FBI FLASH

FEDERAL BUREAU OF INVESTIGATION ♦ CYBER DIVISION

25 March 2022

FLASH Number

CU-000166-MW

SocGholish Malware Indicators of Compromise

Summary

SocGholish (aka FakeUpdates) is a JavaScript-based malware that masquerades as a legitimate browser update delivered to victims via compromised websites. SocGholish establishes an initial foothold onto victim networks that threat actors use for further targeting with ransomware. Since 2020, the FBI has observed SocGholish malware as the most common initial intrusion vector across multiple variants of ransomware suspected to be operated by subjects associated with the Evil Corp cybercriminal organization, including BitPaymer, WastedLocker, Hades, Phoenix, PayloadBIN, and Macaw Locker. SocGholish has infected thousands of US businesses, government, academic, non-profit, and healthcare organizations, resulting in subsequent ransomware events with losses ranging between $1 million and $40 million per incident.

Technical Details

SocGholish is delivered via compromised websites injected with JavaScript that redirects visitors to a series of malicious websites hosting SocGholish payloads. There are typically three stages to a SocGholish incident, with multiple browser redirects and obfuscated code used throughout to evade anti-virus detections.

In the initial stage, SocGholish collects victim browser information upon visiting the compromised website. The malware initiates a series of HTTP redirects before prompting the victim to download a software update for their web browser. The second stage initiates if the victim downloads the fake browser update, upon which the malware delivers a zipped JavaScript payload and executes with wscript.exe. The malware collects additional information about the victim host computer via whoami and netuser/netgroup commands, as well as PowerShell scripts, and communicates the information back to a command and control (C2) server. The final stage typically involves the delivery of a Cobalt Strike Beacon payload used by threat actors for further network reconnaissance and lateral movement, ultimately leading to ransomware deployment.

SocGholish C2 domains rotate regularly and often use hijacked subdomains of legitimate websites that can blend in with seemingly normal network traffic. Potential SocGholish C2 activity can be identified with the following domain pattern that has been observed by the FBI in SocGholish campaigns since 2018:

[8 random hex characters].subdomain.domain.topleveldomain

Indicators

IP Addresses:	
179.43.169.30	179.43.169.31
179.43.169.32	79.110.52.138
79.110.52.139	79.110.52.140

File Names and Hashes:
c495cfee1981974cf76d07193a3c6b6e45b04fff
033812cbd4ff548c14715078f8777777bf61f26d
10459c6ac3e90b1881aaea002cbeccfc56db51f1
3b1b5907f2781506f9561cd1f520ba8fcf18b462
a40e93621562911c5b68e959cc228de85c131a70
4c15f6373f626ec3805a5a80403541252236ae4a

File Names and Hashes:
f870379f1993228547acc5446085205ec7e4b04a
10459c6ac3e90b1881aaea002cbeccfc56db51f1
10459c6ac3e90b1881aaea002cbeccfc56db51f1
a40e93621562911c5b68e959cc228de85c131a70
d1bf6b1f8dad5da49556510c996192652400467e
10a13cb164d4ccfe573cf23555071c42ffeb40cd
bc1b4ae7a6171561aba09636c139719c8c358c78
854ece5389ca85cd7616befd27f8d4e0aa38ac38
7c8e4f2f79df91f0f929b0447c321eea2ad861c1
048a7b85d7a3c17781f2fa420a9e5e392b705c20
0fad03d96658c952382a074e5f7b305b6b132eaf
3340061cea2a8eb1116285a8284a80b3752f6148
cecd2af742ea6b06371b7b9961bc8fc6ab428dd0
8aa898ccae9a06f0d5e488a489b6b54a747be83c
9c57ee8be0d48d60ed46900e532ffb2ad43d89dd
3b64b2a97310a7bfcb9ce7abce3585a84b89c618
76e82eb8841a2afa435be65e9fed6e19f961508e
3a4848828e8e9f67da67ab8cbba5159fcdec1ef5
a738db6d900d34f651c0de322176bc2bca484288
6f7e9a1997113f840e075b84d31da03d8cd3fd9c
a733fb551022b82994191f8a1e052ca82656f205
f3e57b1d3e22c01ed5e060356df7f7e9707dba6d
e4e52cc23852243bc79536ae1b175f49ee8193ab
ec37bb517261285fb24df21e82963a878fdd009e
c25efbda7435671ea52c64630f3782c908599eb8
0ac2f3b75f5918d7e807e55b954ac0ef9998679a
582aa29e188a604d1a49fde0d9740f403fe9de93
f7533d2307b9bf449ea83ba48f58940217158251
a102e5be89558352cf29f27e011042f508d59b8f
e2825d27aabd7b2e4c011713bb65bbfd089c62dd
d69c336619e5de591270adbff395c969716b355c
505b375befa7e636679a6e97228e656b7144acbc
3246b0987e14f28970c23fe4104ffb26e017c1dd
01b71bd417c2d6b9900ba8028d7659cf67275d99
ff13f5e89c51b0b9af963d080ef0899c7a169080
8ea2e0d7b2eed28e0545fc517c5f9dd191354d93
5228c1e9a24dc8afc0134639e033867ae993a27a
2bbaaa4545e52824083cad51385f19a88ad2a9bd
c44858db442ccd3363613778c3dfdc491c3926e7
1cd433f3b9957efa2de55fd644ce9f4abd02ec24
a53f6c33ef607d583265a54289ee59682a152a0f

Domains:
C2 pattern -- [8 random hex characters].subdomain.domain.topleveldomain
*.edge.wholesalerandy.com
*.news.pocketstay.com
*.auth.codingbit.co.in
*.nodes.fioressence.com
*.push.youbyashboutique.com
*.click.clickanalytics208.com
*.green.mattingsolutions.co
*.login.lilscrambler.com
*.notify.aproposaussies.com
*.login.nuwealthmedia.com
*.jobs.tracybrey.com
*.second.pmservicespr.com
*.popcorn.net-zerodesign.com
*.minion.maxxcorp.net
*.news.nuwealthmedia.com

Information Requested:

Please contact the FBI if you are a victim of SocGholish. Provide timeline of compromise, details of post-compromise activity, and monetary losses incurred. Details on how to report are provided below.

Recommended Mitigations:

- Implement regular backups of data. Maintain backups offline, and ensure the data is encrypted and immutable.
- Store copies of data offline using multi-factor authentication with strong password protection.
- Install and regularly update antivirus software with real-time detection.
- Implement network segmentation to prevent accessibility across multiple machines on the network.
- Keep computers, devices and applications patched and up to date. Prioritize patching known exploited vulnerabilities. Timely patching is one of the most efficient and cost-

effective steps an organization can take to minimize its exposure to cybersecurity threats.

- Safeguard the network by enacting administrative privileges and configuring access controls with the least privilege in mind.
- Consider adding an email banner to emails received outside of your organization.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Disable hyperlinks in received emails.
- Use double authentication when logging into accounts or services.
- Identify, detect and investigate abnormal activity and potential traversal of the indicated ransomware with a network monitoring tool.
- Use Admin Disabling Tools to support identity and privileged access management.
- Implement time-based access for accounts set at the admin-level and higher.
- Disable command-line and scripting activities and permissions.

Additional Resources:

For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomware.gov is the U.S. Government's new, official one-stop location for resources to tackle ransomware more effectively.

CISA's Ransomware Readiness Assessment (RRA) is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). The Individual indicators is this report, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should be evaluated in light of additional context in this report and your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP: AMBER**. The information in this product may be shared with members of your organization, and with clients and customers who need to know the information to protect themselves or prevent future harm.