SocGholish Malware: A Real Threat from a Fake Update | Proofpoint US

By November 22, 2022 Andrew Northern

Published: 2022-11-21 · Archived: 2026-04-05 17:36:54 UTC

Key Findings:

- SocGholish, while relatively easy to detect, is difficult to stop.
- Careful campaign management makes analysis difficult for incident responders.
- SocGholish is delivered via injected JavaScript on compromised websites.
- Proofpoint attributes SocGholish activity to the threat actor TA569.

Overview

SocGholish is a malware variant which continues to thrive in the current information security landscape. By utilizing an extensive variety of stages, eligibility checks, and obfuscation routines, it remains one of the most elusive malware families to date. SocGholish was observed in the wild as early as 2018. The absence of details surrounding target selection, evasion logic, and specific procedures employed by TA569 and their use of SocGholish in the intermediary phases of infection contributes to this shroud of mystery.

SocGholish Details

SocGholish is primarily known for its “drive-by” download style of initial infection. Such attacks employ malicious JavaScript, which is injected into compromised, but otherwise legitimate, websites. If an unsuspecting victim receives an email containing a link to a compromised website and clicks on it, the injected JavaScript will execute upon the browser loading the page.

If the victim’s browser meets the eligibility requirements for infection (using a Windows host, originating from an external source, and specific cookie checks), the user will be presented with the download for a file masquerading as a browser update. By loading this update prompt from the intended domain, it bolsters the purported authenticity of the update.

This second stage prompts the user to download and execute. Additional eligibility checks are performed prior to serving a compressed archive containing a JavaScript file. An example of the filename would be “AutoUpdater.js.”

Once the targeted user executes the malicious payload, the third stage of the SocGholish attack chain begins. A series of Windows Management Instrumentation (WMI) calls are invoked by the parent process executing the JavaScript payload (wscript was observed in this current generation though cscript or other native Windows script hosts could be leveraged). These WMI calls serve to profile the system to ascertain further eligibility for additional follow-on payloads. Data such as domain trusts, username, and computer name are exfiltrated to the

attacker-controlled infrastructure. This reconnaissance phase is yet another opportunity for the TAs to avoid deploying their ultimate payload in an analysis environment.

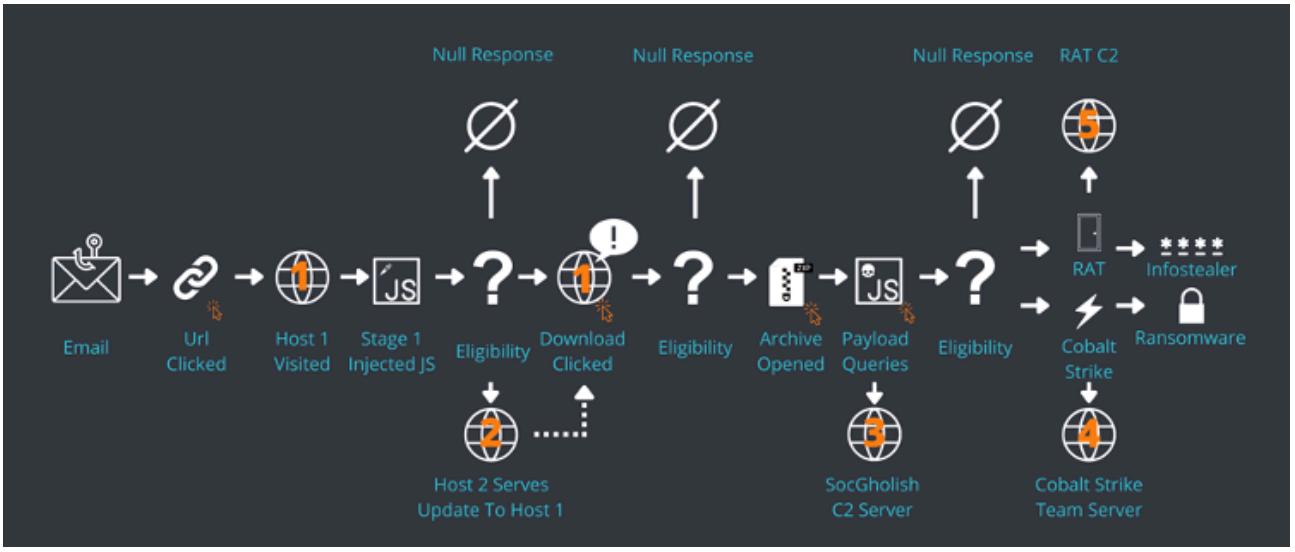

Figure 1: SocGholish Overview

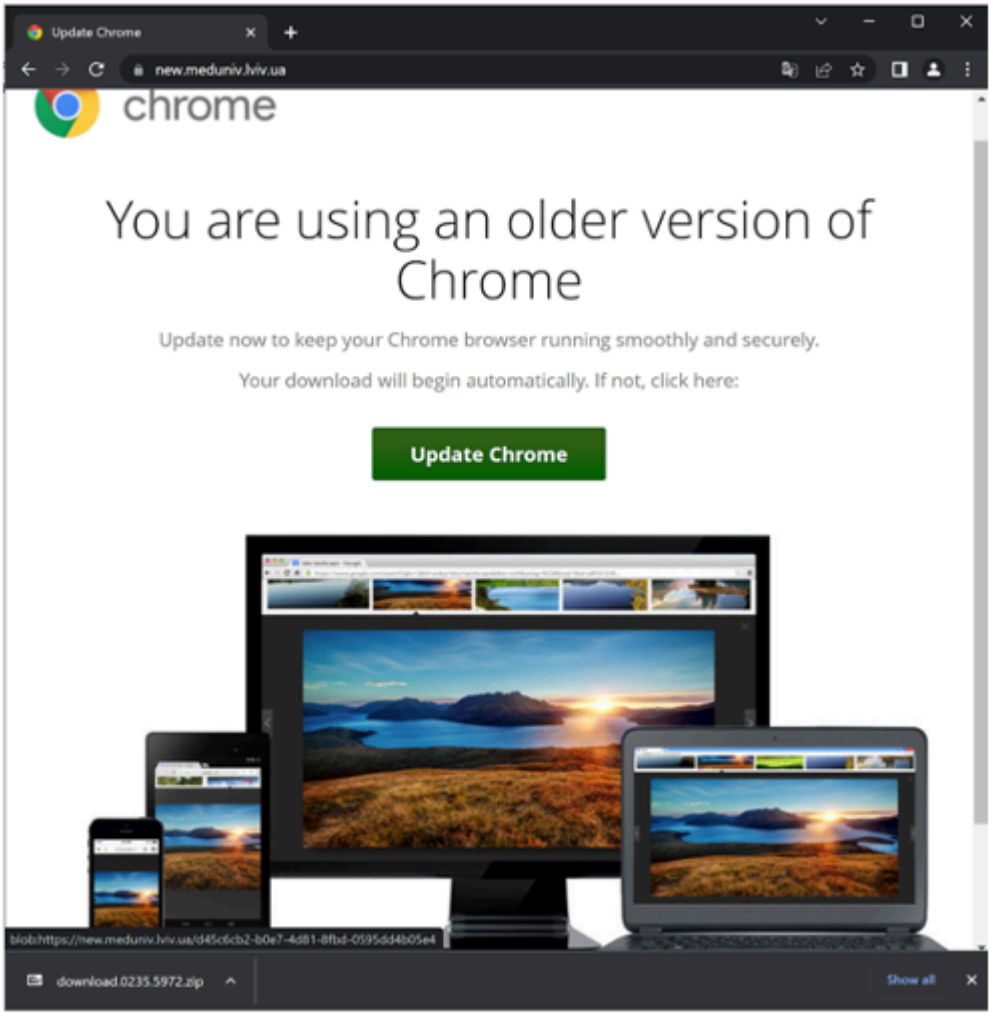

Figure 2: Fake Update Served

Initial Lure – Phishing OR Traffic Funneling?

While the tactics of most phishing campaigns are similar across the spectrum of malware, SocGholish deviates from norms by taking a pass on all traditional hallmarks of phishing campaigns.

- No observed call to action
- No observed sense of urgency
- No threats or promises of rewards
- No blatant trickery or misdirection

Instead, Threat Research has observed SocGholish being leveraged in email campaigns with injections on sites that meet one of two criteria:

1. Extensive marketing and legitimate email advertising campaigns.
2. Strong SEO (Search Engine Optimization) and page rank causing aggregation and dissemination by Google Alerts and other similar services.

It is worth noting though that the vast majority of SocGholish injects are not visible in email campaigns. At the date of publication, Threat Research is tracking over 1000 active implants while only observing a small fraction of those within our own data. According to a two-week sample of SocGholish infection traffic, Proofpoint identified nearly 300 infected websites targeting users in multiple countries, including Poland, Italy, France, Iran, Spain, Germany, the United Kingdom, and the United States, among others.

This begs the question, *"Are there multiple types of campaigns with distinct tactics and targeting?"*

The current generation of SocGholish implants requires a redirect from a specifically formatted source so simply typing in the URL and visiting the page is not enough to trigger the initial JavaScript. This, coupled with other observations, merits Threat Research to assess with moderate confidence that TAs are, in some aspect, relying on the aggregation of injected links by services like Google Alerts and other aggregate feeds and are not directly distributing the URLs via email. Rather, infected URLs are sent legitimately by a user, aggregate service, or marketing service without knowledge that the web page is injected with SocGholish.

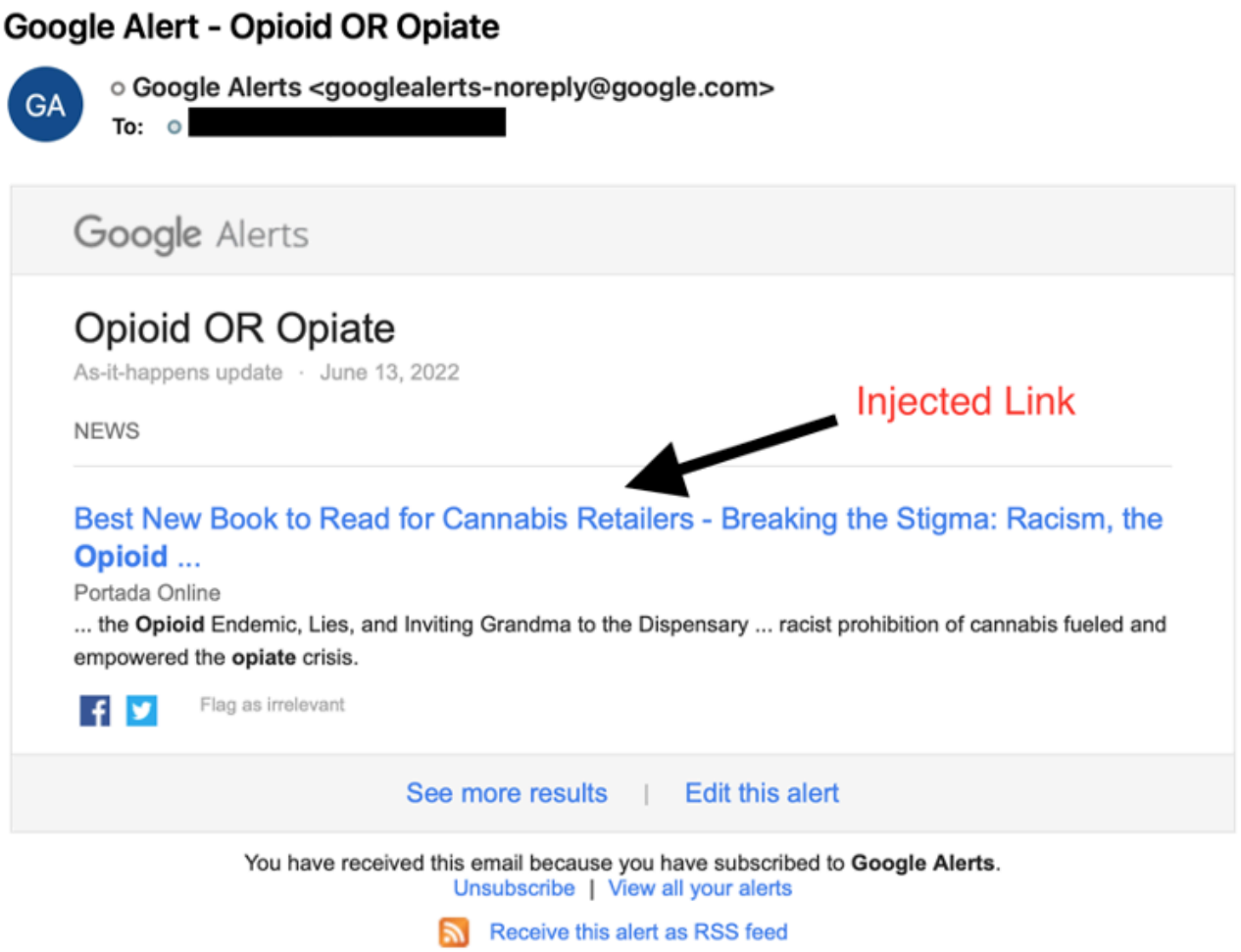

Figure 3: SocGholish delivered via Google Alert

Putting it All Together

Proofpoint assesses with high confidence TA569 is a financially motivated threat actor who almost certainly monetizes access gained through the exclusive use and sale of SocGholish infections. Through our investigation and collaboration with partners, Proofpoint has identified that malware deployed after SocGholish will vary based upon the profile of the infected victim's machine. If the target is domain joined, ransomware, including but not limited to WastedLocker, Hive, and LockBit, is commonly deployed according to a variety of incident response journals. If the victim is not domain joined, a remote access trojan (RAT) will be deployed. Proofpoint assesses with moderate confidence that the deployment of a RAT is an attempt to harvest credentials to secure a foothold on a network suitable for ransomware deployment, such as the target's employer. Regardless of the victim's profile, TA569 is extremely aggressive in deploying follow-on malware leading to a remarkably low dwell time.

The follow-on ransomware activity referenced in this report overlaps with activity publicly reported as EvilCorp, Gold Drake, and UNC2165. As TA569 focuses on initial access into target environments, Proofpoint does not suggest equivalence in attribution between TA569 and actors conducting post-infection activity.

Figure 4: SocGholish as part of a kill chain

Conclusion

Users should be aware of novel social engineering and exploitation mechanisms used by TA569 to deliver malicious payloads, even from trusted sources. This attack chain underscores the importance of consistent, clear communication from organizations concerning user awareness training and software update best practices. SocGholish remains a serious threat to enterprises due to it being delivered through legitimate means and the speed at which the attack progresses from initial access to ransomware. Defenders must be diligent in evaluating alerts and must not be quick to dismiss them as false positives.

Learn more

For more on this topic, register to attend our webinar, Threat Research Flash Brief: SocGholish Poisons Supply Chain for Major Media Websites, on Tuesday, November 22, 2022, at 10 AM PT, or watch it on demand.

In our next report on TA569, we'll dive deep into the injections, payloads, and changes in activity observed in 2022 from this threat actor. Stay tuned!
