

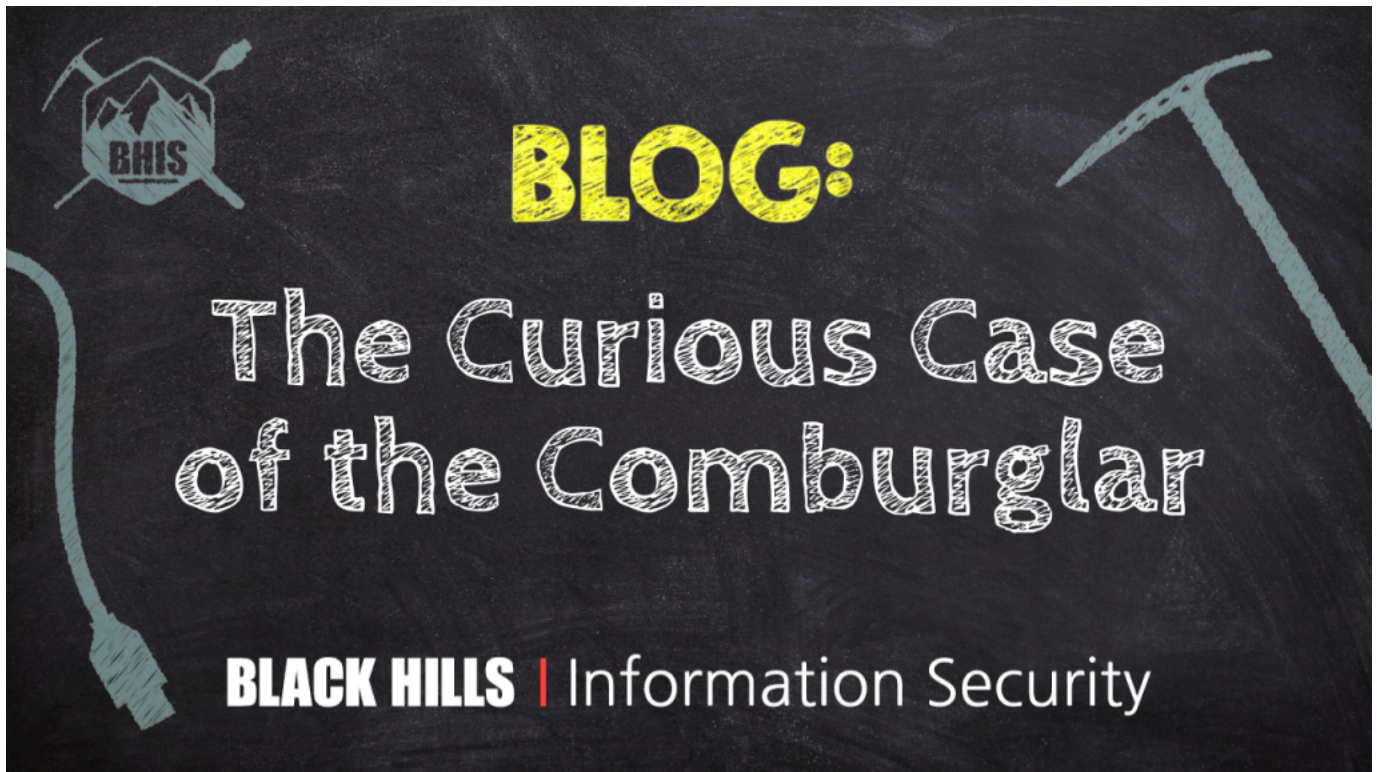
The Curious Case of the Comburlar

 blackhillsinfosec.com/the-curious-case-of-the-comburlar

BHIS

December 18, 2025

By [Troy Wojewoda](#)



During a recent Breach Assessment engagement, BHIS discovered a highly stealthy and persistent intrusion technique utilized by a threat actor to maintain Command-and-Control (C2) within the client's network. The attacker had modified Scheduled Tasks in the environment to use a **ComHandler** to create and execute a method within a registered Component Object Model (COM)¹, leveraging custom surrogate DLL files for code execution. The attacker particularly targeted tasks named *User_Feed_Synchronization-{GUID}* to carry out this technique. BHIS currently tracks this activity under the moniker *UKC-1230*.

This technique allowed the threat actor to remain persistent in the environment for at least seven months. BHIS also found evidence in the wild that indicates the attacker and associated threat activity have been in use for over a year, with related artifacts dating back nearly two years, as early as January 31, 2024.

Investigative Discoveries

During the collection phase of the Breach Assessment, BHIS was made aware of an alert that had fired in the customer's SOC – an alert on a file hash from an incident that occurred a month prior to the engagement with BHIS.

SHA256 Hash: 407d179f920342312dd526abc8a194b2620d0b19a95032dd36eeb70ec3bf5d65

Filename: C:\ProgramData\Microsoft\Windows\{0759c13d-5d0f-4513-8707-98a6cc3536d5}.dll

BHIS performed a triage collection and analyzed the system. Pivoting on the *GUID* value associated with the DLL name, a scheduled task named *User_Feed_Synchronization-{0759c13d-5d0f-4513-8707-98a6cc3536d5}* was uncovered. BHIS inspected the task's contents which revealed the use of a **ComHandler** to execute code.

```
<AllowStartOnDemand>true</AllowStartOnDemand>
<Enabled>true</Enabled>
<Hidden>false</Hidden>
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>PT0M</ExecutionTimeLimit>
<Priority>7</Priority>
<RestartOnFailure>
  <Interval>PT1M</Interval>
  <Count>1</Count>
</RestartOnFailure>
</Settings>
<Actions Context="Author">
  <ComHandler>
    <ClassId>{0759c13d-5d0f-4513-8707-98a6cc3536d5}</ClassId>
  </ComHandler>
</Actions>
```

Malicious ComHandler Setting – User_Feed_Synchronization Scheduled Task

This configuration setting was highly suspicious because although **ComHandler** activity can be common in certain scheduled tasks on Windows OS's, it is atypical for tasks of *User_Feed_Synchronization-{GUID}*.

For comparative purposes, a normal/benign *User_Feed_Synchronization-{GUID}* configuration references the Windows executable file, *msFeedsync.exe* at *C:\WINDOWS\system32\msFeedsync.exe*. This scheduled task type is a legacy carryover from earlier Windows OS's and is still found on supported versions of the OS today.

```
<Actions Context="Author">
  <Exec>
    <Command>C:\WINDOWS\system32\msfeedssync.exe</Command>
    <Arguments>sync</Arguments>
  </Exec>
</Actions>
```

Normal/Benign Command Setting in User_Feed_Synchronization Scheduled Task

Following the ComHandler Action

A COM object is typically an in-process COM server (a surrogate DLL, as determined by the *ClassId* lookup in the Windows Registry); it cannot run on its own and requires a host process to execute its code. This host process is *dllhost.exe*, also known as the *COM Surrogate* process, and is a necessary component of the Microsoft Windows OS. It acts as a generic host process for surrogate DLLs.

Knowing the *ClassId* value, the following registry path can be used to determine where on disk the associated DLL resides:

```
Registry::HKEY_CLASSES_ROOT\CLSID\{<ClassId-value>}\InprocServer32
```

The following PowerShell command was used during the Breach Assessment to query the registry key's value at

```
Registry::HKEY_CLASSES_ROOT\CLSID\{0759c13d-5d0f-4513-8707-98a6cc3536d5}\InprocServer32
Get-ItemProperty -Path 'Registry::HKEY_CLASSES_ROOT\CLSID\{0759c13d-5d0f-4513-8707-98a6cc3536d5}\InprocServer32' (default) : C:\ProgramData\Microsoft\Windows\{0759c13d-5d0f-4513-8707-98a6cc3536d5}.dll
```

The default value of the *InprocServer32* key pointed to the attacker attributed DLL file at *C:\ProgramData\Microsoft\Windows\{0759c13d-5d0f-4513-8707-98a6cc3536d5}.dll*

BHIS used the following yara rule to scan the environment which uncovered several additional compromised hosts.

```
rule ComHandler {
  meta:
    author = "Breach Assessment"
    date = "2024-01-31"
    version = "1.0"
  strings:
    $GUID = "GUID"
    $ComHandlerTag = "ComHandler"
  condition:
    $GUID at $GUID or $ComHandlerTag at $ComHandlerTag
}
```

It should be noted that the above yara rule can be applied to any scheduled task; however, care should be taken to avoid scheduled tasks where a *ComHandler* may be used legitimately.

BHIS found that scanning efforts scoped to target scheduled tasks at *C:\Windows\System32\Tasks\User_Feed_Synchronization-{...}* proved to have the highest fidelity detection from a true positive perspective since this task is: a.) native to Windows, and b.) designed to invoke *msfeedsync.exe* (i.e., not execute via a *ComHandler*).

In one instance, an administrator logged onto a server, triggering an attacker-modified scheduled task. The system then attempted to beacon to the address *38[.]180[.]143[.]167* which at the time was resolved from the domain *push[.]techdataservice[.]us*

For each attacker-modified scheduled task found, BHIS collected the location of the surrogate DLL cataloged in the registry at *Registry::HKEY_CLASSES_ROOT\CLSID\{<ClassId-value>}\InprocServer32*

In all instances but one, the surrogate DLL was located at:

```
C:\ProgramData\Microsoft\Windows\{GUID}.dll
```

One host was found with the associated DLL located at:

```
C:\Users\%UserProfile%\AppData\Local\Microsoft\Windows\{GUID}.dll
```

Every surrogate DLL found in the environment was named with the pattern *{GUID}.dll*

Additionally, each attacker-attributed DLL file was found to have a different file hash, indicating that searching/hunting via file hashes is the least effective approach in detecting this activity. Conversely, the one consistent observable was that all the DLL files shared the same Import Table Hash (imphash), *c4f69d93110080cc2432c9cc3d2c58ab*. This proved to be a solid indicator and was also used by BHIS to discover additional related DLLs in the wild.

Furthermore, looking for file creation events where the filename matches the regular expression (regex) pattern, *{[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}}\.dll*, could be used as an alternative for hunting efforts if the *imphash* is not an option. BHIS used this method in both the compromised environment as well as threat hunting against BHIS SOC customers' telemetry; no false positives were identified using those methodologies.

The earliest indicator of compromise found in the Breach Assessment environment was a scheduled task modified on March 19, 2025, at 16:00:25 UTC, with the associated surrogate DLL created seven minutes later at 16:07:24 UTC.

Because the environment lacked historical log collection for the affected systems and this technique persisted for several months prior to BHIS's involvement, efforts to identify the initial entry vector proved inconclusive.

Pivots in the Wild

The domain *techdataservice[.]us* was registered on September 5, 2024, with *push[.]techdataservice[.]us* still resolving to *38[.]180[.]143[.]167* when this blog article was published. BHIS found several other FQDNs and IP addresses associated with the *techdataservice[.]us* domain, which are listed in the IOC table below.

All surrogate DLLs discovered in the environment had the same *imphash* of *c4f69d93110080cc2432c9cc3d2c58ab*. This enabled BHIS to uncover additional files in the wild – all file hashes discovered to date are listed in the IOC table below.

Another interesting artifact was that all the DLLs found had a compile date/time of *2024-01-31 07:04:38 UTC* and although this attribute can be modified/spoofed, BHIS observed a related DLL that was "first seen" by VirusTotal the same day, at *2024-01-31 11:27:00 UTC*:

Moreover, BHIS found three executable files that were identified by VirusTotal as having contact with one or more domains of *techdataservice[.]us*

File 1 (note: identical compile date/time as surrogate DLLs)

SHA256 Hash: *1a783fcab9ae545dee58228b38dc9d4fa9c2d0dc35c23f4f5a9d01303ecabd72*

Purported Filename: *doc_20240930_Prenuptial_Agreement.exe*

First seen: *2024-09-30 17:36:01 UTC*

Compiled Date: *2024-01-31 07:04:38 UTC*

File 2

SHA256 Hash: 9ed58663f7a0bb01c0d9e058a376e78f6748fa4a89e69a9e4598312b3ba75a0c

Purported Filename: Contract_3Bormann_fully.exe

First seen: 2025-03-05 20:55:04 UTC

Compiled Date: 2023-06-29 08:00:00 UTC

File 3

SHA256 Hash: a68bcf09f8c83c67dfe0b17030367ebccf0905f4f531663c73b990202e2a13b0

Purported Filename: PT-20934_MKhan_Contract_fully.exe

First seen: 2025-03-07 17:27:14 UTC

Compiled Date: 2023-06-29 08:00:00 UTC

Although no evidence of these three files was found in the engagement environment, BHIS believes these malicious files were likely used by *UKC-1230* in related campaigns, possibly within other victim networks.

Threat Hunting and Detection Opportunities for UKC-1230 Activity

Active SOC customers are already covered by the activity detailed in this blog.

At the time of this publication, the domains, IP addresses, and surrogate DLL files were found to have very little (if any) malicious reputations when referencing OSINT sources.

For organizations looking to threat hunt or detect this activity, BHIS recommends the following:

1. **Search for IOCs:** Utilize the IOCs (particularly the *imphash*) listed in the IOC table below. Perform retroactive searches for the domains and IP addresses also provided.
2. **Inspect Scheduled Tasks for ComHandler:** Inspect all scheduled tasks of *User_Feed_Synchronization-{GUID}* for signs of *ComHandler* actions. Expand this effort to look for other common scheduled tasks that are not normally associated with *ComHandler* activity. Utilize the yara rule provided in this article. For organizations unable to leverage yara, the following PowerShell query can be used supplementally:

```
Write-Host "Host file (host) path: $Path" | ForEach-Object { if (Select-String -Path $.FullName -Pattern '<ClassId>' -Quiet) { Write-
```

3. **Look for File Creation Events of {GUID}.DLL:** File creation events of DLLs with a filename pattern `[[0-9a-fa-f]{8}-[0-9a-fa-f]{4}-[0-9a-fa-f]{4}-[0-9a-fa-f]{4}]-[0-9a-fa-f]{12}}\*.dll`. The following Sigma rule is provided as an example for organizations that utilize Sysmon:

```
title "File Creation Events of {GUID}.DLL"
meta:
  author: "BHIS"
  date: "2025-03-07"
  logsource:
    product: "Microsoft Windows"
    provider: "Sysmon"
  detection:
    - selection1:
        FileCreated:
          - FileName: "[0-9a-fa-f]{8}-[0-9a-fa-f]{4}-[0-9a-fa-f]{4}-[0-9a-fa-f]{4}]-[0-9a-fa-f]{12}*.dll"
```

Note: Sysmon EventID-29 (FileExecutableDetected) contains the *imphash* of executable files created; therefore, searching/alerting on the *imphash* `c4f69d93110080cc2432c9cc3d2c58ab` will yield greater true positive results than filename patterns.

Summary

BHIS identified a long-term persistence technique during a breach assessment where a threat actor, tracked as *UKC-1230*, modified Windows Scheduled Tasks to maintain C2 and access to environment. The attacker replaced the normal execution of *msfeedsync.exe* in *User_Feed_Synchronization-{GUID}* tasks with a *ComHandler* that invoked malicious surrogate DLLs registered as *COM objects* and executed via the host process *dllhost.exe*. These DLLs, named using GUID patterns matching their respective scheduled task name, shared the same *imphash* but had unique file hashes, making file hash-based detection ineffective. The intrusion persisted for at least seven months, with evidence suggesting *UKC-1230* was active with this technique for nearly two years and may still be active in other victim environments. Any network traffic associated to the domain `techdataservice[.]us` and its subdomains should be investigated immediately.

Active SOC customers are covered by this activity and will receive continual updates as new information is discovered.

For organizations interested in BHIS services, including Active SOC, Breach Assessment, or Incident Response services, please contact BHIS at: <https://www.blackhillsinfosec.com/contact-us/>

Yara Rule(s)

```
rule "Yara Rule(s)" {
  meta:
    author: "BHIS"
    date: "2025-03-07"
    logsource:
      product: "Microsoft Windows"
      provider: "Sysmon"
    detection:
      - selection1:
          FileCreated:
            - FileName: "[0-9a-fa-f]{8}-[0-9a-fa-f]{4}-[0-9a-fa-f]{4}-[0-9a-fa-f]{4}]-[0-9a-fa-f]{12}*.dll"
```

Indicators of Compromise (IOCs)

Indicator	Type	Description
23.95.182.21	IPv4 Address	IP address associated with C2 traffic (resolved from push.telemetry.techdataservice [.] us)
38.180.143.167	IPv4 Address	IP address associated with C2 traffic (resolved from push.telemetry.techdataservice [.] us, mdns.techdataservice [.] us)
52.129.44.42	IPv4 Address	IP address associated with C2 traffic (resolved from ch9.techdataservice [.] us)
87.121.61.185	IPv4 Address	IP address associated with C2 traffic (resolved from ch7.techdataservice [.] us)
87.121.61.251	IPv4 Address	IP address associated with C2 traffic (resolved from ch6.techdataservice [.] us and ch7.techdataservice [.] us)
88.99.163.99	IPv4 Address	IP address associated with C2 traffic (resolved from ch3.techdataservice [.] us, console.techdataservice [.] us)
104.225.131.18	IPv4 Address	IP address associated with C2 traffic (resolved from ch4.techdataservice [.] us, sync.techdataservice [.] us)
techdataservice [.] us	Domain	Root domain used for C2. Registered on: 2024-09-05
ch3.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 88.99.163.99
ch4.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 104.225.131.18
ch6.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 87.121.61.251
ch7.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 87.121.61.251, 87.121.61.185
ch9.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 52.129.44.42
console.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 104.225.131.18
mdns.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 38.180.143.167
push.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 38.180.143.167
sync.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 104.225.131.18
telemetry.techdataservice [.] us	FQDN	Fully qualified domain name associated with malicious DLL domain Resolved to: 23.95.182.21, 38.180.143.167
0073473b4baf3c29156597aab6d948fe7dc91972fdf350f88753e1e9e5217009	SHA256 Hash	SHA256 hash of malicious DLL found in wild (imphash match 2025-11-26 16:34:35 UTC Compiled date: 2024-01-31 07:04:38 UTC
1a783fcab9ae545dee58228b38dc9d4fa0c2d0dc35c23f4f5a9d01303ecabd72	SHA256 Hash	SHA256 hash of file found in wild (attacker-attributed infrastructure). Filename: doc_20240930_Prenuptial_Agreement.docx First seen: 2024-09-30 17:36:01 UTC Compiled Date: 2024-01-31 07:04:38 UTC
1f529a76faea1e7fa56cbc24c66ddeb5a18d025af654c7e92635d9866e22819d	SHA256 Hash	SHA256 hash of malicious DLL file dropped to disk and launched modified scheduled tasks First seen: <not observed in the wild Compiled date: 2024-01-31 07:04:38 UTC
3e9efef4121da751f36070a7ffed49eb1b1f72831651e8ecf47e45dd7602c05e	SHA256 Hash	SHA256 hash of malicious DLL found in wild (imphash match 2025-11-13 17:14:17 UTC Compiled date: 2024-01-31 07:04:38 UTC
3f5bc475d9394d352341b1f843b85cfb300e363dd27d4ca867e9e6d54317d881	SHA256 Hash	SHA256 hash of malicious DLL found in wild (imphash match 2024-01-31 11:27:00 UTC Compiled date: 2024-01-31 07:04:38 UTC

407d179f920342312dd526abc8a194b2620d0b19a95032dd36eeb70ec3bf5d65	SHA256 Hash	SHA256 hash of malicious DLL file dropped to disk and laur modified scheduled tasks First seen: 2025-03-05 20:58:53 Compiled date: 2024-01-31 07:04:38 UTC
498eaa0d4e5dfa6495a8c3308a3f02f38841809b0d3cab86448b559dbbe8e47c	SHA256 Hash	SHA256 hash of malicious DLL found in wild (imphash matc 2025-11-13 17:22:03 UTC Compiled date: 2024-01-31 07:04:38 UTC
4a85f0d06561ea94150fd84a536993119ba62638e23b95cecac3e17fc21874cb	SHA256 Hash	SHA256 hash of malicious DLL found in wild (imphash matc 2025-09-12 21:46:12 UTC Compiled date: 2024-01-31 07:04:38 UTC
9ed58663f7a0bb91c0d9e058a376e78f6748fa4a88e69a0e4598312b3ba75a0c	SHA256 Hash	SHA256 hash of file found in wild (attacker-attributed infrastructure). Filename: Contract_JBornmann_fully.exe 03-05 20:55:04 UTC Compiled date: 2023-06-20 08:00:00 UTC
a68bcf09f8c83c67dfe0b17030367ebccf0905f4f531663c73b990202e2a13b0	SHA256 Hash	SHA256 hash of file found in wild (attacker-attributed infrastructure). Filename: PT-20934_MKhan_Contract_full 2025-03-07 17:27:14 UTC Compiled date: 2023-06-20 08:00:00 UTC
c4f69d93110080cc2432c9cc3d2c58ab	imphash	Import table hash of malicious DLL files

Psst If you liked this blog, we think you'd enjoy Troy's class:

[Network Forensics and Incident Response](#)

Available live/virtual and on-demand!



1. <https://learn.microsoft.com/en-us/windows/win32/com/the-component-object-model> ↵
2. <https://www.virustotal.com/gui/file/3f5bc475d9394d352341b1f843b85cfb300e363dd27d4ca867e9e6d54317d881/details>