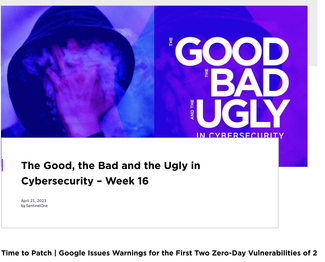
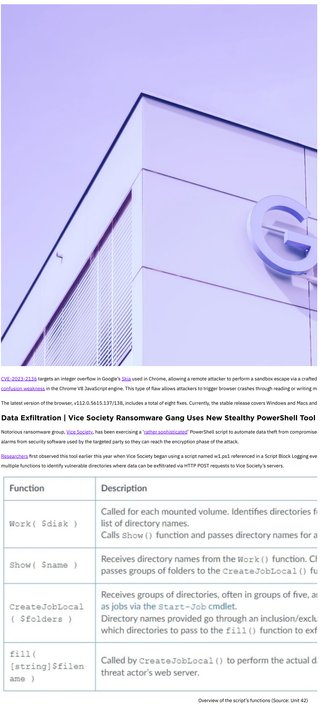


The Good, the Bad and the Ugly in Cybersecurity – Week 16

April 21, 2023
by SentinelOne

Time to Patch | Google Issues Warnings for the First Two Zero-Day Vulnerabilities of 2

Google has released emergency patches for two high-severity zero-day vulnerabilities affecting Chrome, CVE-2023-2136 and CVE-2023-2033, wit
a majority of Chrome's 3 billion users have applied the fix.



CVE-2023-2136 targets an integer overflow in Google's Skia used in Chrome, allowing a remote attacker to perform a sandbox escape via a crafted
confusion weakness in the Chrome V8 JavaScript engine. This type of flaw allows attackers to trigger browser crashes through reading or writing m

The latest version of the browser, v112.0.5615.137/138, includes a total of eight fixes. Currently, the stable release covers Windows and Macs and

Data Exfiltration | Vice Society Ransomware Gang Uses New Stealthy PowerShell Tool

Notorious ransomware group, Vice Society, has been exercising a "lother sophisticated" PowerShell script to automate data theft from compromise
alarms from security software used by the targeted party so they can reach the encryption phase of the attack.

Researchers first observed this tool earlier this year when Vice Society began using a script named w1.ps1 referenced in a Script Block Logging eve
multiple functions to identify vulnerable directories where data can be exfiltrated via HTTP POST requests to Vice Society's servers.

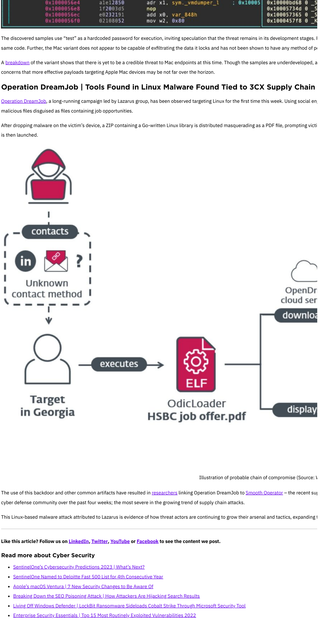
Function	Description
`Work( $disk )`	Called for each mounted volume. Identifies directories fo list of directory names. Calls `Show()` function and passes directory names for a
`Show( $name )`	Receives directory names from the `Work()` function. Cl passes groups of folders to the `CreateJobLocal()` fu
`CreateJobLocal ( $folders )`	Receives groups of directories, often in groups of five, ar as jobs via the `Start-Job` cmdlet. Directory names provided go through an inclusion/exclu which directories to pass to the `fill()` function to exf
`fill( [string]$filen ame )`	Called by `CreateJobLocal()` to perform the actual d threat actor's web server.

Overview of the script's functions (Source: Unit 42)

Threat actors often leverage stolen corporate and customer data to extort a higher ransom from their victims and resell to other criminals for additi
all signs of further evolution since debuting their new file encryptor, Polylnx, back in December 2022.

Critical RCE Flaws | Sandbox Escape PoCs Available for VM2 JavaScript Library

Three recent sandbox escape proof-of-concept (POC) exploits have been released, all enabling attackers to execute malicious code on hosts runni
editors to run and test untrusted code in isolation. All three flaws have been assigned a critical scoring of 9.8.



CVE-2023-29017 describes a case where VM2 does not properly handle host objects passed to Error.prepareStackTrace during unhandled async e
code transformer. If exploited, it allows attackers to bypass sandbox protections and gain remote code execution rights on the host running the sar
the sandbox. By escaping these sandbox restrictions, attackers can perform arbitrary code execution in the host and potentially set up severe cybe

VM2 strongly recommends all users and developers using the VM2 library to upgrade to version 3.9.17 to address the security flaws.

LockBit Ransomware | New & Incomplete Samples of macOS Variant Surface

Researchers this week revealed details of a LockBit ransomware sample compiled for Apple's macOS arm64 architecture. As of now, there are no k

The discovered samples use "test" as a hardcoded password for execution, inviting speculation that the threat remains in its development stages. I
same code. Further, the Mac variant does not appear to be capable of exfiltrating the data it locks and has not been shown to have any method of p

A breakdown of the variant shows that there is yet to be a credible threat to Mac endpoints at this time. Though the samples are underdeveloped, a
concerns that more effective payloads targeting Apple Mac devices may be not far over the horizon.

Operation DreamJob | Tools Found in Linux Malware Found Tied to 3CX Supply Chain

Operation DreamJob, a long-running campaign led by Lazarus group, has been observed targeting Linux for the first time this week. Using social en
malicious files disguised as files containing job opportunities.

After dropping malware on the victim's device, a ZIP containing a Go-written Linux library is distributed masquerading as a PDF file, prompting vict
is then launched.

Illustration of probable chain of compromise (Source: L

The use of this backdoor and other common artifacts have resulted in researchers linking Operation DreamJob to Smooth Operator – the recent su
cyber defense community over the past four weeks; the most severe in the growing trend of supply chain attacks.

This Linux-based malware attack attributed to Lazarus is evidence of how threat actors are continuing to grow their arsenal and tactics, expanding t

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- SentinelOne's Cybersecurity Predictions 2023 | What's Next?
- SentinelOne Named to Deloitte Fast 500 List for 6th Consecutive Year
- Apple's macOS Ventura 7 New Security Changes to Be Aware Of
- Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results
- Lionel Cliff Windows Defender | LockBit Ransomware Sidelloads Cobalt Strike Through Microsoft Security Tool
- Enterprise Security Essentials | Top 15 Most Routinely Exploited Vulnerabilities 2022