


Mphasis SOC – Information Security News

Date & Time Issued: 02-JUL-2024, 22:00 IST

Title	SocGholish_Malware	
Summary	<ul style="list-style-type: none"> SecurID researcher have uncovered the SocGholish Malware. This is a JavaScript malware framework that has been used by cybercriminals since 2017 to trick people into downloading malicious files by pretending to be urgent browser updates. It creates fake update notifications on websites to trick users. Once users download and run these files, the malware installs more dangerous software like Remote Access Trojans (RATs) and infostealers, causing serious security breaches and ransomware attack. SocGholish also uses compromised domains and WordPress plugins to spread its malware. Common SocGholish campaigns include NDSW/NDSX and khutmhpx, which inject malicious code into websites. In 2024, there has been increased activity from SocGholish groups, indicating that the threat is growing and ongoing. 	
Severity	Medium 	
Attack Vectors	<ul style="list-style-type: none"> One of the primary tactics used by SocGholish is the fake browser update scheme. This involves creating malicious websites or compromising legitimate ones to display fake browser update notifications and pop-ups on infected websites. Notifications are designed to look convincing, often mimicking the design and language of real update prompts from popular browsers like Chrome, Firefox, and Edge. When a user visits an infected website, they are greeted with a pop-up or banner urging them to update their browser to the latest version for security reasons. The urgency and legitimacy of the message can easily persuade users to follow the instructions, especially if they are not tech-savvy or are in a rush. If a user falls for the SocGholish fake update prompt, they are directed to download a file, typically in the form of a .zip or .js file. These files are carefully crafted to appear harmless but are, in fact, laden with malware. If a user clicks on the downloaded JavaScript file, it is executed by the Windows Script Host (wscript). For .zip downloads the user is instructed to decompress and execute the file. This step requires user interaction, making the malware delivery method a form of social engineering. Once the malicious file is executed, SocGholish collects information about the environment and sends this data to a Command & Control server (C2). C2 uses this data to decide whether to proceed with deploying various types of secondary malware. These can include remote access trojans (RATs), which allow attackers to gain control of the infected system, information stealers that harvest sensitive data such as credentials and financial information, and Cobalt Strike beacons, which are used for further exploitation and lateral movement within a network. 	
Indicator of Compromise	INDICATOR TYPE	INDICATORS
	Domain	<ul style="list-style-type: none"> subscribe.3gbling[.]com pastor.cntcog[.]org dashboard.skybacherslocker[.]com mini.ptipexcel[.]com progress.cashdigger[.]com myfood.silverspringfoodproject[.]org perspective.cdsigner[.]com wiki.clotheslane[.]com
	IP	<ul style="list-style-type: none"> 179.43.134[.]167 88.210.11[.]17 179.43.178[.]73 179.43.133[.]61
	URLs	<ul style="list-style-type: none"> hxxps://aitcaid[.]com/9659650c81ce1b984c58.js hxxps://marvin-occentus[.]net/statistic/js/stat.js hxxps://mini.ptipexcel[.]com

Recommendations	<ul style="list-style-type: none">• Update your admin credentials.• Check for malicious administrators.• Inspect all themes, plugins, and other third-party components installed on your website. A simple deactivation is not enough – delete anything that you don't recognize or no longer use.• Remove the malicious code.• Patch all of your website software.• Consider using a website firewall that will protect your site from most known attacks and virtually patch known vulnerabilities until you are able to update your software. <p>NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.</p>
References	<ul style="list-style-type: none">• https://blog.sucuri.net/2022/11/new-wave-of-socgholish-cid27x-injections.html• https://www.sitelock.com/blog/socgholish-malware/

The information contained in this message is proprietary. It is for Mphasis and its customers only.
Copyright © 2024. All rights reserved by Mphasis.