UNC6384 Weaponizes ZDI-CAN-25373 Vulnerability to Deploy PlugX Against Hungarian and Belgian Diplomatic Entities

by Arctic Wolf Labs ⋮ ⋮ 10/30/2025

Threat Actor Name: UNC6384
Targeted Industries: Government, Diplomatic Services
Geographic Focus: Hungary, Belgium, Serbia, Italy, Netherlands (broader European diplomatic community)

Executive Summary

Arctic Wolf Labs has identified an active cyber espionage campaign by Chinese-affiliated threat actor UNC6384 targeting European diplomatic entities in Hungary, Belgium, and additional European nations during September and October 2025. The campaign represents a tactical evolution incorporating the exploitation of ZDI-CAN-25373, a Windows shortcut vulnerability disclosed in March 2025, alongside refined social engineering leveraging authentic diplomatic conference themes.

The attack chain begins with spearphishing emails containing an embedded URL that is the first of several stages that lead to the delivery of malicious LNK files themed around European Commission meetings, NATO-related workshops, and multilateral diplomatic coordination events. These files exploit the recently disclosed Windows vulnerability to execute obfuscated PowerShell commands that extract and deploy a multi-stage malware chain, culminating in PlugX remote access trojan (RAT) deployment through DLL side-loading of legitimate signed Canon printer assistant utilities.

This campaign demonstrates UNC6384's capability for rapid vulnerability adoption within six months of public disclosure, advanced social engineering leveraging detailed knowledge of diplomatic calendars and event themes, and operational expansion from traditional Southeast Asia targeting to European diplomatic entities. The threat actor maintains multiple parallel operational approaches, including the captive portal hijacking methodology documented by the Google Threat Intelligence Group alongside the direct spearphishing approach observed by Arctic Wolf Labs.

Arctic Wolf Labs assesses with high confidence that this campaign is attributable to UNC6384. This attribution is based on multiple converging lines of evidence including malware tooling, tactical procedures, targeting alignment, and infrastructure overlaps with previously documented UNC6384 operations.

Key Findings:

- UNC6384 rapidly adopted the ZDI-CAN-25373 Windows vulnerability within six months of its March 2025 disclosure.
- This campaign targets Hungarian and Belgian diplomatic entities, with expansion across the broader European diplomatic community.

- Social engineering leverages diplomatic conference details including European Commission border facilitation meetings and NATO defense procurement workshops.
- The multi-stage attack chain employs DLL side-loading of legitimate signed Canon printer utilities.
- PlugX malware deployed via in-memory execution establishes a persistent remote-access capability within targeted environments, enabling covert intelligence collection.
- C2 infrastructure includes racineupci[.]org, dorareco[.]net, naturadeco[.]net, and additional domains.
- The CanonStager loader evolved from approximately 700KB to 4KB in size between September and October 2025, indicating active development.

Introducing UNC6384

UNC6384 is a Chinese-affiliated cyber espionage threat actor recently documented by Google's Threat Intelligence Group. The group has demonstrated a persistent focus on diplomatic entities, having previously targeted diplomats in the Southeast Asia region before expanding operations to European diplomatic targets. UNC6384 employs multi-faceted execution chains that combine social engineering, traffic manipulation techniques, digitally signed downloaders, and memory-resident malware deployment to achieve operational objectives.

The threat actor specializes in deploying variants of PlugX malware, which Google tracks as SOGU.SEC. PlugX has been actively used since at least 2008 and remains a favored tool among Chinese-nexus threat actors due to its modular architecture, extensive remote access capabilities, and evolving evasion techniques.

UNC6384 is believed to have associations with the well-established People's Republic of China (PRC) threat actor Mustang Panda, also tracked as TEMP.Hex. Both groups share multiple operational characteristics including targeting profiles focused on government sectors, overlapping command and control (C2) infrastructure, deployment of PlugX malware variants, and utilization of DLL side-loading techniques for payload execution. Google's attribution assessment is based on similarities in tooling, tactics, procedures, practices, targeting alignment with PRC's strategic interests, and infrastructure overlaps between the two groups.

Campaign Overview and Attack Methodology

Arctic Wolf Labs identified a new campaign by UNC6384 specifically targeting Hungarian and Belgian diplomatic entities during September and October 2025. This campaign represents a tactical evolution from the group's previously documented operations, introducing exploitation of a recently disclosed Windows vulnerability alongside refined social engineering approaches.

The attack begins with targeted spearphishing emails that kick off several stages that lead to the delivery of malicious LNK files, themed around diplomatic meetings and conferences. These files leverage ZDI-CAN-25373, a Windows shortcut vulnerability disclosed in March 2025, that enables covert command execution through whitespace padding within the LNK file's COMMAND_LINE_ARGUMENTS structure.

Research from Trend Micro identified this vulnerability being exploited as a zero-day by multiple advanced persistent threat (APT) groups from North Korea, China, Russia, and Iran, for the purposes of espionage and data theft. UNC6384's adoption of this technique demonstrates the group's capability to rapidly integrate newly disclosed vulnerabilities into operational tradecraft.

The malicious LNK files use diplomatic conference themes as lures, including Agenda_Meeting 26 Sep Brussels.lnk, which references a European Commission meeting on facilitating the free movement of goods at EU-Western Balkans border crossing points. Upon execution, the LNK file invokes PowerShell to decode and extract a tar (tape archive) archive file, which is then decompressed to deploy multiple components, including a legitimate signed Canon printer assistant utility, a malicious DLL, and an encrypted payload file.

This campaign differs from UNC6384's operations previously documented by Google Threat Intelligence Group, which employed adversary-in-the-middle attacks through captive portal hijacking to deliver malware disguised as Adobe plugin updates. Our findings indicate that UNC6384 maintains multiple parallel operational approaches adapted to specific target environments and access opportunities.

Technical Analysis

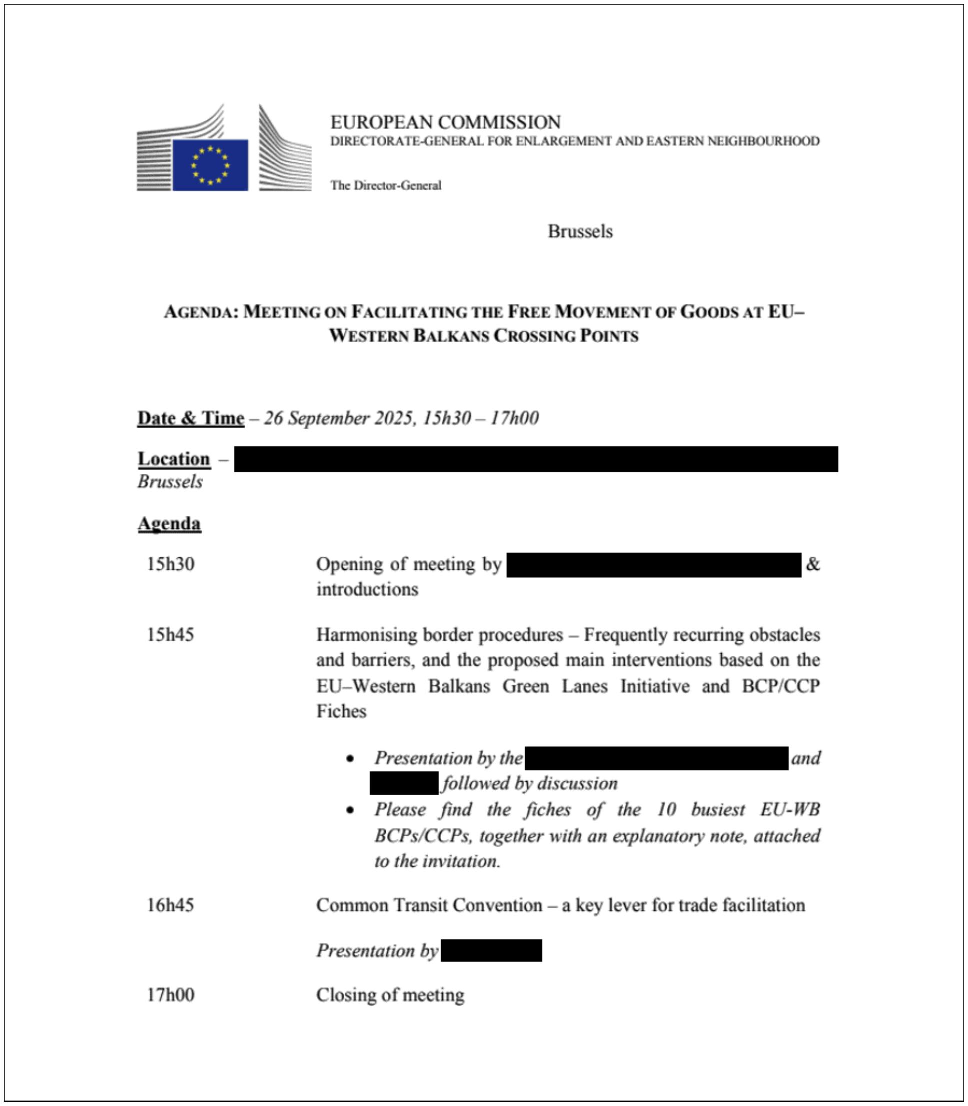
Stage 1: Initial Access via Malicious LNK File

The attack chain initiates with a weaponized LNK file, delivered to targets through spearphishing operations. The LNK file exploits ZDI-CAN-25373, a Windows shortcut vulnerability that allows the threat actor to execute commands covertly by adding whitespace padding within the COMMAND_LINE_ARGUMENTS structure.

Field	Value
Name	Agenda_Meeting 26 Sep Brussels.lnk

SHA-256	911cccd238fbfdb4babafc8d2582e80dcfa76469fa1ee27bbc5f4324d5fca539
File Type	.lnk file
Size	2.58KB

Upon execution, the LNK file invokes PowerShell with an obfuscated command that decodes a tar archive file named rjnlzlkfe.ta, which it saves it to the AppData\Local\Temp directory. The PowerShell command then extracts the tar archive using tar.exe -xvf and initiates execution of the contained cnmpaui.exe file. Simultaneously, a PDF decoy document is displayed, showing the authentic agenda for a European Commission meeting that was scheduled for September 26, 2025, in Brussels. This maintains the illusion of legitimate document access while malicious actions occur in the background.



EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENLARGEMENT AND EASTERN NEIGHBOURHOOD

The Director-General

Brussels

AGENDA: MEETING ON FACILITATING THE FREE MOVEMENT OF GOODS AT EU–WESTERN BALKANS CROSSING POINTS

Date & Time – *26 September 2025, 15h30 – 17h00*

Location – [redacted] *Brussels*

Agenda

15h30	Opening of meeting by [redacted] & introductions
15h45	Harmonising border procedures – Frequently recurring obstacles and barriers, and the proposed main interventions based on the EU–Western Balkans Green Lanes Initiative and BCP/CCP Fiches • *Presentation by the* [redacted] *and* [redacted] *followed by discussion* • *Please find the fiches of the 10 busiest EU-WB BCPs/CCPs, together with an explanatory note, attached to the invitation.*
16h45	Common Transit Convention – a key lever for trade facilitation *Presentation by* [redacted]
17h00	Closing of meeting

Figure 1: *Decoy PDF document displaying European Commission meeting agenda on facilitating the free movement of goods at EU-Western Balkans border crossing points.*

Stage 2: DLL Side-Loading via Legitimate Signed Binary

The extracted tar archive contains three critical files that enable the attack chain through DLL side-loading, a technique that abuses the Windows DLL search order to load malicious code through legitimate applications.

Name	Date modified	Type	Size
cnmpaui.dll	26/09/2025 08:48	Application extension	4 KB
cnmpaui.exe	26/09/2025 08:48	Application	352 KB
cnmplog.dat	26/09/2025 08:48	DAT File	818 KB

__Figure 2:__ Contents of extracted tar archive showing three files: cnmpaui.dll (4KB), cnmpaui.exe (352KB), and cnmplog.dat (818KB).

The primary executable is a legitimate Canon printer assistant utility that possesses a valid digital signature from Canon Inc., signed with a certificate issued by Symantec Class 3 SHA256 Code Signing CA. Although the certificate expired on April 19, 2018, Windows continues to trust binaries whose signatures include a valid timestamp proving they were signed while the certificate was valid.

Field	Value
Name	cnmpaui.exe
SHA-256	4ed76fa68ef9e1a7705a849d47b3d9dcdf969e332bd5bcb68138579c288a16d3
File Type	PE32 executable
Size	352.67KB
Certificate Issuer	Symantec Class 3 SHA256 Code Signing CA
Certificate Valid From	July 9, 2015
Certificate Valid Until	April 19, 2018 (expired)

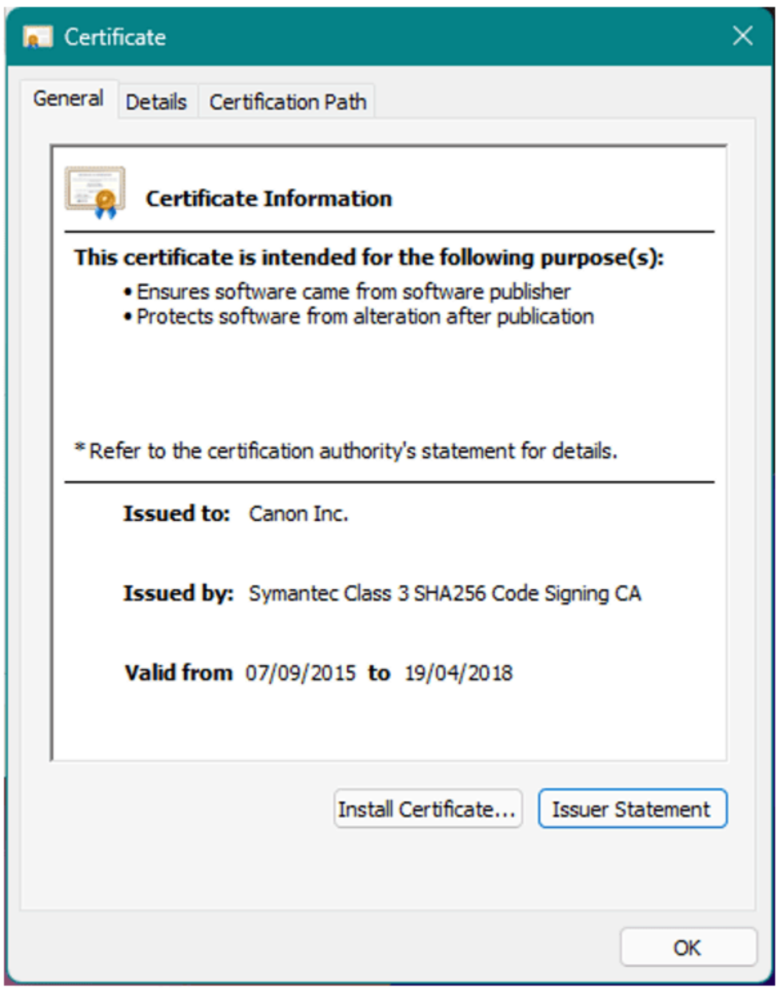


__Figure 3:__ Digital certificate information showing a valid Canon Inc. signature issued by Symantec, with a validity period from 2015 to 2018.

This legitimate binary is susceptible to DLL side-loading attacks. When cnmpaui.exe executes, it searches for cnmpaui.dll in its current directory before checking system directories. The threat actor exploits this behavior by planting a malicious cnmpaui.dll in the same directory.

Field	Value
Name	cnmpaui.dll
SHA-256	e53bc08e60af1a1672a18b242f714486ead62164dda66f32c64ddc11ffe3f0df
File Type	PE32 DLL

Size	4.00KB

The malicious DLL functions as a lightweight loader designed to decrypt and execute the third file in the archive, cnmplog.dat, which contains the encrypted PlugX payload.

Stage 3: Encrypted Payload Decryption and In-Memory Execution

The cnmplog.dat file is an RC4-encrypted blob containing the PlugX malware. The malicious DLL decrypts this file using a hardcoded 16-byte RC4 key and loads the resulting PlugX payload directly into the address space of the legitimate cnmpaui.exe process, enabling the malware to execute within a trusted process context and evade detection mechanisms that rely on process reputation or executable file analysis.

Field	Value
Name	cnmplog.dat
SHA-256	c9128d72de407eede1dd741772b5edfd437e006a161eecfffdf27b2483b33fc7
File Type	Encrypted blob
Size	817.09KB
Encryption	RC4 with 16-byte hardcoded key
RC4 Key	eQkiwoiuDsvIPsmd

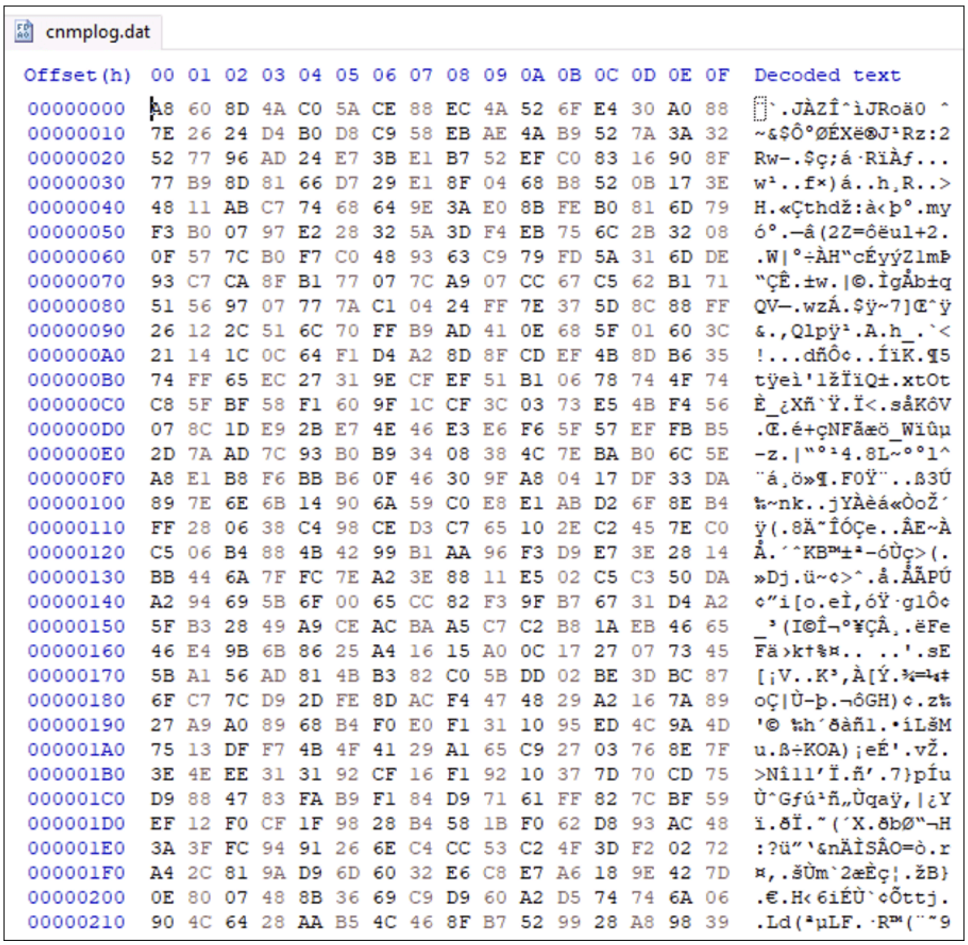


Figure 4: *Hexadecimal view of cnmplog.dat showing encrypted content before decryption.*

This three-stage execution flow completes the deployment of PlugX malware running stealthily within a legitimate signed process, significantly reducing the likelihood of detection by endpoint security solutions.

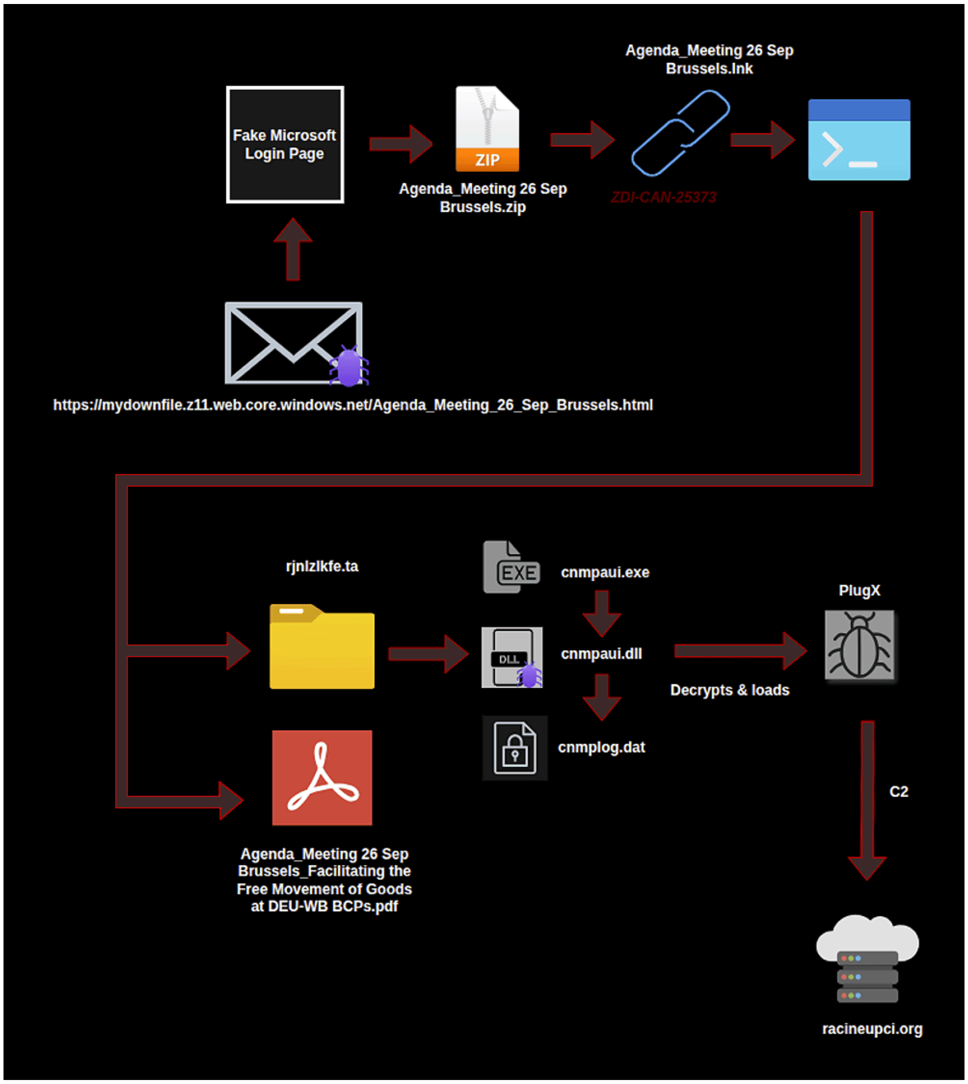


Figure 5: *Graph overview showing the high-level execution chain.*

PlugX Malware Analysis

PlugX is a Remote Access Trojan (RAT) that was first observed in 2008. It has seen many evolutions and variations since then, including as a modular malware, and it is a threat that remains actively deployed by Chinese-affiliated threat actors.

The malware provides comprehensive remote access capabilities including command execution, keylogging, file upload and download operations, persistence establishment, and extensive system reconnaissance functions. Its modular architecture allows operators to extend functionality through plugin modules tailored to specific operational requirements.

PlugX operates under multiple aliases including Korplug, TIGERPLUG, and SOGU. The Google Threat Intelligence Group tracks the memory-resident variant deployed by UNC6384 as SOGU.SEC.

Analyzed Sample Details:

- **SHA-256:** 3fe6443d464f170f13d7f484f37ca4bcae120d1007d13ed491f15427d9a7121f
- **MD5:** dc1dba02ab1020e561166aee3ee8f5fb
- **Compilation Timestamp:** Friday, September 5, 2025, 05:15:45 UTC
- **File Type:** x86 PE DLL

Loading Phase Technical Details:

All PlugX variants observed in this campaign export the MSGInitialize function. The PE header of the decrypted DLL contains shellcode that invokes this export at a specific offset. Analysis reveals the exported MSGInitialize implements control-flow flattening by using a central dispatcher loop controlled by a state variable, a technique associated with commercial obfuscators designed to complicate reverse engineering efforts.

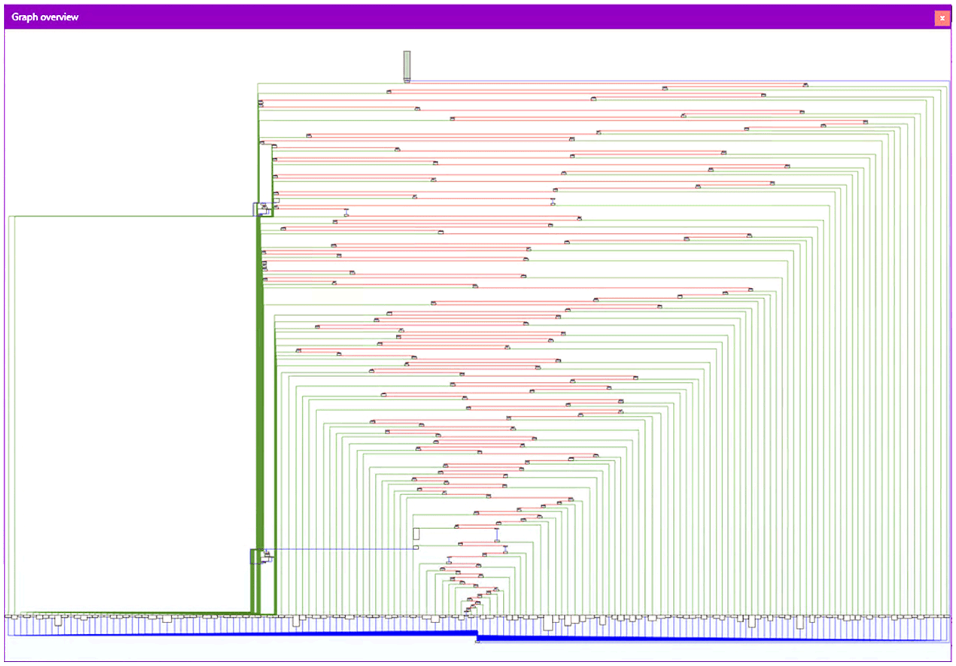


Figure 6: *Graph overview showing control-flow flattening obfuscation pattern with a state machine dispatcher creating complex execution paths.*

Beneath the obfuscation layer, MSGInitialize walks the Process Environment Block (PEB) and Loader Data Table to enumerate loaded modules. The routine computes a rolling 32-bit hash using a bitwise rotate-left by 0x13 (19) bits on each iteration (functionally equivalent to a ROR-13) and compares the resulting values against embedded constants to identify specific modules. Notable hash values include 0x6A4ABC5B corresponding to KERNEL32.DLL and 0x3CFA685D corresponding to NTDLL.DLL.

Once target modules are identified, the same hashing algorithm is applied to export names within those modules, comparing hashes to additional embedded constants to locate specific APIs required for loading and mapping portable executable (PE) files into memory.

Hash Value	API Function	Module
0x8C394D89	NtProtectVirtualMemory	ntdll.dll
0xD33BCABD	NtAllocateVirtualMemory	ntdll.dll
0x91AFCA54	VirtualAlloc	kernel32.dll
0x7946C61B	VirtualProtect	kernel32.dll
0x7C0DFCAA	GetProcAddress	kernel32.dll
0xEC0E4E8E	LoadLibraryA	kernel32.dll
0xE54CC407	LdrGetProcedureAddress	ntdll.dll
0xEB6C8389	RtlAnsiStringToUnicodeString	ntdll.dll
0x7CC3283D	RtlInitAnsiString	ntdll.dll
0x534C0AB8	NtFlushInstructionCache	ntdll.dll
0xB0988FE4	LdrLoadDll	ntdll.dll

Following API resolution, the code uses Reflective Code Loading to map the PE into memory and finalizes memory protections. The module's entry point is invoked twice in succession: first with the fdwReason parameter set to 1 corresponding to DLL_PROCESS_ATTACH for normal initialization, then immediately with a non-standard fdwReason value of 0x04, which the module recognizes as a signal to execute its payload. This loading methodology is consistent with techniques previously documented by ESET in their most recent PlugX analysis.

```
.text:10006103
.text:10006103 loc_10006103:
.text:10006103 mov     eax, 0FFFFFFFFh
.text:10006108 xor     ecx, ecx
.text:1000610A mov     [esp+0E8h+var_E8], eax
.text:1000610D mov     [esp+0E8h+var_E4], 0
.text:10006115 mov     [esp+0E8h+var_E0], 0
.text:1000611D call    [esp+0E8h+var_7C] ; NtFlushInstructionCache
.text:10006121 sub     esp, 0Ch
.text:10006124 mov     eax, [esp+0E8h+var_8C]
.text:10006128 lea     ecx, [esp+0E8h+var_80]
.text:1000612C mov     edx, 0FFFFFFFFh
.text:10006131 lea     esi, [esp+0E8h+var_84]
.text:10006135 lea     edi, [esp+0E8h+var_20]
.text:1000613C mov     [esp+0E8h+var_E8], edx
.text:1000613F mov     [esp+0E8h+var_E4], ecx
.text:10006143 mov     [esp+0E8h+var_E0], esi
.text:10006147 mov     [esp+0E8h+var_DC], 20h ; ' '
.text:1000614F mov     [esp+0E8h+var_D8], edi
.text:10006153 call    eax             ; ZwProtectVirtualMemory 0x20
.text:10006155 sub     esp, 14h
.text:10006158 mov     eax, [esp+0F0h+var_D0]
.text:1000615C mov     ecx, [esp+0F0h+var_D4]
.text:10006160 xor     edx, edx
.text:10006162 mov     [esp+0F0h+var_F0], ecx
.text:10006165 mov     [esp+0F0h+var_EC], 1
.text:1000616D mov     [esp+0F0h+var_E8], 0
.text:10006175 call    eax             ; DllEntryPoint,1
.text:10006177 sub     esp, 0Ch
.text:1000617A mov     eax, [esp+0E8h+var_C8]
.text:1000617E mov     ecx, [esp+0E8h+var_CC]
.text:10006182 xor     edx, edx
.text:10006184 mov     [esp+0E8h+var_E8], ecx
.text:10006187 mov     [esp+0E8h+var_E4], 4
.text:1000618F mov     [esp+0E8h+var_E0], 0
.text:10006197 call    eax             ; DllEntryPoint,4
.text:10006199 sub     esp, 0Ch
.text:1000619C mov     eax, [esp+0E8h+var_C8]
.text:100061A0 add     esp, 0DCh
.text:100061A6 pop     esi
.text:100061A7 pop     edi
.text:100061A8 pop     ebx
.text:100061A9 retn
```

Figure 7: *Disassembly code showing manual PE loading sequence with NtFlushInstructionCache call and DLL entry point invocation.*

Anti-Analysis and Evasion Techniques:

The malware implements extensive anti-analysis measures, including heavy code obfuscation, multiple anti-debugging checks (e.g., CheckRemoteDebuggerPresent), and numerous encrypted strings that are only decrypted at runtime. The code demonstrates heavy obfuscation to prevent analysis, with control-flow flattening implemented by using a central dispatcher loop controlled by a state variable, patterns commonly associated with commercial obfuscators.

The payload also dynamically loads several system DLLs – user32.dll, shlwapi.dll, psapi.dll, version.dll, msvcrt.dll, winhttp.dll, and ole32.dll and resolves their APIs at runtime, with some API names derived from decrypted strings. These modules supply the Windows APIs the malware uses during execution.

Persistence Establishment:

The malware creates a hidden directory in one of several possible locations within the user profile and copies all extracted files to maintain persistent access. Directory names vary between infections and may include “SamsungDriver,” “Intelnet,” “VirtualFile,” “SecurityScan,” or “DellSetupFiles.” The malware establishes persistence through registry modification, creating a value named “CanonPrinter” in the registry key `Software\Microsoft\Windows\CurrentVersion\Run` with the path set to the copied cnmpaui.exe location.

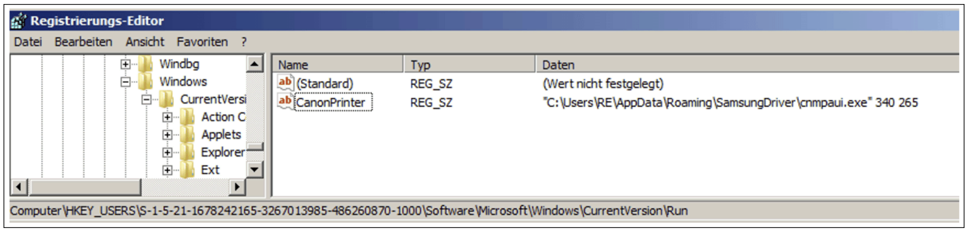


Figure 8: *Windows Registry Editor showing persistence mechanism via Run key entry pointing to cnmpaui.exe in SamsungDriver directory*

Each time the system launches, the directory name may change and all files are transferred to the new location, complicating forensic analysis and detection based on static file paths.

Command and Control Communication:

Upon successful deployment, the malware establishes communication with C2 infrastructure using WinHTTP APIs. The payload employs a consistent user agent string across samples: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 10.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729).

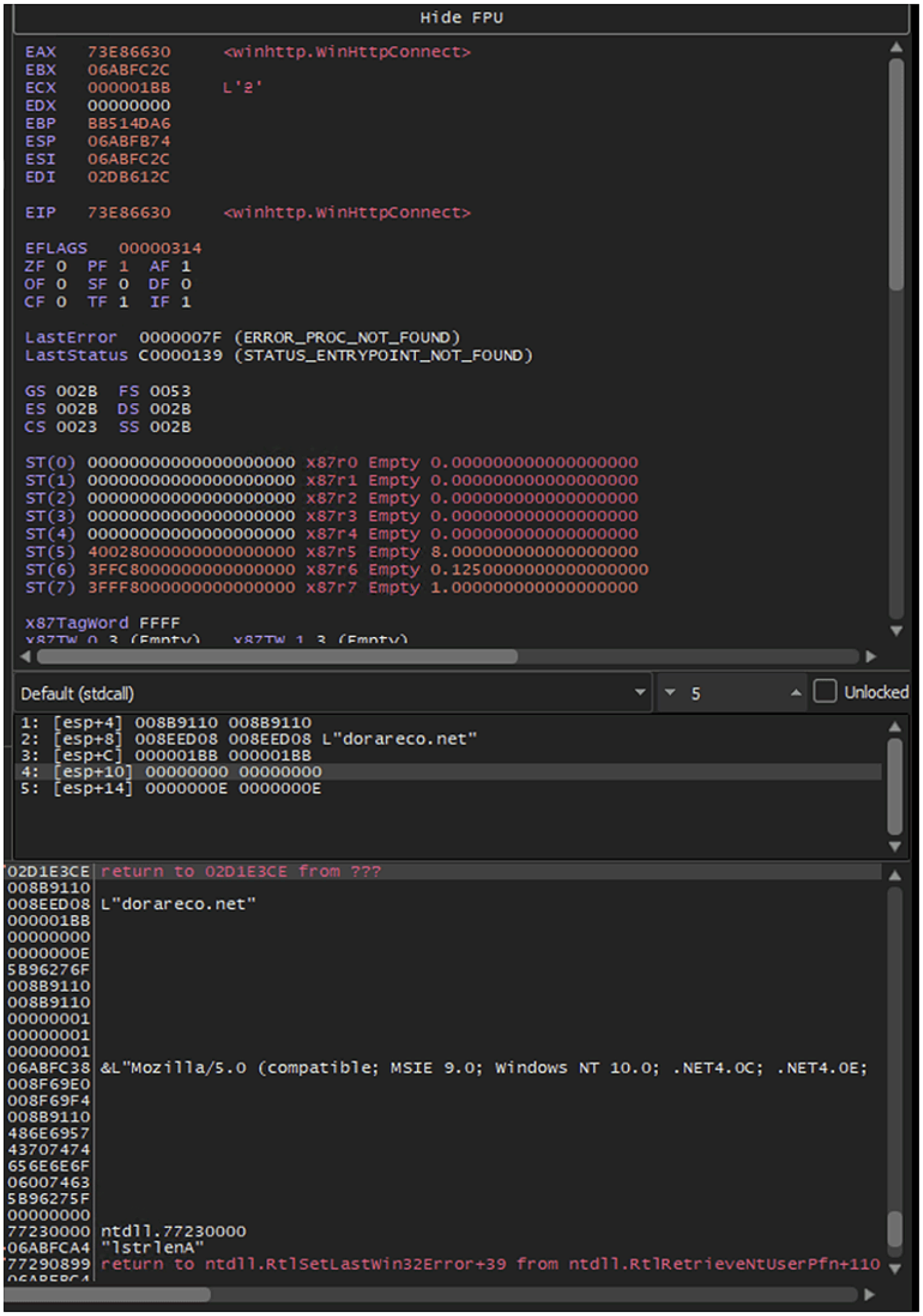


__Figure 9:__ Debugger output showing WinHttp.WinHttpConnect call preparing connection to the threat actor's C2 server, dorareco[.]net.

Initial check-in requests incorporate epoch timestamps and randomized URL parameters that likely contain victim fingerprinting data. Observed request patterns include:

- /download?t=1760103992&LeQa=PKDugp&VE=ZY6tyOYZWNxK2a
- /settings?t=1760106491&D=XAl0cJ&WB=qKVsKW7KF&xRcH=dQ3SFEgr0v&78=dAi0sahua

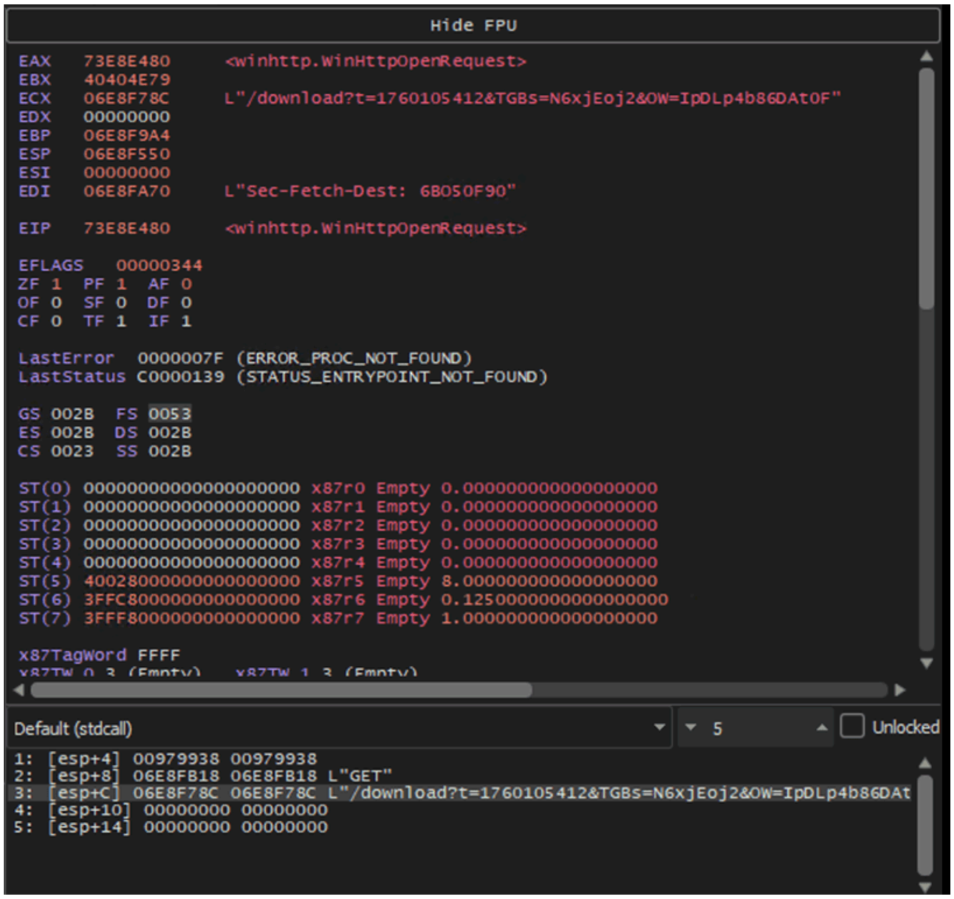


Figure 10: *Debugger output showing WinHttpOpenRequest with epoch timestamp and encoded parameters for initial C2 communication.*

The parameter following the forward slash is randomly selected across requests (observed endpoints include /download, /settings, /profile, /bookmark, /help/? and /developer), suggesting dynamic request generation to complicate network-based detection. Analysis indicates the epoch timestamp provides temporal context while additional parameters likely convey system fingerprinting information, though complete parameter decoding was not achieved within the analysis timeframe.

PlugX Configuration Extraction:

Analysis of the encrypted payload reveals embedded configuration data containing operational parameters:

Sample 1 Configuration (Brussels-themed lure):


```
{
  "mutex": "uUbAmgDu",
  "lure_filename": "Agenda_Meeting 26 Sep Brussels_Facilitating the Free Movement of
Goods at EU-WB BCPs.pdf",
  "c2": [
    {"host": "racineupci[.]org", "port": 443, "flags": "0x0001"},
    {"host": "racineupci[.]org", "port": 443, "flags": "0x0001"},
    {"host": "racineupci[.]org", "port": 443, "flags": "0x0001"}
  ]
}
```


Sample 2 Configuration (Copenhagen-themed lure):


```
{
  "mutex": "esUdgquBv",
  "lure_filename": "EPC invitation letter Copenhagen 1-2 October 2025.pdf",
  "c2": [
    {"host": "dorareco[.]net", "port": 443, "flags": "0x0001"},
    {"host": "dorareco[.]net", "port": 443, "flags": "0x0001"},
```

```
    {"host": "dorareco[.]net", "port": 443, "flags": "0x0001"}
  ]
}
```

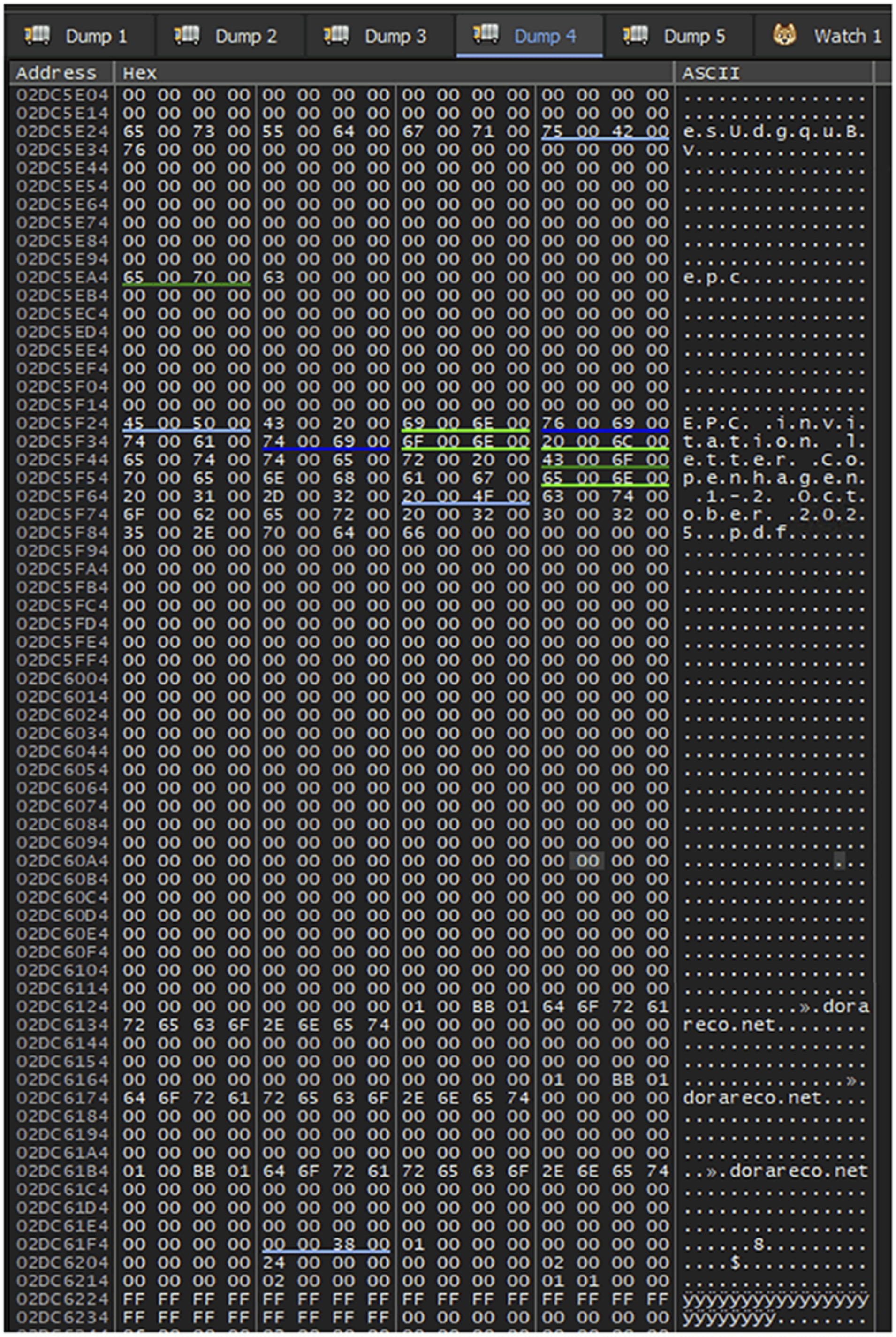



Figure 11: *Memory dump showing embedded PlugX configuration with the C2 domain dorareco[.]net visible in plaintext.*

The configuration specifies unique mutex names for each sample variant, references to the decoy PDF lures used in social engineering ploys, and C2 infrastructure utilizing HTTPS over port 443 for encrypted communications.

CanonStager Evolution Analysis

Arctic Wolf Labs observed significant evolution in the CanonStager loader component between early September and October 2025, indicating active development and refinement of the malware delivery mechanism.

Early September Evolution

Two CanonStager samples showed substantial size reduction from approximately 700KB to approximately 100KB. These samples retained the Thread Local Storage array data structure for storing function addresses resolved through custom API hashing algorithms. However, the samples demonstrated simplified execution flow with removal of the custom Windows procedure and message queue functionality, reducing code complexity while maintaining core loader capabilities.

Early October Evolution

Three CanonStager samples measuring approximately 4KB represent a dramatic simplification of the loader architecture. This version eliminates previous complexity, including the TLS array for resolved API addresses, custom Windows procedures, message queues, and threading mechanisms. The streamlined loader walks the Process Environment Block to locate required modules, employs API hashing to resolve function addresses, stores these addresses in standard variables rather than TLS storage, performs RC4 decryption of the payload, and invokes execution via an EnumSystemGeoID callback function.

The evolution from complex loaders to minimal, streamlined variants suggests operational adaptation based on detection challenges or performance requirements. The latest 4KB version maintains essential functionality while dramatically reducing forensic footprint and analysis surface area.

An important technical distinction: the original Google Threat Intelligence Group sample was implemented in the D programming language and compiled with DMD compiler. In contrast, all three of the latest 4KB Arctic Wolf samples utilize C runtime libraries and employ general-purpose registers rather than XMM registers, indicating different development approaches or separate development teams within the UNC6384 operational structure.

Alternative Delivery Mechanisms

Also observed in early September, Arctic Wolf identified UNC6384's use of an HTA file configured to run invisibly in the background, which loads external JavaScript from a CloudFront URL. The JavaScript facilitated payload retrieval from the same CloudFront-based C2 and served as a delivery mechanism for three critical files: cnmpaui.exe, cnmpauix.exe, and cnmplog.dat.

Field	Value
Name	XgPK9CpZENdh.js
SHA-256	c3b7abcb583b90559af973dd18bf5ccba48d3323e5e2e8bc0b11ff54425e34dd
File Type	JavaScript
Size	4.86KB
In-The-Wild URL	http[:]//d32tpl7xt7175h[.]cloudfront[.]net/XgPK9CpZENdh
Execution Parent	7a49310a9192cab1aa05256b6ca0d0c1a54fe084b103ff4df2d17be9effa3300 (No.4638.hta)
	a7d12712673a4e3b6d62a9d84f124e62689da12f0a3ee6009369ecf469ce8182 (cnmplog.dat)
Delivered Payload	ee9295fa36e29808ff36beb55be328b68d82f267d2faa54db26e0bf86b78fa56 (cnmpaui.dll)
	4ed76fa68ef9e1a7705a849d47b3d9dcdf969e332bd5bcb68138579c288a16d3 (cnmpaui.exe)
PlugX C2	Vnptgroup[.]it[.]com

Field	Value
Name	oxF3dIMDi339.js
SHA-256	274adf7f60e0799b157e7524d503d345f6870010703fb6b56a3dd1e62b4de3e8
File Type	JavaScript
Size	4.88KB
Delivered Payload	716637a424bce58ff8c75e40b6e29c33318ff185af6e9e62d85b61e56a560eac (cnmpaui.dll) 4ed76fa68ef9e1a7705a849d47b3d9dcdf969e332bd5bcb68138579c288a16d3 (cnmpaui.exe)
PlugX C2	Vnptgroup[.]it[.]com

Network Infrastructure Analysis

UNC6384 maintains distributed C2 infrastructure utilizing multiple domains registered through various providers and geographic regions. The infrastructure demonstrates operational security awareness through domain selection that mimics legitimate organizational naming patterns, while maintaining geographic diversity to complicate takedown efforts.

Command and Control Infrastructure:

The campaign employs the following C2 domains, all configured to communicate over HTTPS port 443:

Primary Campaign Infrastructure:

- Racineupci[.]org (Hungarian/Belgian targeting)
- Dorareco[.]net (Hungarian/Belgian targeting)

Overlapping Campaign Infrastructure (identified through pivoting):

- naturadeco[.]net (Serbian government targeting)
- cseconline[.]org (Belgian targeting)
- vnptgroup[.]it.com (Italian targeting)
- paquimetro[.]net (earlier campaign infrastructure)

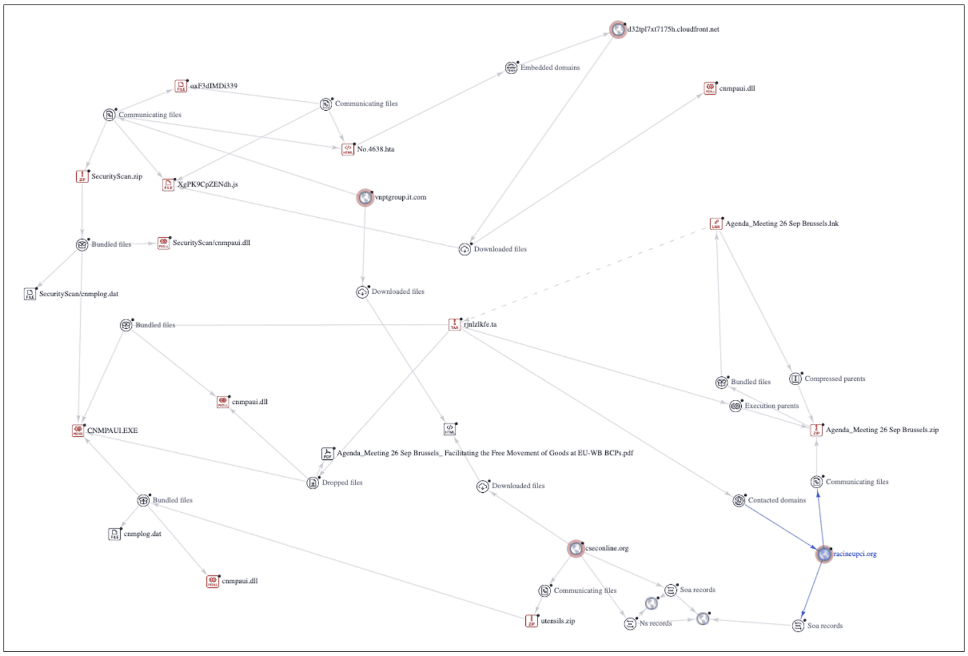


Figure 12: *Network infrastructure visualization showing relationships between C2 domains, malware samples, decoy documents, and targeted entities across multiple European nations (Click to enlarge).*

Infrastructure analysis reveals registration patterns consistent with operational security practices employed by nation-state threat actors. Domains are registered through different providers to prevent single-point disruption, employ HTTPS with valid “Let’s Encrypt” certificates to avoid browser security warnings, and utilize naming conventions that superficially resemble legitimate organizations or technical services.

Passive DNS analysis indicates C2 domains resolve to hosting infrastructure distributed across multiple autonomous systems and geographic locations, complicating network-based blocking efforts. The threat actor maintains multiple simultaneous C2 domains for operational redundancy, with individual samples configured to communicate with specific domains based on target or operational phase.

Victimology and Target Analysis

This UNC6384 campaign demonstrates precise targeting of European diplomatic entities, with a focus on organizations involved in cross-border policy, defense cooperation, and multilateral coordination activities.

Confirmed Targets

Hungarian Diplomatic Entities

Arctic Wolf identified malicious LNK files delivered to Hungarian diplomatic personnel using European Commission meeting themes as lures. The “Agenda_Meeting 26 Sep Brussels” lure references an authentic Directorate-General for Enlargement and Eastern Neighbourhood meeting that was scheduled for September 26, 2025, in Brussels, addressing the harmonization of border procedures and facilitation of free movement of goods at EU-Western Balkans border crossing points.

Belgian Diplomatic Entities

Targeting of Belgian diplomatic personnel was confirmed through delivery of lures themed around Joint Arms Training and Evaluation Centre workshops on wartime defense procurement scheduled for September 9-11, 2025. Belgium's role as host nation for NATO headquarters and numerous EU institutions makes Belgian diplomatic entities valuable intelligence targets for monitoring alliance activities and policy development.

Serbian Government Entities

StrikeReady research documented targeting of Serbian government aviation departments using lures themed around NAJU flight training plans for October 2025. This targeting aligns with Serbian government's complex diplomatic position balancing EU accession aspirations with traditional relationships with Russia and China, making Serbian government communications valuable for monitoring geopolitical alignment and policy trajectories.

Additional European Targeting

Infrastructure analysis and malware sample pivoting identified additional campaigns targeting diplomatic entities in Italy and the Netherlands, with lures including "EPC invitation letter Copenhagen 1-2 October 2025" suggesting targeting around European Political Community summit activities.

Targeting Rationale

The geographic and thematic focus of this campaign indicates intelligence collection priorities aligned with PRC strategic interests in European defense cooperation, cross-border infrastructure development, and multilateral diplomatic coordination.

Specific targeting themes include:

Defense and Security Cooperation

Lures referencing defense procurement workshops and military training suggest interest in NATO and EU defense initiatives, procurement decisions, and military readiness assessments during the period of heightened European security concerns following Russia's invasion of Ukraine.

Cross-Border Infrastructure and Trade

Targeting around EU-Western Balkans border facilitation and free movement of goods initiatives indicates intelligence requirements concerning European supply chain resilience, infrastructure development in candidate countries, and trade policy evolution affecting China's economic interests.

Multilateral Diplomatic Coordination

Focus on European Commission meetings, European Political Community summits, and NATO-related events demonstrates interest in understanding alliance cohesion, policy coordination mechanisms, and potential divisions or disagreements within European multilateral frameworks.

Comparison with Historical Targeting

Google's March 2025 reporting documented UNC6384 targeting diplomats primarily in Southeast Asia, representing traditional Chinese intelligence collection priorities in a region of direct territorial and economic interest. The expansion to European diplomatic targeting observed in this campaign indicates either broadened operational mandate or deployment of additional operational teams with geographic specialization. The consistency in tooling and techniques across both geographic theaters suggests centralized tool development with regional operational deployment.

Attribution Assessment

Arctic Wolf Labs assesses with high confidence that this campaign is attributable to UNC6384, a Chinese-affiliated cyber espionage threat actor. This attribution is based on multiple converging lines of evidence including malware tooling, tactical procedures, targeting alignment, and infrastructure overlaps with previously documented UNC6384 operations.

Impact Analysis

Successful compromise of diplomatic entities by UNC6384 poses significant national security implications extending beyond immediate data theft to encompass long-term intelligence collection, strategic positioning, and potential influence operations.

Intelligence Collection Capabilities

The PlugX malware deployed in this campaign acts as a remote-access implant, providing persistent unauthorized control over compromised endpoints, and granting operators the ability to conduct exfiltration of classified or sensitive documents, monitoring of real-time policy discussions and decision-making processes, collection of credentials for accessing diplomatic networks and partner systems, and surveillance of diplomatic calendars and travel plans.

Successful long-term compromise enables collection of strategic intelligence concerning European foreign policy development, defense cooperation initiatives, economic policy coordination, negotiating positions for international agreements, internal assessments of geopolitical situations, and relationship dynamics within multilateral frameworks. This intelligence serves People's Republic of China strategic planning by providing early warning of policy shifts, identifying opportunities for influence or division within alliances, understanding economic regulatory developments affecting Chinese interests, and assessing military cooperation and capability development trends.

Operational Security Implications

The campaign's exploitation of ZDI-CAN-25373, a vulnerability disclosed in March 2025, within six months of public disclosure demonstrates UNC6384's capability for rapid vulnerability adoption. This timeline suggests either direct monitoring of vulnerability disclosures with rapid development cycles, or potential pre-disclosure awareness through other intelligence channels. The group's willingness to exploit vulnerabilities that have been publicly documented as actively being exploited by multiple nation-state actors indicates risk tolerance and confidence in success rates despite increased defender awareness.

The evolution of CanonStager from approximately 700KB to 4KB between September and October 2025 indicates active development responding to detection challenges. This rapid iteration cycle suggests either dedicated development resources or access to broader Chinese state-sponsored malware development infrastructure supporting multiple operational groups.

Broader Campaign Scope

Infrastructure analysis and malware sample pivoting conducted by Arctic Wolf Labs and recently documented by StrikeReady researchers indicates this campaign extends beyond Hungarian and Belgian diplomatic targeting to encompass broader European diplomatic entities, including Serbian government agencies, Italian diplomatic entities, Netherlands diplomatic organizations, and likely additional targets not yet identified through available telemetry.

The breadth of targeting across multiple European nations within a condensed timeframe suggests either a large-scale coordinated intelligence collection operation or deployment of multiple parallel operational teams with shared tooling but independent targeting. The consistency in tradecraft across disparate targets indicates centralized tool development and operational security standards even if execution is distributed across multiple teams.

Mitigation Recommendations

Organizations, particularly those in diplomatic and government sectors, should implement the following defensive measures to protect against UNC6384 operations and similar nation-state espionage campaigns.

Immediate Actions

As there is no official patch for the ZDI-CAN-25373 vulnerability, the blocking or restricting of the usage of .lnk files from questionable sources can be carried out by deactivating the automatic resolution of them in Windows Explorer. This should be put in place across all Windows systems, prioritizing endpoints used by personnel with access to sensitive diplomatic or policy information. While this vulnerability was disclosed in March 2025, adoption by threat actors within months of disclosure necessitates urgent monitoring and countermeasures.

Review and block C2 infrastructure identified in this report, including racineupci[.]org, dorareco[.]net, naturadeco[.]net, cseconline[.]org, vnptgroup[.]it.com, and paquimetro[.]net at network perimeters and within web filtering solutions. Implement monitoring for attempted connections to these domains even after blocking, to identify potentially compromised systems attempting C2 communication.

Conduct searches across endpoint environments for the presence of Canon printer assistant utilities (specifically cnmpaui.exe) in unusual locations including user AppData directories, especially when accompanied by cnmpaui.dll and cnmplog.dat files in the same directory. Investigate any instances of legitimate Canon printer binaries executing from non-standard installation directories.

Continuous user education, such as general security awareness training, is one of the most important elements in preventing malicious entities from obtaining access to your networks. Ensure all employees are aware of good cybersecurity hygiene practices, including training on spotting the typical red flags of a phishing attack, and consider implementing a Cyber Threat Intelligence (CTI) program in your organization.

For organizations without a dedicated security operations (SOC) team, Arctic Wolf® Managed Detection and Response (MDR) provides 24×7 monitoring of your networks, endpoints, and cloud environments to detect, respond to, and remediate modern cyberattacks.

Conclusions

This UNC6384 campaign demonstrates the continued evolution and operational expansion of Chinese cyber espionage capabilities targeting diplomatic entities. The threat actor's rapid adoption of ZDI-CAN-25373 within six months of disclosure illustrates sustained capability for vulnerability exploitation integration into operational tradecraft. The expansion from documented Southeast Asia targeting to European diplomatic entities indicates either broadened intelligence collection mandates or deployment of additional operational teams with geographic specialization while maintaining centralized tool development.

The campaign's focus on European diplomatic entities involved in defense cooperation, cross-border policy coordination, and multilateral diplomatic frameworks aligns with PRC strategic intelligence requirements concerning European alliance cohesion, defense initiatives, and policy coordination mechanisms. Successful long-term compromise of diplomatic entities provides strategic intelligence concerning policy development, negotiating positions, relationship dynamics within multilateral frameworks, and early warning of policy shifts affecting Chinese interests.

Organizations in diplomatic and government sectors should implement the detailed mitigation recommendations provided in this report, with priority focus on mitigating against ZDI-CAN-25373, blocking identified C2 infrastructure, enhancing detection for DLL side-loading attacks, and conducting proactive threat hunting for indicators of historical compromise given the extended operational timeline characteristic of nation-state espionage campaigns.

Arctic Wolf remains committed to protecting customers from advanced persistent threats and will continue enhancing detection capabilities as UNC6384 operations evolve.

How Arctic Wolf Protects Its Customers

Arctic Wolf is committed to ending cyber risk, and when active campaigns are identified, we move quickly to protect our customers. Arctic Wolf Labs has leveraged threat intelligence around UNC6384 activity to implement new detections in the Arctic Wolf® Aurora™ Platform to protect customers.

As we discover new information, we will enhance our detections to account for additional IOCs and techniques leveraged by the threat group behind this malicious activity.

APPENDIX

Indicators of Compromise

File Indicators:

Name	SHA-256	MD5
Agenda_Meeting 26 Sep Brussels.lnk	911cccd238fbfdb4babafc8d2582e80dcfa76469fa1ee27bbc5f4324d5fca539	–
cnmpaui.exe	4ed76fa68ef9e1a7705a849d47b3d9dcdf969e332bd5bcb68138579c288a16d3	–
cnmpaui.dll	e53bc08e60af1a1672a18b242f714486ead62164dda66f32c64ddc11ffe3f0df	–
cnmplog.dat	c9128d72de407eede1dd741772b5edfd437e006a161eecfffdf27b2483b33fc7	–
PlugX payload (decrypted)	3fe6443d464f170f13d7f484f37ca4bcae120d1007d13ed491f15427d9a7121f	dc1dba02ab1020e561166aee3ee
rjnlzlkfe.ta	7168838787039d82961836e5f2f9c70f3fe7c4d99a6c7c61405b3364ce37e760	–

AA.zip	f8d03814986599ed98ce8c83fbc9ce55b83095c179c54ec555c4ab372fa99700	–
Agenda_Meeting 26 Sep Brussels.zip	bb491248bb8f6067af39e196b11f4e408a7a3885704cadbd4266db52ae4b03e2	0a02938e088b74fe6be2f10bb913
JATEC workshop on wartime defence procurement (9-11 September).zip	–	f15c9d7385cffd1d04e54c5ffdb765
EPC invitation letter Copenhagen 1-2 October 2025.zip	–	227045c5c5c47259647f280bee8f
NAJU Plan Obuka OKTOBAR 2025.lnk	0d0dd1cbde02e4e138c352b82a0288cc	–
NAJU Plan Obuka OKTOBAR 2025.zip	f2d1fa1890e409996ed4a23bc69461fe	–
cnmpaui.dll	c96338533d0ab4de8201ce1f793e9ea18d30c6179daf1e312e0f01aff8f50415	
cnmpaui.dll	e53bc08e60af1a1672a18b242f714486ead62164dda66f32c64ddc11ffe3f0df	
cnmpaui.dll	ae8d2cef8eac099f892e37cc50825d329459baa9625b71fb6f4b7e8f33c6ccce	
cnmpaui.dll	716637a424bce58ff8c75e40b6e29c33318ff185af6e9e62d85b61e56a560eac	
cnmpaui.dll	ee9295fa36e29808ff36beb55be328b68d82f267d2faa54db26e0bf86b78fa56	
SecurityScan.zip	1564e19b36ffc4e12becc4fb73359de13191ac8df62def45f045efbd6ef36e79	
Utensils.zip	218ed813d8a4d9d05473338795021c66012cd6c36368561d3aaf831a5c494740	
XgPK9CpZENdh.js	c3b7abcb583b90559af973dd18bf5ccba48d3323e5e2e8bc0b11ff54425e34dd	
oxF3dIMDi339.js	274adf7f60e0799b157e7524d503d345f6870010703fb6b56a3dd1e62b4de3e8	
No.4638.hta	7a49310a9192cab1aa05256b6ca0d0c1a54fe084b103ff4df2d17be9effa3300	
rphbqultm.ta	f04340f93e2f5f7d6d5521572f17c5b80f39984ee6b4b8c0899380e95a825127	
cnmpaui.dll		
cnmpaui.dat	d70600f0e4367e6e3e07f7b965b654e5bfbcb0afbccfe0f6a9a8d9f69c7061a3	

Network Indicators

Command and Control Domains
racineupci[.]org (Port 443, HTTPS)
racineupci[.]org (Port 443, HTTPS)
naturadeco[.]net (Port 443, HTTPS)
cseconline[.]org (Port 443, HTTPS)
vnptgroup[.]it[.]com (Port 443, HTTPS)
paquimetro[.]net (Port 443, HTTPS)

Delivery Infrastructure
mydownload.z29[.]web.core.windows[.]net
mydownloadfile[.]z7.web.core.windows[.]net
mydownfile[.]z11.web.core.windows[.]net
d32tpl7xt7175h[.]cloudfront[.]net

User Agent String
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 10.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)

Host Indicators:

Mutex Names
uUbAmgDu
esUdgquBv
Registry Keys Created
Software\Microsoft\Windows\CurrentVersion\Run\CanonPrinter
Registry Keys Queried
Software\CLASSES\ms-pu Value CLSID
Software\Microsoft\Windows\CurrentVersion\InternetSetting Value ProxyEnable, ProxyServer
Software\Microsoft\Internet Explorer\Version Vector Value IE
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform
Software\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform

File Paths
C:\Users[Username]\AppData\Roaming\SamsungDriver\cnmpaui.exe
C:\Users[Username]\AppData\Roaming\Intelnet*
C:\Users[Username]\AppData\Roaming\VirtualFile*
C:\Users[Username]\AppData\Roaming\SecurityScan*
C:\Users[Username]\AppData\Roaming\DellSetupFiles*
C:\Users[Username]\AppData\Local\Temp\rjnlzlkfe.ta
C:\Users[Username]\AppData\Local\Temp\krnqdyvmlb.ta
C:\Users[Username]\AppData\Local\Temp\tmp.dat

Decoy PDF Files
Agenda_Meeting 26 Sep Brussels_Facilitating the Free Movement of Goods at EU-WB BCPs.pdf
EPC invitation letter Copenhagen 1-2 October 2025.pdf
NAJU Plan Obuka OKTOBAR 2025.pdf

Applied Countermeasures

YARA Rules:

```
import "pe"

rule targeted_UNC6384_PlugX_2025 : extended description
{
    meta:
        description = "Detects PlugX RAT variant deployed by UNC6384 in 2025 European
diplomatic targeting campaign"
        author = "Arctic Wolf Labs"
        distribution = "TLP:GREEN"
        version = "1.0"
        last_modified = "2025-10-12"
        hash1_md5 = "dc1dba02ab1020e561166aee3ee8f5fb"
        hash1_sha256 =
"3fe6443d464f170f13d7f484f37ca4bcae120d1007d13ed491f15427d9a7121f"

    strings:
        $str1 = "%allusersprofile%\\" ascii wide
        $str2 = "SecurityScan" ascii wide
        $str3 = "CanonPrinter" ascii wide
        $str4 = {63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00 63 00 20 00 73
00 74 00 61 00 72 00}
        $str5 = {57 00 5C 00 5C 00 2E 00 5C 00 2A 00 3A 00}
        $str6 = {26 00 3D 00 25 00 53 00 25 00 63 00 74 00 3D 00 25 00 6C 00 64 00 25
00 53}

    condition:
        uint16(0) == 0x5a4d and
        filesize < 1500KB and
        all of ($str*)
}
```

```
rule targeted_UNC6384_CanonStager_Loader: extended description
{
    meta:
        description = "Detects CanonStager DLL loader used for side-loading PlugX
payload"
        author = "Arctic Wolf Labs"
        distribution = "TLP:GREEN"
        version = "1.0"
        last_modified = "2025-10-12"
        hash1_sha256 =
"e53bc08e60af1a1672a18b242f714486ead62164dda66f32c64ddc11ffe3f0df"

    strings:
        $str1 = ".dat" wide
        $str2 = "\\cnmplog" wide

        // RC4 decryption loop patterns
        $code1 = {43 0F B6 ?? 0F B6 [3]00 D0 0F B6 ?? 8A 74 [2]88 74 [2]88 54 [2]8B 7?
[2]02 54 [2]0F B6 ?? 0F B6 [3]32 14 ?? [0-4] 88 14 ?? 41 39 ?? 75 C?}
        $code2 = {0F B6 [3] 89 ?? 83 E? 0F 00 D0 02 ?? [1-2] 0F B6 ?? 8A 74 [2] 88 74
[2] 4? 88 54 [2]81 F? 00 01 00 00 75 D?}
        $code3 = {40 89 ?? 0F B6 C0 0F B6 [3]00 D9 88 9? [4-5]0F B6 F? 8A 7C 3? ?? 88
7C 0? ?? 88 5C 3? ?? 02 5C 0? ?? 0F B6 F? 0F B6 5C 3? ??}

    condition:
        uint16(0) == 0x5a4d and
        all of ($str*) and
        2 of ($code*)
}

rule targeted_UNC6384_LNK_Exploitation: extended description
{
    meta:
        description = "Detects malicious LNK files exploiting ZDI-CAN-25373 to deploy
UNC6384 payloads"
        author = "Arctic Wolf Labs"
        distribution = "TLP:GREEN"
        version = "1.0"
        last_modified = "2025-10-12"

    strings:
        $lnk_header = {4C 00 00 00 01 14 02 00}
        $powershell = "powershell" nocase
        $tar_extract = "tar" nocase
        $cnmpaui = "cnmpaui.exe" nocase
        $temp_path = "$Env:temp" nocase ascii wide
        $readbytes = "ReadAllBytes" nocase

    condition:
        $lnk_header at 0 and
        filesize < 10KB and
        $powershell and
        $tar_extract and
        ($cnmpaui or $temp_path) and
        $readbytes
}
```

Detailed MITRE ATT&CK® Mapping

Tactic	Technique	Procedure	Evidence

Resource Development	T1587.001 – Develop Capabilities: Malware	Refinement of CanonStager from approx. 700KB in May to 4KB in October.	Comparisons of the CanonStager loader component between the sample documented by GTIG and samples found in early September and October 2025 indicates active development and refinement of the malware delivery mechanism.
Resource Development	T1608.001 – Stage Capabilities: Upload Malware	UNC6384 actors staged malware on their infrastructure for direct download onto compromised devices.	Observed delivery infrastructure used to deliver their payloads: mydownload.z29[.]web.core.windows[.]net mydownloadfile[.]z7.web.core.windows[.]net mydownfile[.]z11.web.core.windows[.]net d32tpl7xt7175h[.]cloudfront[.]net
Initial Access	T1566.001 – Phishing: Spearphishing Attachment	Delivery of malicious LNK files via targeted emails themed around diplomatic conferences and meetings.	LNK files: Agenda_Meeting 26 Sep Brussels.lnk, JATEC workshop lure, EPC invitation letter.
Initial Access	T1189 – Drive-by Compromise	Captive portal hijacking redirecting browsers to malicious update pages (documented in Google research).	GTIG documentation of AitM attacks redirecting legitimate captive portal checks.
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell	LNK files execute obfuscated PowerShell commands to extract and decompress TAR archives.	PowerShell commands in LNK files extract rjnlzlkfe.ta and krnqdyvmlb.ta.
Execution	T1059.001 – Command and Scripting Interpreter: JavaScript	JavaScript file delivers cnmpaui.exe, cnmpaui.dll and cnmpaui.dat.	The JavaScript facilitated payload CanonStager and PlugX retrieval from the same CloudFront-based C2.
Execution	T1204.002 – User Execution: Malicious File	User opens LNK file disguised as conference agenda or policy document.	Diplomatic-themed file names leveraging authentic event details.
Execution	T1106 – Native API	Both CanonStager and PlugX use dynamic API resolution native API calls.	UNC6384 uses native API calls in CanonStager to load and execute the PlugX payload via EnumSystemGeoID. PlugX uses a variety of dynamically resolved APIs.
Execution	T1129 – Shared Modules	LoadLibraryA is called by PlugX to load additional modules.	PlugX calls LoadLibraryA to load the following modules: advapi32.dll, Ws2_32.dll, User32.dll, Shell32.dll, Shlwapi.dll, Psapi.dll, Version.dll, Msvrt.dll, Winhttp.dll, Ole32.dll
Persistence	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Creation of registry Run key entries pointing to malware in AppData directories.	Registry key: Software\Microsoft\Windows\CurrentVersion\Run\CanonPrinter
Defense Evasion	T1574.002 – Hijack Execution Flow: DLL Side-Loading	Malicious DLL loaded by legitimate signed Canon printer assistant binary.	cnmpaui.exe (legitimate signed) loading malicious cnmpaui.dll.
Defense Evasion	T1027 – Obfuscated Files or Information	RC4 encryption of PlugX payload, code obfuscation, control-flow flattening.	cnmplog.dat encrypted with 16-byte RC4 key, MSGInitialize implements control-flow flattening obfuscation
Defense Evasion	T1027.009 – Obfuscated Files or Information: Embedded Payloads	PlugX payload embedded within encrypted .dat file alongside legitimate binaries.	cnmplog.dat containing encrypted PlugX within TAR archive.
Defense Evasion	T1055 – Process Injection	In-memory loading of PlugX payload into legitimate cnmpaui.exe process space.	Manual PE mapping and execution via EnumSystemGeoID callback.
Defense Evasion	T1140 – Deobfuscate/Decode Files or Information	Runtime decryption of encrypted payload and strings.	RC4 decryption of cnmplog.dat, runtime string decryption in PlugX.
Defense Evasion	T1036.005 – Masquerading: Match Legitimate Name or Location	Malware uses printer-related directory and file names mimicking legitimate software.	Directory names: SamsungDriver, DellSetupFiles; Registry value: CanonPrinter.
Defense Evasion	T1218 – System Binary Proxy Execution	Execution through legitimate signed binary to evade application whitelisting.	Legitimate Canon cnmpaui.exe with valid expired certificate loading malicious DLL.
Defense Evasion	T1497.001 – Virtualization/Sandbox Evasion: System Checks	CheckRemoteDebuggerPresent API calls to detect debugging environments.	API calls documented in malware analysis section.
Defense Evasion	T1553.002 – Subvert Trust Controls: Code Signing	Use of legitimately signed binaries and stolen/expired code signing certificates.	Canon binary signed by Symantec Class 3, GTIG documented STATICPLUGIN signed by Chengdu Nuoxin Times Technology.

Defense Evasion	T1562.001 – Impair Defenses: Disable or Modify Tools	Anti-debugging techniques and checks to prevent analysis.	CheckRemoteDebuggerPresent, anti-analysis obfuscation.
Discovery	T1082 – System Information Discovery	Collection of system information for C2 check-in and fingerprinting.	Initial C2 check-in with system fingerprint data in URL parameters.
Discovery	T1083 – File and Directory Discovery	Malware searches for and reads files in user profile directories.	PowerShell get-childitem commands, file system enumeration.
Discovery	T1057 – Process Discovery	Enumeration of running processes for anti-analysis and operational purposes.	Standard PlugX reconnaissance capabilities.
Discovery	T1012 – Query Registry	Registry queries for Internet Explorer version, proxy settings, and system configuration.	Registry queries: Software\CLASSES\ms-pu Value CLSID Software\Microsoft\Windows\CurrentVersion\InternetSetting Value ProxyEnable, ProxyServer Software\Microsoft\Internet Explorer\Version Vector Value IE Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform Software\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols	HTTPS communication over port 443 for C2 traffic.	WinHttpConnect to C2 domains over port 443.
Command and Control	T1573.001 – Encrypted Channel: Symmetric Cryptography	HTTPS encryption of C2 communications.	TLS certificates on C2 domains, HTTPS protocol usage.
Command and Control	T1132.001 – Data Encoding: Standard Encoding	Encoding of C2 parameters and data in URL query strings.	URL parameters with encoded data: /download?t=1760103992&LeQa=PKDugp
Command and Control	T1001.003 – Data Obfuscation: Protocol Impersonation	Impersonation of legitimate browser traffic through user agent strings.	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0…).
Command and Control	T1105 – Ingress Tool Transfer	Download of additional payloads and tools from C2 infrastructure.	STATICPLUGIN downloading MSI packages, potential for additional tool deployment.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Data exfiltration through established HTTPS C2 channels.	Standard PlugX exfiltration capabilities over C2 infrastructure.

About Arctic Wolf Labs

Arctic Wolf Labs is a group of elite security researchers, data scientists, and security development engineers who explore security topics to deliver cutting-edge threat research on new and emerging adversaries, develop and refine advanced threat detection models with artificial intelligence and machine learning, and drive continuous improvement in the speed, scale, and detection efficacy of Arctic Wolf's solution offerings.

Arctic Wolf Labs brings world-class security innovations to not only Arctic Wolf's customer base, but the security community at large.