ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access

mandiant.com/resources/blog/alphv-ransomware-backup

Mandiant has observed a new ALPHV (aka BlackCat ransomware) ransomware affiliate, tracked as UNC4466, target publicly exposed Veritas Backup Exec installations, vulnerable to CVE-2021-27876, CVE-2021-27877 and CVE-2021-27878, for initial access to victim environments. A commercial Internet scanning service identified over 8,500 installations of Veritas Backup Exec instances that are currently exposed to the internet, some of which may still be unpatched and vulnerable. Previous ALPHV intrusions investigated by Mandiant primarily originated from stolen credentials suggesting a shift to opportunistic targeting of known vulnerabilities. This blog post covers the UNC4466 attack lifecycle, indicators, and detection opportunities.

ALPHV emerged in November 2021 as a ransomware-as-a-service that some researchers have claimed is the successor to BLACKMATTER and DARKSIDE ransomware. While some ransomware operators enacted rules to avoid impacting critical infrastructure and health entities, ALPHV has continued to target these sensitive industries.

Timeline

- In March 2021, Veritas published an advisory reporting three critical vulnerabilities in Veritas Backup Exec 16.x, 20.x and 21.x.
- On September 23, 2022, a METASPLOIT module was released which exploits these vulnerabilities and creates a session which the threat actor can use to interact with the victim system.
- On October 22, 2022, Mandiant first observed exploitation of the Veritas vulnerabilities in the wild.

Attack Phases

Initial Compromise and Establish Foothold

In late 2022, UNC4466 gained access to an internet-exposed Windows server, running Veritas Backup Exec version 21.0 using the Metasploit module \`exploit/multi/veritas/beagent_sha_auth_rce\`. Shortly after, the Metasploit persistence module was invoked to maintain persistent access to the system for the remainder of this intrusion.

Internal Reconnaissance

After gaining access to the Veritas Backup Exec server, UNC4466 used Internet Explorer, the browser installed by default on older Windows systems, to download Famatech’s Advanced IP Scanner from its website, hxxps://download.advanced-ip-scanner[.]com. This tool is capable of scanning individual IP addresses or IP address ranges for open ports, and returns hostnames, operating system and hardware manufacturer information.

UNC4466 also made use of ADRecon to gather network, account, and host information in the victim’s environment. When executed by a privileged domain account, ADRecon generates several reports about the Active Directory environment, including the Trusts, Sites, Subnets, password policies, user and computer account listings. These reports can be generated in a variety of formats, including CSV, XML, JSON, and HTML.

Ingress Tool Transfer

UNC4466 made heavy use of the Background Intelligent Transfer Service (BITS) to download additional tools such as LAZAGNE, LIGOLO, WINSW, RCLONE, and finally the ALPHV ransomware encryptor.

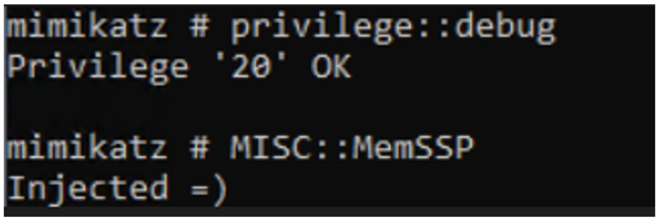
Command and Control

UNC4466 leveraged SOCKS5 tunneling to communicate with compromised systems in the victim network. This technique is typically used to evade network defenses or other preventative network controls. Two separate tools were deployed to execute this technique, LIGOLO and REVSOCKS.

Escalate Privileges

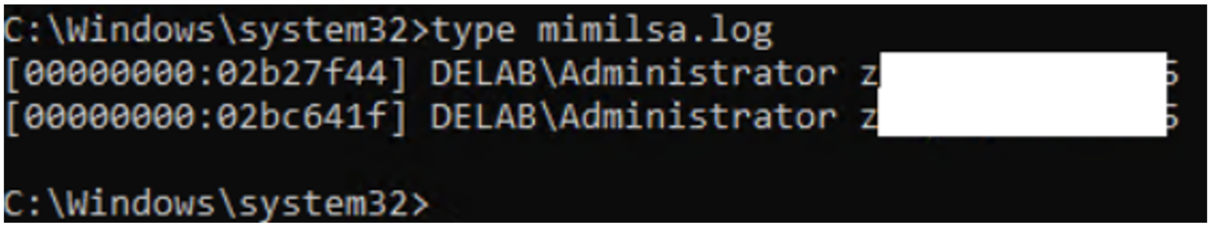
The threat actor utilized multiple credential access tools, including Mimikatz, LaZagne and Nanodump to gather clear-text credentials and credential material.

In November 2022, UNC4466 utilized the MIMIKATZ Security Support Provider injection module (`MISC::MemSSP`). This module collects credentials in clear text as they are used, by manipulating the Local Security Authority Server Service (LSASS) on victim systems. This module creates a file named `C:\Windows\System32\mimilsa.log`.



```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # MISC::MemSSP
Injected =)
```



```
C:\Windows\system32>type mimilsa.log
[00000000:02b27f44] DELAB\Administrator [redacted]
[00000000:02bc641f] DELAB\Administrator

C:\Windows\system32>
```

[Nanodump] was also used to dump LSASS memory. Like the examples shown on Helpsystems' GitHub page, the output file specified was a file in the `C:\Windows\Temp` directory.

Defense Evasion

During operations, UNC4466 takes steps to evade detection. Apart from clearing event logs, UNC4466 also used the built in Set-MpPrefernce cmdlet to disable Microsoft Defender’s real-time monitoring capability.

```
powershell.exe Set-MpPreference -DisableRealtimeMonitoring 1 -ErrorAction
SilentlyContinue
```

Command and Control

UNC4466 made use of BITS transfers (using the Start-BitsTransfer PowerShell cmdlet) to download various resources to the staging directory `c:\ProgramData`. Using this technique, SOCKS5 tunneling tools, REVSOCKS and LIGOLO were downloaded from their official GitHub repositories.

Complete Mission

UNC4466 deploys the Rust-based ALPHV ransomware. In Late 2022, UNC4466 added immediate tasks to the default domain policy. These tasks were configured to perform actions which disabled security software, downloaded the ALPHV encryptor, then execute it.

Exposure

As of this blog post's date, one commercial Internet scanning service reported over 8500 IP addresses which advertise the "Symantec/Veritas Backup Exec ndmp" service on the default port 10000, as well as port 9000 and port 10001. While this search result does not directly identify vulnerable systems, as the application versions were not identifiable, it demonstrates the prevalence of Internet exposed instances that could potentially be probed by attackers.

Detection Opportunities

Defenders should place priority on monitoring internet-exposed Veritas Backup Exec Windows installations, for versions before 21.2. Mandiant observed the exploitation of Veritas Backup Exec can leave a noticeable imprint on the Backup Exec log files. Where feasible, these log files should be forwarded to a SIEM or similar technology which enables detection and alerting when certain events are recorded.

In addition to any available network connection logging, Veritas Backup Exec logs will record evidence of connections to remote systems.

```
[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpsrvr]      + ndmpd.cpp (nnn):

[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpsrvr]      | Session 1 started

[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpsrvr]      - sslOpen() : Opening
SSL for: 0x00000

[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpsrvr]      - sslOpen(): certinfo =
0x00000; sslConn = 0x00000

[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpcomm]      - ndmpRun: Control
connection accepted : connection established between end-points [Server
IP]:10000 and [Remote IP]:[remote port]
```

These connections should be triaged for any unknown IP addresses. Additionally, these logs can also record the execution of suspicious pre and post backup job commands.

```
[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpsrvr]      -
SetPreCommandEnvironment: Could not obtain the BE Job ID to pass to the
command C:\Windows\System32\cmd.exe /c "C:\Windows\Temp\[random chars].exe"

[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpsrvr]      - Could not obtain the
BE Job Name to pass to the command C:\Windows\System32\cmd.exe /c
"C:\Windows\Temp\[random chars].exe"

[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpsrvr]      - At least one of the
Pre / Post Command environment variables could not be set

[nnnn] YYYY-mm-ddTHH:MM:SS.sss [ndmp\ndmpcomm]      - ndmp_readit: Caught
message on closed connection. Socket 0x8e0 len 0x0
```

UNC4466

- DS0015 - Application log
    - Backup Exec logs
        - Connections to unknown IP addresses
        - Suspicious pre or post job commands being set (SetPreCommandEnvironment/ SetPostCommandEnvironment). E.g: C:\Windows\System32\cmd.exe /c "C:\Windows\Temp\***UNKNOWN_EXEC***.exe”
    - Windows Event Logs
        - Suspicious BITS transfers with the source argument targeting unknown hosts and GitHub repositories.
        - Pre-ransomware activity: deletion of volume shadow copies
- DS0017 – Command
    - Disabling AMSI: use of Set-MpPreference PowerShell cmdlet
    - Ingress tool transfer: Use of Start-BitsTransfer PowerShell cmdlet

- DS0022 – File
  New Executables created in staging directories: C:\ProgramData, C:\Windows\Temp, C:\Windows\Tasks
- DS0024 – Windows Registry
  Modification of Registry run keys

Outlook

Mandiant recommends implementing secure access controls, segmenting networks, enabling multi-factor authentication, and regularly testing and evaluating backup strategies to limit the impact of a ransomware attack. Additionally, organizations should inventory externally facing services and reduce the attack surface available to attackers.

Acknowledgements

With special thanks to Nick Richard for technical review.

MITRE ATT&CK

Mandiant has observed UNC4466 use the following techniques:

ATT&CK Tactic Category	Techniques	
Impact		
	T1486:	Data Encrypted for Impact
	T1489:	Service Stop
	T1490:	Inhibit System Recovery
	T1529:	System Shutdown/Reboot
Execution		
	T1047:	Windows Management Instrumentation
	T1053:	Scheduled Task/Job

	T1053.005:	Scheduled Task
	T1059.001:	PowerShell
	T1059.006:	Python
	T1569.002:	Service Execution
Defense Evasion		
	T1027:	Obfuscated Files or Information
	T1027.002:	Software Packing
	T1027.009:	Embedded Payloads
	T1055:	Process Injection
	T1070.001:	Clear Windows Event Logs
	T1070.004:	File Deletion
	T1112:	Modify Registry
	T1134:	Access Token Manipulation
	T1134.001:	Token Impersonation/Theft
	T1222:	File and Directory Permissions Modification
	T1497:	Virtualization/Sandbox Evasion
	T1497.001:	System Checks
	T1548.002:	Bypass User Account Control

	T1562.001:	Disable or Modify Tools
	T1564.010:	Process Argument Spoofing
	T1574.011:	Services Registry Permissions Weakness
	T1620:	Reflective Code Loading
	T1622:	Debugger Evasion
	T1484.001	Domain Policy Modification: Group Policy Modification
Discovery		
	T1007:	System Service Discovery
	T1012:	Query Registry
	T1016:	System Network Configuration Discovery
	T1033:	System Owner/User Discovery
	T1057:	Process Discovery
	T1082:	System Information Discovery
	T1083:	File and Directory Discovery
	T1087:	Account Discovery
	T1135:	Network Share Discovery
Persistence		
	T1543:	Create or Modify System Process

	T1543.003:	Windows Service
	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Command and Control		
	T1095:	Non-Application Layer Protocol
	T1105:	Ingress Tool Transfer
Lateral Movement		
	T1021.001:	Remote Desktop Protocol
Collection		
	T1213:	Data from Information Repositories
Resource Development		
	T1583.003:	Virtual Private Server

Indicators of Compromise

da202cc4b3679fdb47003d603a93c90d	MIMIKATZ
5fe66b2835511f9d4d3703b6c639b866	NANODUMP
1f437347917f0a4ced71fb7df53b1a05	LIGOLO
b41dc7bef82ef384bc884973f3d0e8ca	REVSOCKS
c590a84b8c72cf18f35ae166f815c9df	Sysinternals PSEXEC

24b0f58f014bd259b57f346fb5aed2ea	WINSW
e31270e4a6f215f45abad65916da9db4	REVSOCKS
4fdabe571b66ceec3448939bfb3ffcd1	Advanced Port Scanner
68d3bf2c363144ec6874ab360fdda00a	LAZAGNE
ee6e0cb1b3b7601696e9a05ce66e7f37	ALPHV
f66e1d717b54b95cf32154b770e10ba4	METASPLOIT
17424a22f01b7b996810ba1274f7b8e9	METASPLOIT
45[.]61[.]138[.]109	
185[.]141[.]62[.]123	
5[.]199[.]169[.]209	
45[.]61[.]138[.]109:45815	
45[.]61[.]138[.]109:43937	
45[.]61[.]138[.]109:36931	
5[.]199[.]169[.]209:31600	
45[.]61[.]138[.]109:41703	
185[.]99[.]135[.]115:39839	
185[.]99[.]135[.]115:41773	
45[.]61[.]138[.]109:33971	

185[.]141[.]62[.]123:50810
185[.]99[.]135[.]115:49196
hxxp://185[.]141[.]62[.]123:10228/update[.]exe