Mphasis
The Next Applied

SocGholish Malware

Severity: Medium | Date: 28th June 2022

Description

SocGholish leverages drive-by-downloads masquerading as software updates to trick visitors of compromised websites into executing malware.

How It Works

The website displays content that might lure end-users, such as critical browser updates. To infect the system, an end-user must first manually decompress the archive file and then execute the malware by double-clicking. An infection with SocGholish may result in the deployment of the Cobalt Strike framework and ransomware.

A drive-by attack is when a user visits an infected website, and the website triggers a malicious download without user intervention.

SocGholish operators host a malicious website that implements a drive-by-download mechanism.

SocGholish operators use a legitimate website and host another, malicious website in its context, for example, in an inline frame (iframe) object. The legitimate website displays content to which end-users may be lured, such as critical browser updates. The malicious website may implement, for example, JavaScript code, or conduct URL redirections to trigger the download of an archive file that stores a malicious JavaScript script.

Post Infection

SocGholish employs several scripted reconnaissance commands. While much of this activity occurs in memory, one that stands out is the execution of whoami with the output redirected to a local temp file with the naming convention rad<5-hex-chars>.tmp.

Enumerating domain trust activity with nltest.exe. SocGholish may lead to domain discovery. This type of behaviour is often a precursor to ransomware activity and should be quickly quelled to prevent further progression of the threat.

The majority of SocGholish infections detected did not result in a second-stage payload, sometimes due to existing mitigations or rapid response to isolate the host. In most cases observed reconnaissance activity that only identified the infected endpoint and user. In some cases, Active Directory and domain enumeration followed user discovery.

Both can be a precursor to lateral movement; however, the hosts were isolated before any lateral movement activity could begin. Much of the reconnaissance conducted by the malicious JavaScript file happens in memory, with data being exfiltrated directly via POST commands to the C2 domain

IOC's

Hash Values

- 7b3f8c85c34fbda4125704220773509d578cbf862b0c3311241db1fe3003c8a5
- bcab0580712475c75baee610f1f372ef524156bf097662fba710f293c8656f9f
- 75bec26067d15141bbfb8d18f0af2be190d6ae1a276640c182a5bf3137f76ffa

Reference Links

- https://redcanary.com/threat-detection-report/threats/socgholish/
- https://www.socinvestigation.com/socgholish-malware-on-the-rise-detection-response/