_180002CB0(a1, a2);
      break;
    case 2u:
    case 3u:
    case 4u:
      return result;
    case 0x90u:
      result = sub_180002DE0(a1, 48, a2, 16);
      break;
    case 0x91u:
      result = sub_1800053E0(a1, a2, a3);
      break;
    case 0x93u:
      result = sub_180005700(a1, a2);
      break;
    default:
      result = *(_QWORD *)(a1 + 368);
      if ( result )
      {
        while ( *(_DWORD *)(result + 8) != (a4 & 0xFF00) )
        {
          result = *(_QWORD *)(result + 56);
          if ( !result )
            return result;
        }
        if ( !*(_DWORD *)result )
        {
          v6 = *(__int64 (__fastcall **)(int *, _QWORD, _QWORD))(result + 16);
          if ( v6 )
            result = v6(a2, a3, a4);
        }
      }
      break;
  }
  return result;
}
```

```
if ( ("InstallPlugin" & 0xFFFF0000) != 0 )
{
  v13 = *(v8 + 6);
  v14 = 0;
  v15 = 0;
  if ( v13 <= 0 )
    return 0;
  while ( strcmp(a1->qword10 + *(v11 + v15), "InstallPlugin") )
  {
    ++v15;
    ++v14;
    if ( v15 >= v13 )
      return 0;
  }
  if ( v14 < 0 )
    return 0;
  v12 = *&v10[2 * v14];
}
else
{
  v12 = "InstallPlugin" & (0xFFFF - *(v8 + 4));
}
```

Infrastructure

June 2024 ~

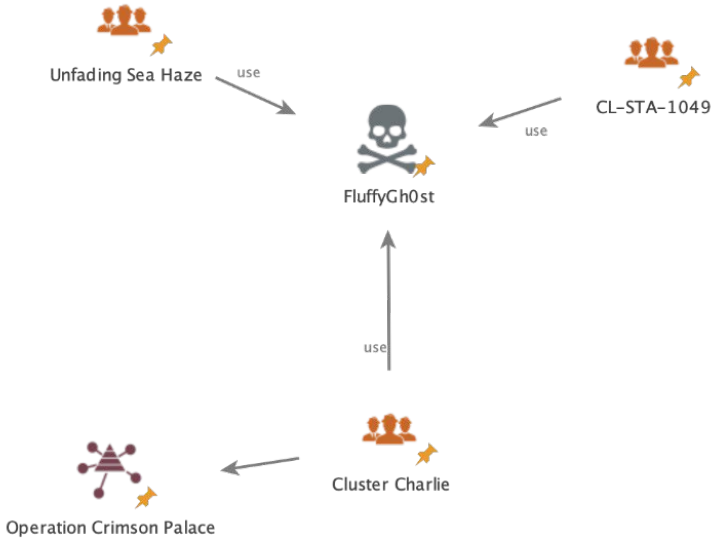
- Heavy use of **Digital Ocean**
- All of the observed IPs located in **Singapore**
- Frequently changing IP associated with domain



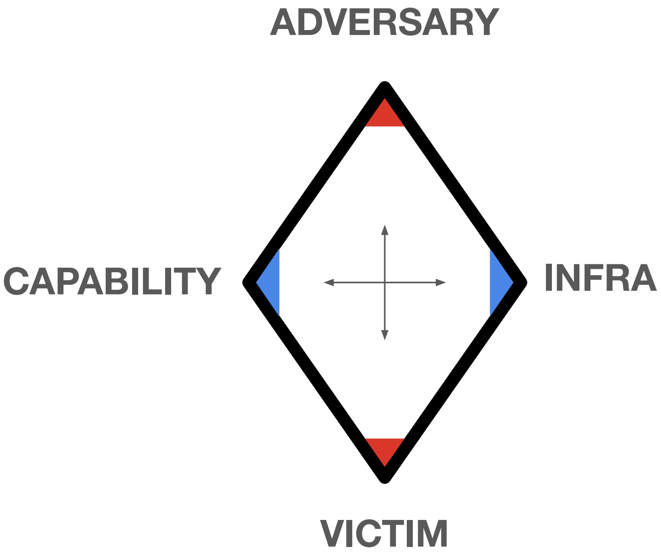
Potential Links with Known Groups

Actually, **FluffyGh0st** has also been mentioned in the report concerning other group

- Sophos included a hash of FluffyGh0st in their report about **Cluster Charlie** from **Crimson Palace** in 2024
    - https://www.sophos.com/en-us/blog/crimson-palace-new-tools-tactics-targets
    - Sha256: 58ed0463d4cb393cd09198a6409591b39cae06bb0ba5f5d760186de88410f6b8



Diamond Model of CL-STA-1049

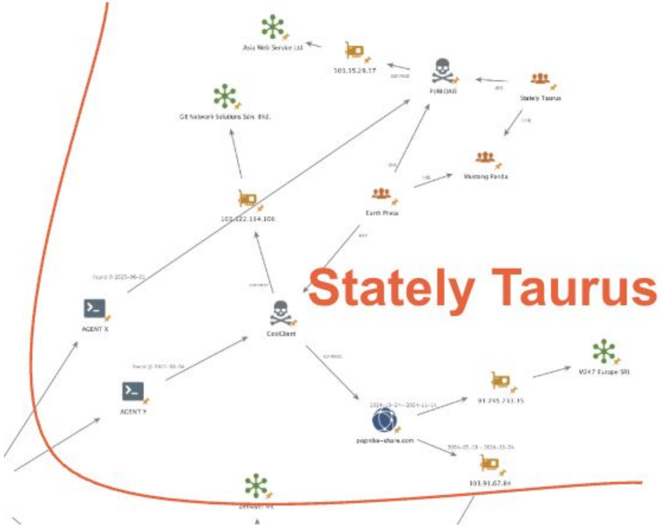


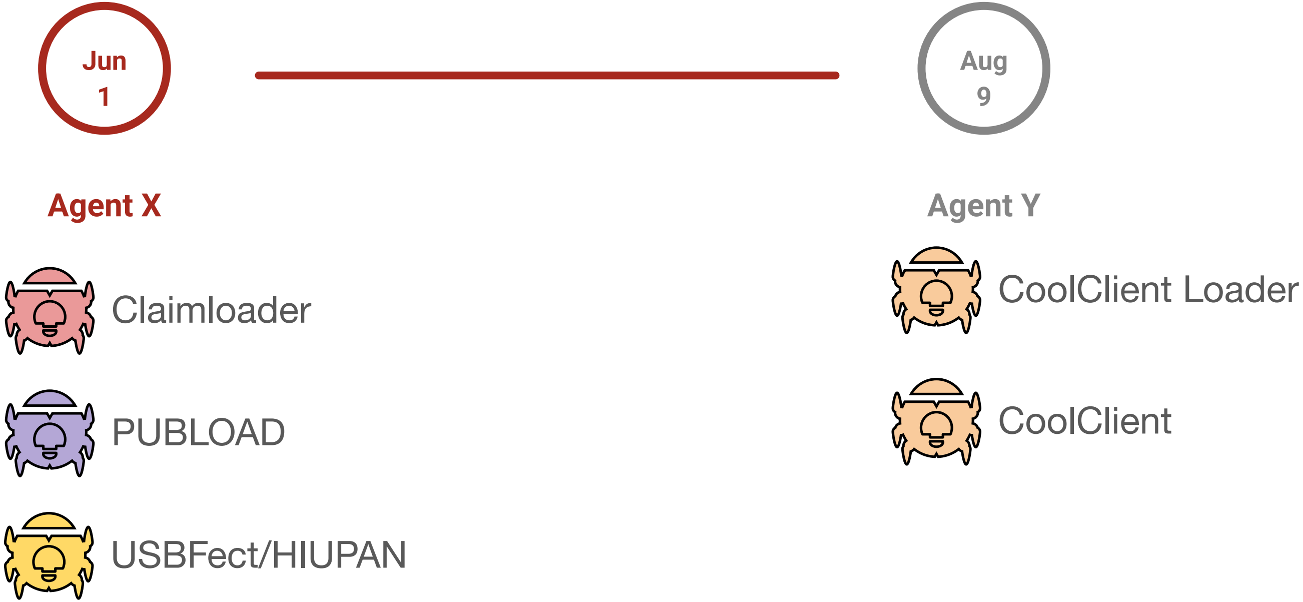
ADVERSARY	● China-aligned espionage motivated cluster ● Attribute to Unfading Sea Haze with high confidence ● Potential connection with Cluster Charlie of Crimson Palace
VICTIM	● South China Sea ● Military
INFRASTRUCTURE	● Use domains and frequently change IP ● Heavy use of Digital Ocean ● All the IP located in SG
CAPABILITY	● DLL Proxy-Sideloading / DLL Sideloading ● Reuse of old samples (compiled in 2021, 2023) ● Reuse of publicly available tools (OpenSSL, Gh0st RAT)

Stately Taurus

Espionage motivated threat actor aka Mustang Panda, Earth Preta

- Victimology
  - Philippines, Taiwan, Myanmar
- Observed Tools
  - HIUPAN/MISTCLOAK/USBFect
  - Variant of Claimloader -> PUBLOAD
  - CoolClient Loader -> CoolClient





Jun 1

Agent X

- Claimloader
- PUBLOAD
- USBFect/HIUPAN

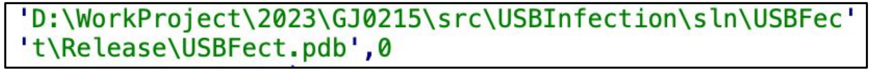
Aug 9

Agent Y

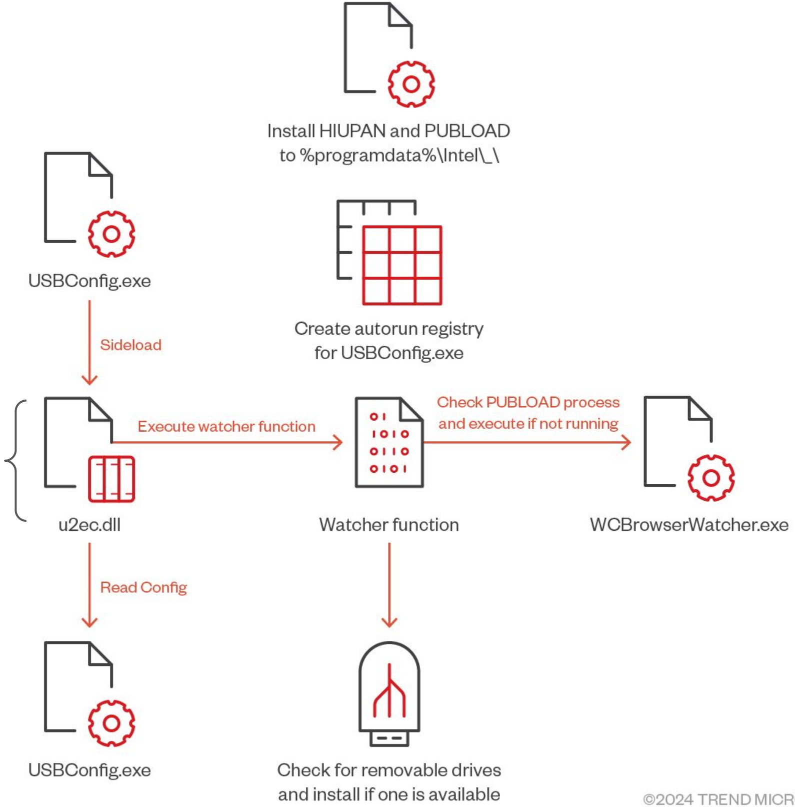
- CoolClient Loader
- CoolClient

USB-Wormable PUBLOAD

Earth Preta Evolves its Attacks with New Malware and Strategies
https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html

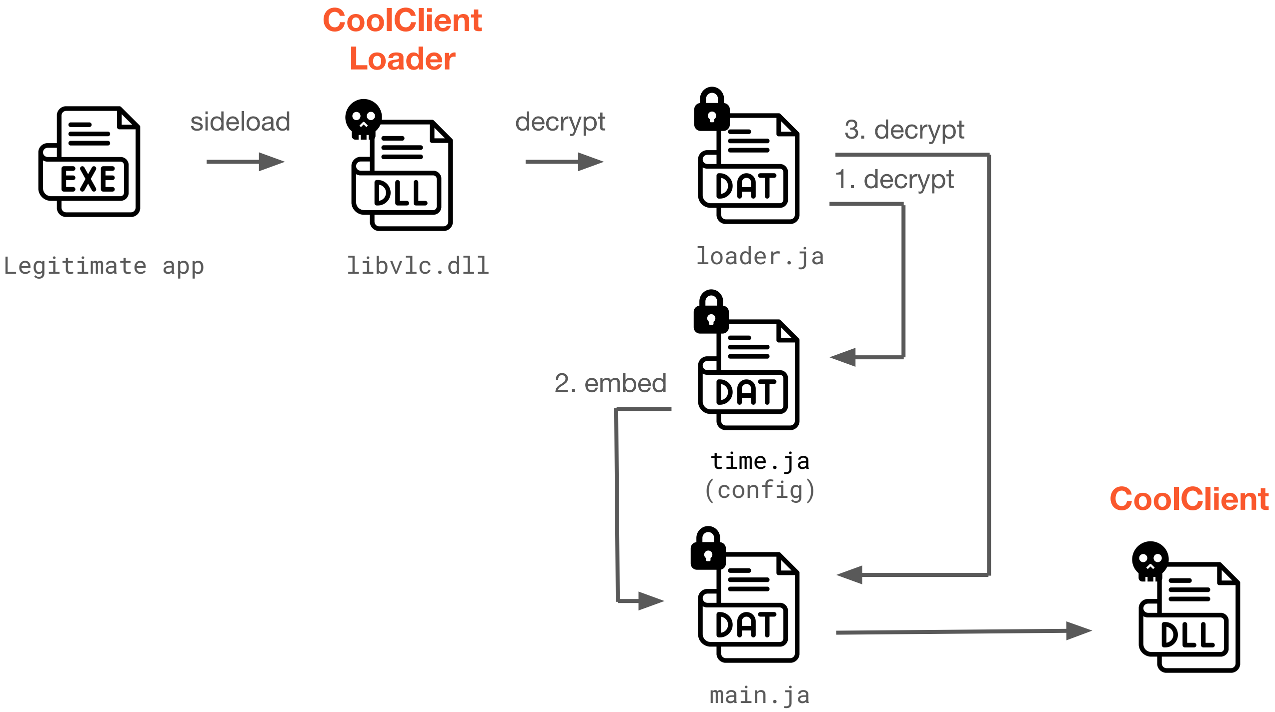


```
'D:\WorkProject\2023\GJ0215\src\USBInfection\sln\USBFec'
't\Release\USBFect.pdb',0
```



©2024 TREND MICRO

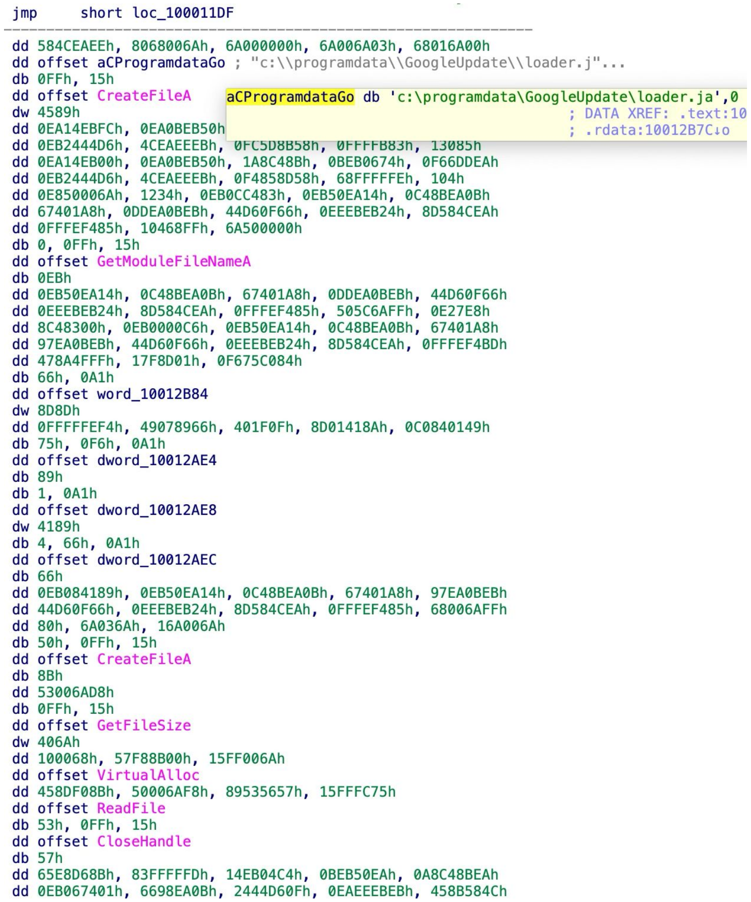
Infection Chain of CoolClient



CoolClient Loader

Multi-layered loader of CoolClient

- Earliest ITW timeline is June 2021
- Heavily employed **anti-disassembly technique**
- Sophos has already mentioned this loader in 2022 but no attribution
  - ○ https://news.sophos.com/en-us/2022/10/19/covert-channels/
- Trend Micro observed this loader during Earth Preta activity in 2023
  - ○ https://www.trendmicro.com/en_us/research/23/c/earth-preta-updated-stealthy-strategies.html

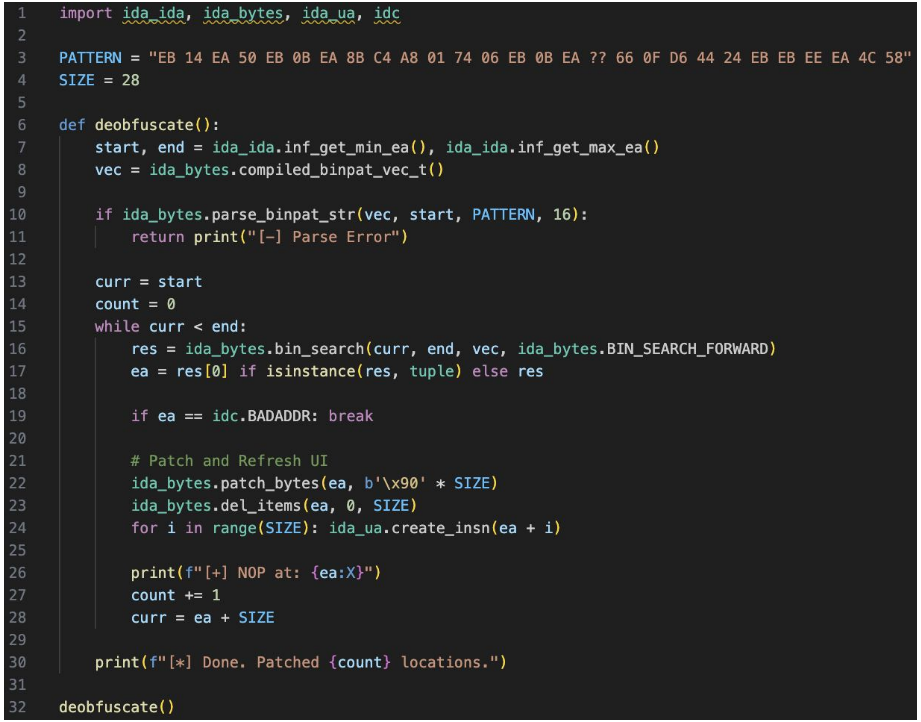


```
jmp     short loc_100011DF
-------------------------------------------------------------
dd 584CEAEEh, 8068006Ah, 6A000000h, 6A006A03h, 68016A00h
dd offset aCProgramdataGo ; "c:\\programdata\\GoogleUpdate\\loader.j"...
db 0FFh, 15h
dd offset CreateFileA
dw 4589h
dd 0EA14EBFCh, 0EA0BEB50h
dd 0EB2444D6h, 4CEAEEEBh, 0FC5D8B58h, 0FFFFB83h, 13085h
dd 0EA14EB00h, 0EA0BEB50h, 1A8C48Bh, 0BEB0674h, 0F66DDEAh
dd 0EB2444D6h, 4CEAEEEBh, 0F4858D58h, 68FFFFFEh, 104h
dd 0E850006Ah, 1234h, 0EB0CC483h, 0EB50EA14h, 0C48BEA0Bh
dd 67401A8h, 0DDEA0BEBh, 44D60F66h, 0EEEBEB24h, 8D584CEAh
dd 0FFFEF485h, 10468FFh, 6A500000h
db 0, 0FFh, 15h
dd offset GetModuleFileNameA
db 0EBh
dd 0EB50EA14h, 0C48BEA0Bh, 67401A8h, 0DDEA0BEBh, 44D60F66h
dd 0EEEBEB24h, 8D584CEAh, 0FFFEF485h, 505C6AFFh, 0E27E8h
dd 8C48300h, 0EB0000C6h, 0EB50EA14h, 0C48BEA0Bh, 67401A8h
dd 97EA0BEBh, 44D60F66h, 0EEEBEB24h, 8D584CEAh, 0FFFEF4BDh
dd 478A4FFFh, 17F8D01h, 0F675C084h
db 66h, 0A1h
dd offset word_10012B84
dw 8D8Dh
dd 0FFFFFEF4h, 49078966h, 401F0Fh, 8D01418Ah, 0C0840149h
db 75h, 0F6h, 0A1h
dd offset dword_10012AE4
db 89h
db 1, 0A1h
dd offset dword_10012AE8
dw 4189h
db 4, 66h, 0A1h
dd offset dword_10012AEC
db 66h
dd 0EB084189h, 0EB50EA14h, 0C48BEA0Bh, 67401A8h, 97EA0BEBh
dd 44D60F66h, 0EEEBEB24h, 8D584CEAh, 0FFFEF485h, 68006AFFh
dd 80h, 6A036Ah, 16A006Ah
db 50h, 0FFh, 15h
dd offset CreateFileA
db 8Bh
dd 53006AD8h
db 0FFh, 15h
dd offset GetFileSize
dw 406Ah
dd 100068h, 57F88B00h, 15FF006Ah
dd offset VirtualAlloc
dd 458DF08Bh, 50006AF8h, 89535657h, 15FFFC75h
dd offset ReadFile
db 53h, 0FFh, 15h
dd offset CloseHandle
db 57h
dd 65E8D68Bh, 83FFFFFDh, 14EB04C4h, 0BEB50EAh, 0A8C48BEAh
dd 0EB067401h, 6698EA0Bh, 2444D60Fh, 0EAEEEBEBh, 458B584Ch
```

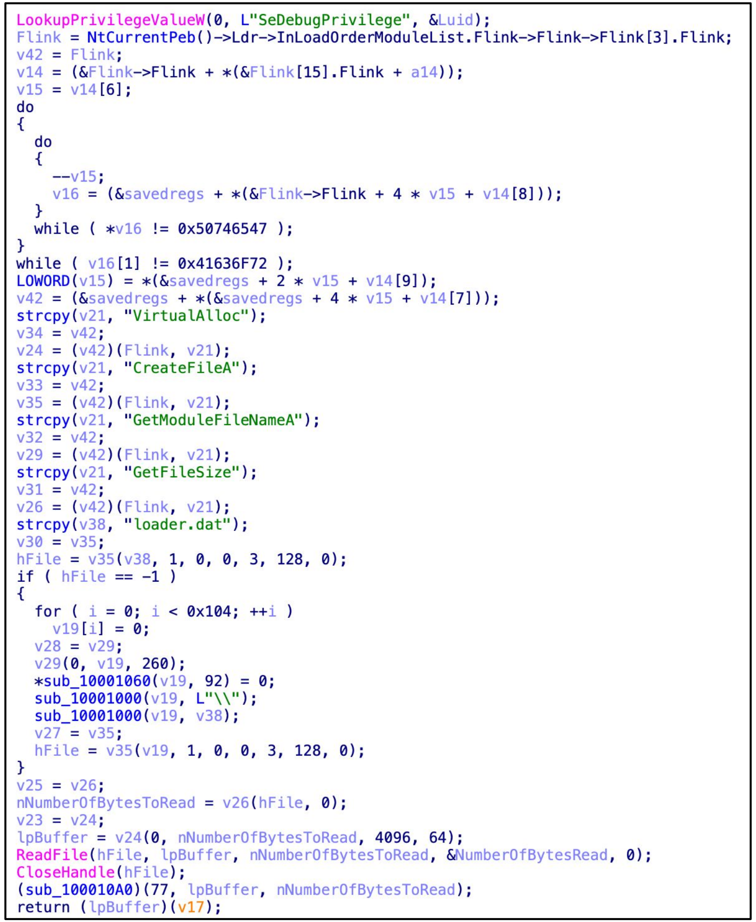
```
aCProgramdataGo db 'c:\programdata\GoogleUpdate\loader.ja',0
                                        ; DATA XREF: .text:10
                                        ; .rdata:10012B7C↓o
```

Deobfuscate CoolClient

Replace the block of anti-disassemble pattern with NOP



```python
import ida_ida, ida_bytes, ida_ua, idc

PATTERN = "EB 14 EA 50 EB 0B EA 8B C4 A8 01 74 06 EB 0B EA ?? 66 0F D6 44 24 EB EB EE EA 4C 58"
SIZE = 28

def deobfuscate():
    start, end = ida_ida.inf_get_min_ea(), ida_ida.inf_get_max_ea()
    vec = ida_bytes.compiled_binpat_vec_t()

    if ida_bytes.parse_binpat_str(vec, start, PATTERN, 16):
        return print("[-] Parse Error")

    curr = start
    count = 0
    while curr < end:
        res = ida_bytes.bin_search(curr, end, vec, ida_bytes.BIN_SEARCH_FORWARD)
        ea = res[0] if isinstance(res, tuple) else res

        if ea == idc.BADADDR: break

        # Patch and Refresh UI
        ida_bytes.patch_bytes(ea, b'\x90' * SIZE)
        ida_bytes.del_items(ea, 0, SIZE)
        for i in range(SIZE): ida_ua.create_insn(ea + i)

        print(f"[+] NOP at: {ea:X}")
        count += 1
        curr = ea + SIZE

    print(f"[*] Done. Patched {count} locations.")

deobfuscate()
```

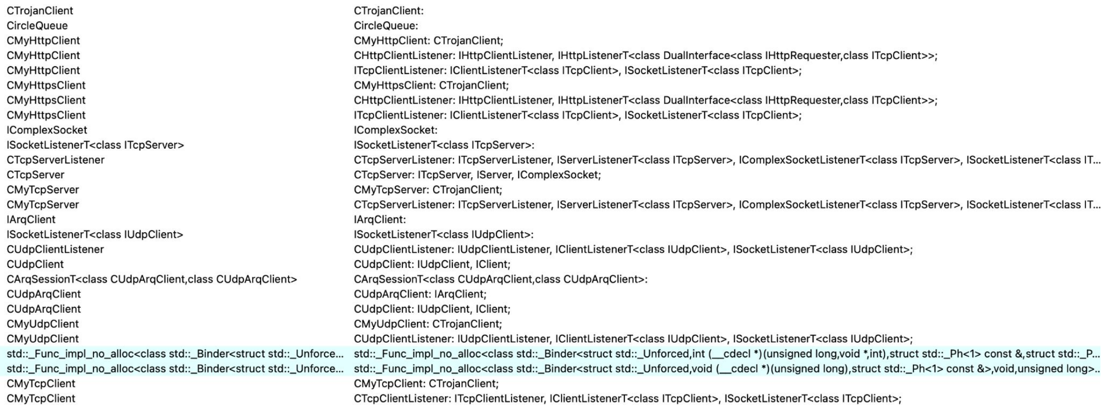


```c
LookupPrivilegeValueW(0, L"SeDebugPrivilege", &Luid);
Flink = NtCurrentPeb()->Ldr->InLoadOrderModuleList.Flink->Flink->Flink[3].Flink;
v42 = Flink;
v14 = (&Flink->Flink + *(&Flink[15].Flink + a14));
v15 = v14[6];
do
{
  do
  {
    --v15;
    v16 = (&savedregs + *(&Flink->Flink + 4 * v15 + v14[8]));
  }
  while ( *v16 != 0x50746547 );
}
while ( v16[1] != 0x41636F72 );
LOWORD(v15) = *(&savedregs + 2 * v15 + v14[9]);
v42 = (&savedregs + *(&savedregs + 4 * v15 + v14[7]));
strcpy(v21, "VirtualAlloc");
v34 = v42;
v24 = (v42)(Flink, v21);
strcpy(v21, "CreateFileA");
v33 = v42;
v35 = (v42)(Flink, v21);
strcpy(v21, "GetModuleFileNameA");
v32 = v42;
v29 = (v42)(Flink, v21);
strcpy(v21, "GetFileSize");
v31 = v42;
v26 = (v42)(Flink, v21);
strcpy(v38, "loader.dat");
v30 = v35;
hFile = v35(v38, 1, 0, 0, 3, 128, 0);
if ( hFile == -1 )
{
  for ( i = 0; i < 0x104; ++i )
    v19[i] = 0;
  v28 = v29;
  v29(0, v19, 260);
  *sub_10001060(v19, 92) = 0;
  sub_10001000(v19, L"\\");
  sub_10001000(v19, v38);
  v27 = v35;
  hFile = v35(v19, 1, 0, 0, 3, 128, 0);
}
v25 = v26;
nNumberOfBytesToRead = v26(hFile, 0);
v23 = v24;
lpBuffer = v24(0, nNumberOfBytesToRead, 4096, 64);
ReadFile(hFile, lpBuffer, nNumberOfBytesToRead, &NumberOfBytesRead, 0);
CloseHandle(hFile);
(sub_100010A0)(77, lpBuffer, nNumberOfBytesToRead);
return (lpBuffer)(v17);
```

CoolClient

Multi-protocol supporting backdoor written in C++

- Built on top of HP-Socket library
  - ○ https://github.com/ldcsaa/HP-Socket
- Probably designed for lateral movement agent
- Features
  - ○ Upload/delete a file
  - ○ Tunnel packets
  - ○ Start keylogging
  - ○ Send portmap information

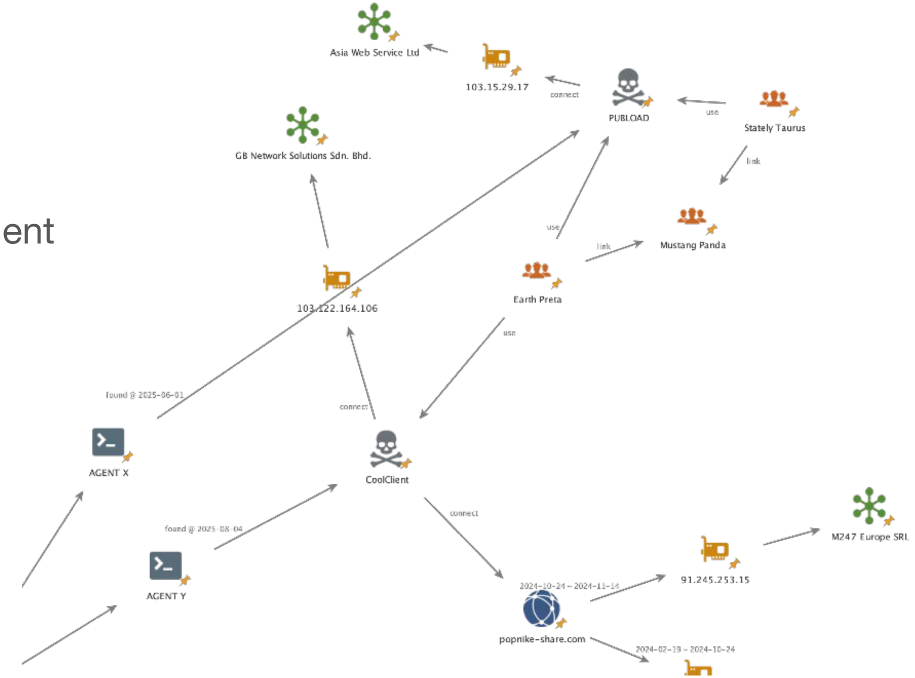


```
CTrojanClient                                                        CTrojanClient:
CircleQueue                                                          CircleQueue:
CMyHttpClient                                                        CMyHttpClient: CTrojanClient;
CMyHttpClient                                                        CHttpClientListener: IHttpClientListener, IHttpListenerT<class DualInterface<class IHttpRequester,class ITcpClient>>;
CMyHttpClient                                                        ITcpClientListener: IClientListenerT<class ITcpClient>, ISocketListenerT<class ITcpClient>;
CMyHttpsClient                                                       CMyHttpsClient: CTrojanClient;
CMyHttpsClient                                                       CHttpClientListener: IHttpClientListener, IHttpListenerT<class DualInterface<class IHttpRequester,class ITcpClient>>;
CMyHttpsClient                                                       ITcpClientListener: IClientListenerT<class ITcpClient>, ISocketListenerT<class ITcpClient>;
IComplexSocket                                                       IComplexSocket:
ISocketListenerT<class ITcpServer>                                   ISocketListenerT<class ITcpServer>:
CTcpServerListener                                                   CTcpServerListener: ITcpServerListener, IServerListenerT<class ITcpServer>, IComplexSocketListenerT<class ITcpServer>, ISocketListenerT<class IT...
CTcpServer                                                           CTcpServer: ITcpServer, IServer, IComplexSocket;
CMyTcpServer                                                         CMyTcpServer: CTrojanClient;
CMyTcpServer                                                         CTcpServerListener: ITcpServerListener, IServerListenerT<class ITcpServer>, IComplexSocketListenerT<class ITcpServer>, ISocketListenerT<class IT...
IArqClient                                                           IArqClient:
ISocketListenerT<class IUdpClient>                                   ISocketListenerT<class IUdpClient>:
CUdpClientListener                                                   CUdpClientListener: IUdpClientListener, IClientListenerT<class IUdpClient>, ISocketListenerT<class IUdpClient>;
CUdpClient                                                           CUdpClient: IUdpClient, IClient;
CArqSessionT<class CUdpArqClient,class CUdpArqClient>                CArqSessionT<class CUdpArqClient,class CUdpArqClient>:
CUdpArqClient                                                        CUdpArqClient: IArqClient;
CUdpArqClient                                                        CUdpClient: IUdpClient, IClient;
CMyUdpClient                                                         CMyUdpClient: CTrojanClient;
CMyUdpClient                                                         CUdpClientListener: IUdpClientListener, IClientListenerT<class IUdpClient>, ISocketListenerT<class IUdpClient>;
std::_Func_impl_no_alloc<class std::_Binder<struct std::_Unforce...  std::_Func_impl_no_alloc<class std::_Binder<struct std::_Unforced,int (__cdecl *)(unsigned long,void *,int),struct std::_Ph<1> const &,struct std::_P...
std::_Func_impl_no_alloc<class std::_Binder<struct std::_Unforce...  std::_Func_impl_no_alloc<class std::_Binder<struct std::_Unforced,void (__cdecl *)(unsigned long),struct std::_Ph<1> const &>,void,unsigned long>..
CMyTcpClient                                                         CMyTcpClient: CTrojanClient;
CMyTcpClient                                                         CTcpClientListener: ITcpClientListener, IClientListenerT<class ITcpClient>, ISocketListenerT<class ITcpClient>;
```

Infrastructure

Feb 2024 ~

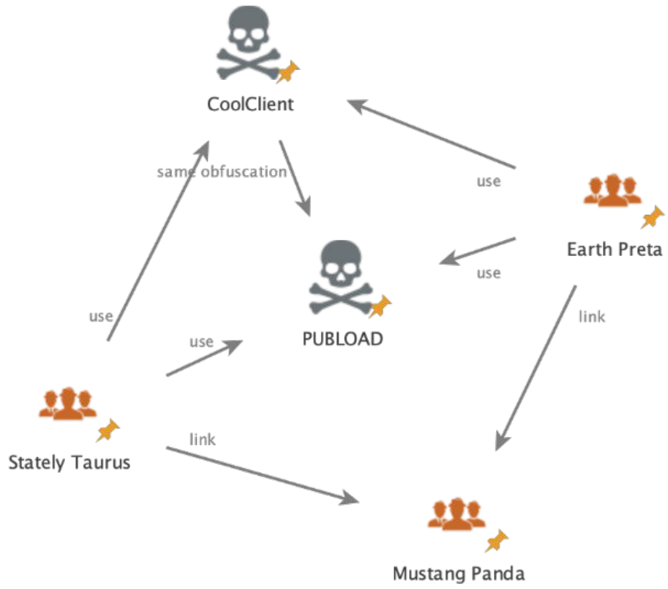
- PUBLOAD keeps using the same IP
- No obvious overlaps in infrastructures of CoolClient
- IPs location in **Singapore** and **Malaysia**



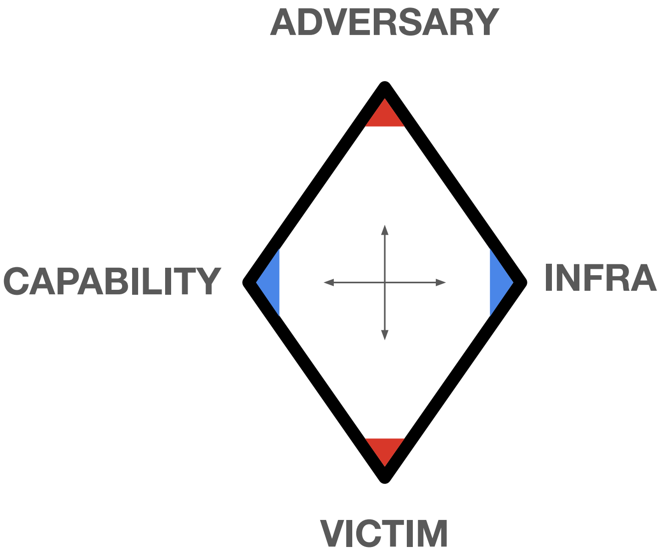
Connections

We concluded to attribute this activity to the existing threat actor **Stately Taurus**, which links to Mustang Panda / Earth Preta

- Technically we haven't observed execution link between PUBLOAD and CoolClient
    - Trend Micro reported that CoolClient was deployed after PUBLOAD infection
- However, **HIUPAN/USBFect and CoolClient Loader share the exact same obfuscation technique**
- This indicates that the operator(s) behind HIUPAN/USBFect and CoolClient should have codebase-level connection, which supports our attribution that this activity belongs to Stately Taurus



Diamond Model of Stately Taurus



ADVERSARY	● Espionage motivated threat actor ● aka Mustang Panda, Earth Preta ● Attribute to China-nexus with high confidence
VICTIM	● Philippines, Taiwan, Myanmar and Mongolia
INFRASTRUCTURE	● IPs located in Singapore and Malaysia
CAPABILITY	● DLL Sideloading ● Reuse of old samples (compiled in 2021, 2023) ● Reuse of publicly available tools (HP-Socket)

Attribution

Clustering

Infrastructure (e.g., IP addresses, domains, URLs)

Capabilities (e.g., malware, tools, TTPs)

Victims and targeting (e.g., organizations, industries, regions, temporal overlaps)

Evaluation

Source verification

Indicator validity

TTP consistency

Victim analysis

Estimating confidence assessments

Admiralty System

The Admiralty System provides the possible values for source reliability and information credibility

Rating	Keywords
A	Reliable
B	Usually reliable
C	Fairly reliable
D	Not usually reliable
E	Unreliable
F	Reliability unknown

Information Credibility

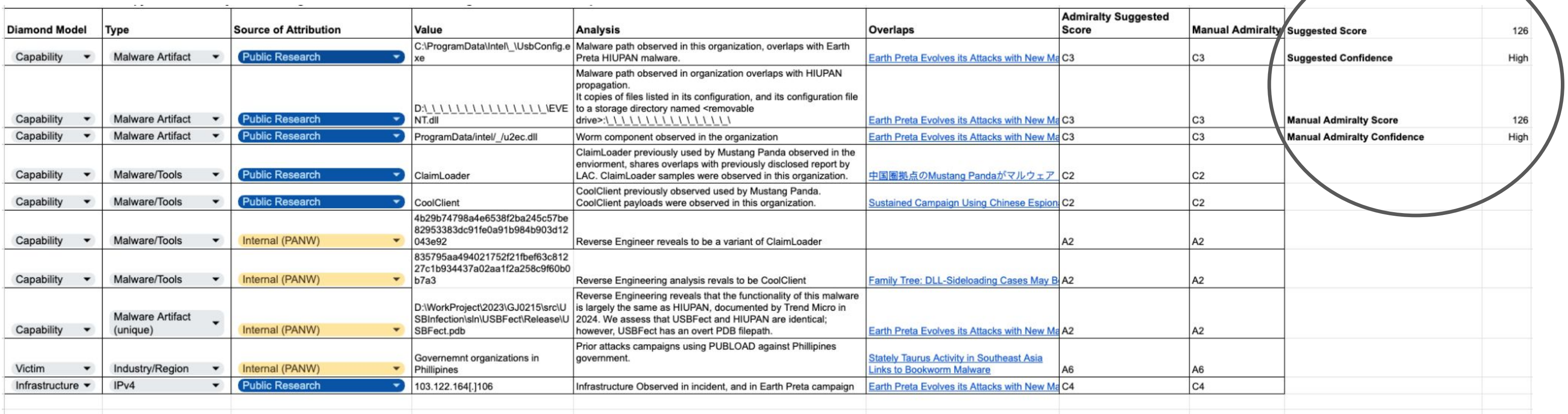
Information credibility can range between 1-6 and is assessed separately from the source’s reliability

Rating	Keywords
1	Confirmed
2	Probably true
3	Possibly true
4	Doubtfully True
5	Improbable
6	Difficult to say

Attribution in Action

We are measuring if Earth Petra is Stately Taurus, and our confidence level.

We input the values observed in our investigation, and identify overlaps to establish a confidence level, based on Source of Attribution and evidence observed.



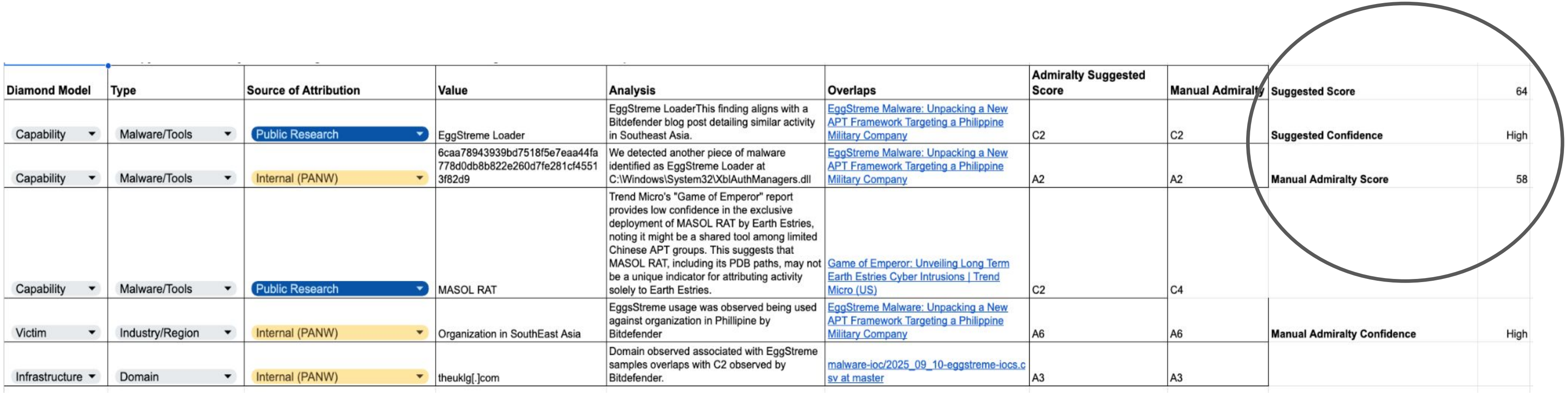
Diamond Model	Type	Source of Attribution	Value	Analysis	Overlaps	Admiralty Suggested Score	Manual Admiralty
Capability	Malware Artifact	Public Research	C:\ProgramData\Intel_\UsbConfig.exe	Malware path observed in this organization, overlaps with Earth Preta HIUPAN malware.	Earth Preta Evolves its Attacks with New Ma	C3	C3
Capability	Malware Artifact	Public Research	D:\________________\EVENT.dll	Malware path observed in organization overlaps with HIUPAN propagation. It copies of files listed in its configuration, and its configuration file to a storage directory named <removable drive>:________________\	Earth Preta Evolves its Attacks with New Ma	C3	C3
Capability	Malware Artifact	Public Research	ProgramData/intel/_/u2ec.dll	Worm component observed in the organization	Earth Preta Evolves its Attacks with New Ma	C3	C3
Capability	Malware/Tools	Public Research	ClaimLoader	ClaimLoader previously used by Mustang Panda observed in the enviorment, shares overlaps with previously disclosed report by LAC. ClaimLoader samples were observed in this organization.	中国圏拠点のMustang Pandaがマルウェア	C2	C2
Capability	Malware/Tools	Public Research	CoolClient	CoolClient previously observed used by Mustang Panda. CoolClient payloads were observed in this organization.	Sustained Campaign Using Chinese Espion	C2	C2
Capability	Malware/Tools	Internal (PANW)	4b29b74798a4e6538f2ba245c57be82953383dc91fe0a91b984b903d12043e92	Reverse Engineer reveals to be a variant of ClaimLoader		A2	A2
Capability	Malware/Tools	Internal (PANW)	835795aa494021752f21fbef63c81227c1b934437a02aa1f2a258c9f60b0b7a3	Reverse Engineering analysis revals to be CoolClient	Family Tree: DLL-Sideloading Cases May B	A2	A2
Capability	Malware Artifact (unique)	Internal (PANW)	D:\WorkProject\2023\GJ0215\src\USBInfection\sln\USBFect\Release\USBFect.pdb	Reverse Engineering reveals that the functionality of this malware is largely the same as HIUPAN, documented by Trend Micro in 2024. We assess that USBFect and HIUPAN are identical; however, USBFect has an overt PDB filepath.	Earth Preta Evolves its Attacks with New Ma	A2	A2
Victim	Industry/Region	Internal (PANW)	Governemnt organizations in Phillipines	Prior attacks campaigns using PUBLOAD against Phillipines government.	Stately Taurus Activity in Southeast Asia Links to Bookworm Malware	A6	A6
Infrastructure	IPv4	Public Research	103.122.164[.]106	Infrastructure Observed in incident, and in Earth Preta campaign	Earth Preta Evolves its Attacks with New Ma	C4	C4

Suggested Score	126
Suggested Confidence	High
Manual Admiralty Score	126
Manual Admiralty Confidence	High

Cluster Attribution

We adjusted the Admiralty Level of the MASOL RAT finding, since it may not be exclusive to group.

This allows us to understand that CL-STA-1048 with high confidence (with a score of 64) is responsible for the campaign observed by BitDefender.



Diamond Model	Type	Source of Attribution	Value	Analysis	Overlaps	Admiralty Suggested Score	Manual Admiralty	Suggested Score	64
Capability	Malware/Tools	Public Research	EggStreme Loader	EggStreme LoaderThis finding aligns with a Bitdefender blog post detailing similar activity in Southeast Asia.	EggStreme Malware: Unpacking a New APT Framework Targeting a Philippine Military Company	C2	C2	Suggested Confidence	High
Capability	Malware/Tools	Internal (PANW)	6caa78943939bd7518f5e7eaa44fa778d0db8b822e260d7fe281cf45513f82d9	We detected another piece of malware identified as EggStreme Loader at C:\Windows\System32\XblAuthManagers.dll	EggStreme Malware: Unpacking a New APT Framework Targeting a Philippine Military Company	A2	A2	Manual Admiralty Score	58
Capability	Malware/Tools	Public Research	MASOL RAT	Trend Micro's "Game of Emperor" report provides low confidence in the exclusive deployment of MASOL RAT by Earth Estries, noting it might be a shared tool among limited Chinese APT groups. This suggests that MASOL RAT, including its PDB paths, may not be a unique indicator for attributing activity solely to Earth Estries.	Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions | Trend Micro (US)	C2	C4		
Victim	Industry/Region	Internal (PANW)	Organization in SouthEast Asia	EggsStreme usage was observed being used against organization in Phillipine by Bitdefender	EggStreme Malware: Unpacking a New APT Framework Targeting a Philippine Military Company	A6	A6	Manual Admiralty Confidence	High
Infrastructure	Domain	Internal (PANW)	theuklg[.]com	Domain observed associated with EggStreme samples overlaps with C2 observed by Bitdefender.	malware-ioc/2025_09_10-eggstreme-iocs.csv at master	A3	A3		

Conclusion

Takeaways

- We introduced a unique case study that involved multiple clusters/actors targeting a single organization
- Our investigation highlighted an emerging trend that espionage campaigns targeting a specific region or organizations may be conducted by distinct clusters/actors using different tools and infrastructures but the same motivation
  - Trend Micro calls this new approach “Premier Pass-as-a-Service”
- (For researchers) Review a rule in your organization to define the process of attribution

IoC

SHA256

```
34bf325492614dd4d842ec24f22a402ab73908cb91a74846945eae4775290ff2
11c7728697d5ea11c592fee213063c6369340051157f71ddc7ca891f5f367720
58ed0463d4cb393cd09198a6409591b39cae06bb0ba5f5d760186de88410f6b8
c47d55ad95a6c6ffac45c2b205e03bddadf5e36f55988599053b1fd0e49448a5
f07b2af21e3fab6af5166a44ca77ed0ebc7c9a3e623202a63d4c4492abce8d65
4e26aa1bb28874f0897ab9a08e61d4b99caaa395fe63cbe4398f7297371e388c
74e7093615da36b28effb3aa6eef5a31e7ea59627bd619b488f087091e8d65e9
84e37e42312b9a502c40cf1f3fc181e3ebd4f3e35c58bbf182740dfe38d3b6b9
05995284b59ad0066350f43517382228f7eee63cd297e787b2a271f69ecf2dfc
6caa78943939bd7518f5e7eaa44fa778d0db8b822e260d7fe281cf45513f82d9
e61a1f4269e934481f6cb19576b3dbc434952b01445fd4e1ebc6906a1b449ef8
1aa37a477c539edf25656a300002a28d4246ec83344422dd705b42d3443a2623
07bd506d2a8db98c2478ac11bb6c46d84f1aa84f4a9af643804ed857ad7399c3
6745422717f0ccdf2ae3330d133945268d4cd21215adcf982400d82b38ebeeca
29d4cc64c7c9b7ecd16d96e9c6dcde1fe22a4c2d202074aadf41cbcef494bc19
e9b52577091c8e25e91c485216de34d5a26ab707a10b1e5cd31ed7aa055939d3
21fe238c462b2f22a7e97f1f06e4f12e8c6e5f3a6fffe671b671909b501fa537
e1672dab0daf1c84f14f7bb827851c27753da067490e10cd6144fe7873892fec
d4d753c6ea5c86a44c9a65cd0d4eaeabb072b19e0ef68ef7da3a879f689772c9
f62223c9750fb2edfd979a8cae204cb9ce5e0950b52a47b62f195cd05dd3e2fb
2616dfadf8aa222303269eb7202c75e2a8fc5b05b6b63ae2cb7576b9a27733f9
6f4f76c7a2638087a0da6002cd2c76d1673305b1e850a1f4068f14755f59d45b
4b29b74798a4e6538f2ba245c57be82953383dc91fe0a91b984b903d12043e92
83f06fa37f1136f765f799851812f11060ab34df3b34bc61777acc59a30b4c6e
851d57a2bf514202f54dafa1eb83a862653be7512b6e9535914b8d1d719d495f
835795aa494021752f21fbef63c81227c1b934437a02aa1f2a258c9f60b0b7a3
```

IP/Domain

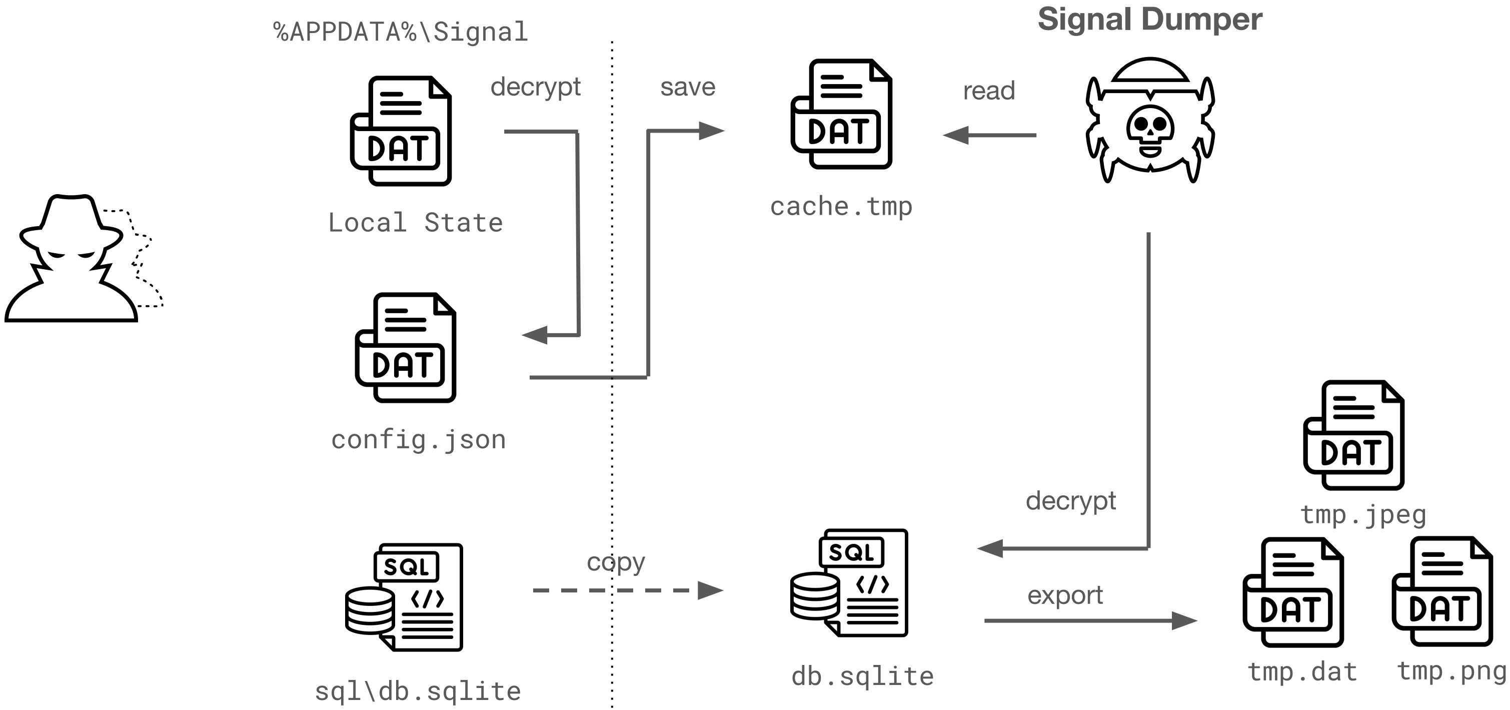
```
120.89.46[.]135
103.131.95[.]107
109.248.24[.]177
103.122.164[.]106
103.15.29[.]17

fikksvex[.]com
laichingte[.]net
theuklg[.]com
shepinspect[.]com
distrilyy[.]net
popnike-share[.]com
webmail[.]homesmountain[.]com
webmail[.]rpcthai[.]com
```

Thank You

paloaltonetworks.com

Signal Dumper

Signal message attachments export tool using the documented technique - https://www.sciencedirect.com/science/article/pii/S2666281725000800


%APPDATA%\Signal
Signal Dumper
decrypt
save
read
Local State
cache.tmp
config.json
tmp.jpeg
decrypt
copy
export
sql\db.sqlite
db.sqlite
tmp.dat
tmp.png