

## 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 2023

Google has [released](#) emergency patches for two high-severity zero-day vulnerabilities affecting Chrome, CVE-2023-2136 and CVE-2023-2033, with 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 memory.

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 is expected to be rolled out to Linux users in the coming days.

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

Notorious ransomware group, [Vice Society](#), has been exercising a 'rather sophisticated' PowerShell script to automate data theft from compromised systems. The script uses 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 event. The script uses multiple functions to identify vulnerable directories where data can be exfiltrated via HTTP POST requests to Vice Society's servers.

Function	Description
<code>Work( \$disk )</code>	Called for each mounted volume. Identifies directories for data theft. Calls <code>Show( )</code> function and passes directory names for processing.
<code>Show( \$name )</code>	Receives directory names from the <code>Work( )</code> function. Calls <code>Get-Childitem</code> to list contents and passes groups of folders to the <code>CreateJobLocal( )</code> function.
<code>CreateJobLocal( \$folders )</code>	Receives groups of directories, often in groups of five, and creates jobs via the <code>Start-Job</code> cmdlet. Directory names provided go through an inclusion/exclusion filter to determine which directories to pass to the <code>fill( )</code> function to exfiltrate data.
<code>fill( [string]\$filename )</code>	Called by <code>CreateJobLocal( )</code> to perform the actual data exfiltration to the threat actor's web server.

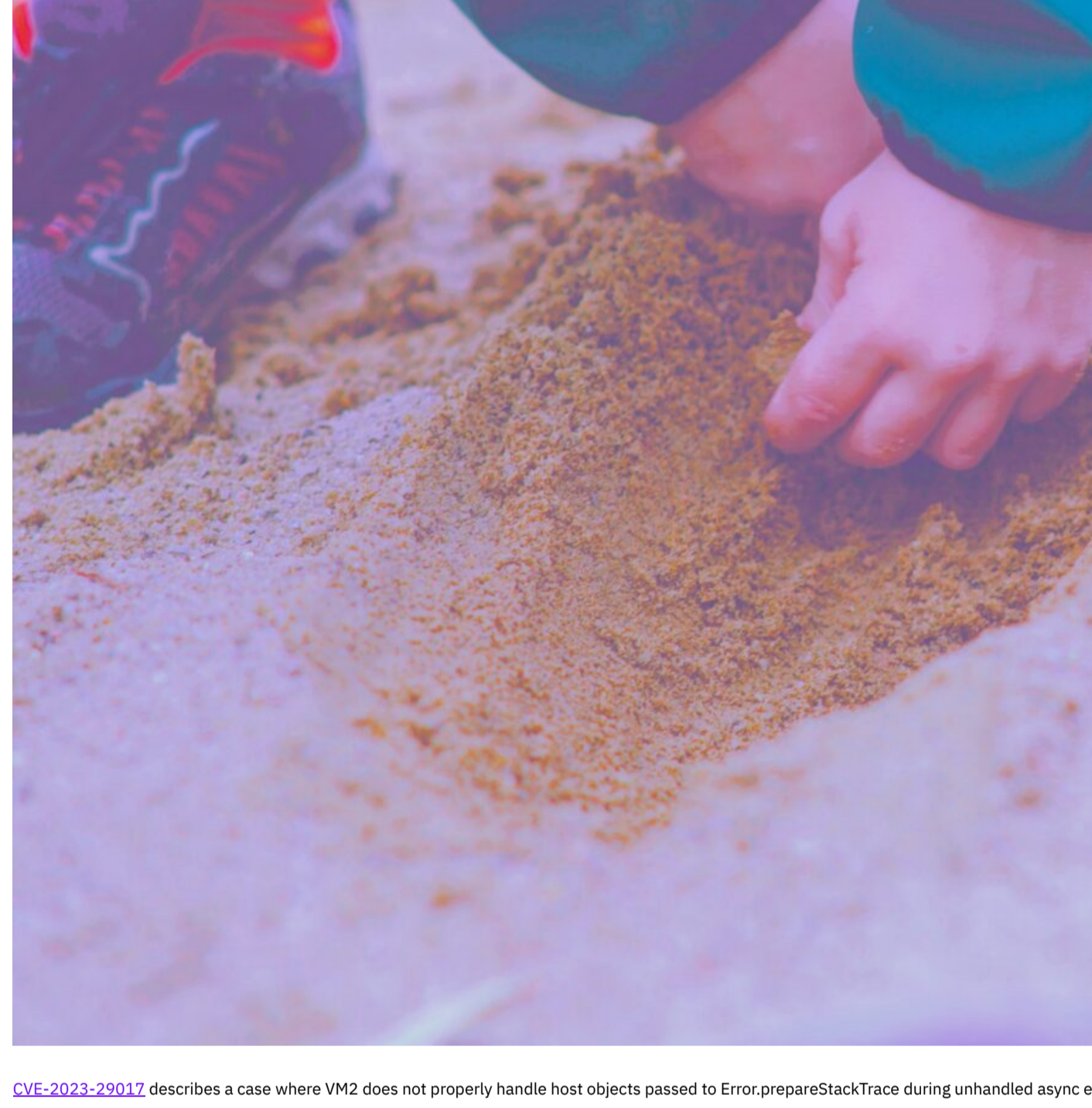
Overview of the script's functions (Source: Unit 42)

Threat actors often leverage stolen corporate and customer data to extort a higher ransom from their victims and resell to other criminals for additional profit. The group has shown signs of further evolution since debuting their new file encryptor, [PolyVice](#), 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 running the VM2 JavaScript library. The exploits allow attackers to bypass sandbox protections and gain remote code execution rights on the host running the sandbox. By escaping these sandbox restrictions, attackers can perform arbitrary code execution in the host and potentially set up severe cyber threats.

VM2 strongly [recommends](#) all users and developers using the VM2 library to upgrade to version 3.9.17 to address the security flaws.



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

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 public samples of this variant, but the discovery indicates a potential threat to Mac users.

```
[X] Disassembly (Disassembly)
    :-- func.100005608
    : CALL XREF from main @ 0x10000b464(x)
552: sym._start_wiping(int64_t arg_cd0h);
    : arg int64_t arg_cd0h @ sp+0x19a0
    : var int64_t var_0h @ sp+0x0
    : var int64_t var_8h @ sp+0x8
    : var int64_t var_8h_2 @ sp+0x10
    : var int64_t var_20h_2 @ sp+0x20
    : var time_t *timeptr @ sp+0x28
    : var int64_t var_30h_2 @ sp+0x30
    : var int64_t var_8h_3 @ sp+0x38
    : var char *s @ sp+0x834
    : var int64_t var_848h @ sp+0x848
    : var char *src @ sp+0x8c8
    : var char *dest @ sp+0x8c9
    : var int64_t var_cc8h @ sp+0xccc8
    : var int64_t var_60h_2 @ sp+0xcd0
    : var int64_t var_60h_2 @ sp+0xcd8
    : var int64_t var_10h_2 @ sp+0xce0
    : var int64_t var_10h_2 @ sp+0xce8
    : var int64_t var_20h @ sp+0xcf0
    : var int64_t var_20h_3 @ sp+0xcf8
    : var int64_t var_30h_3 @ sp+0xd00
    : var int64_t var_40h @ sp+0xd08
    : var int64_t var_40h_2 @ sp+0xd18
    : var int64_t var_50h @ sp+0xd20
    : var int64_t var_50h_2 @ sp+0xd28
0x1000056b8      fc6fbaa9      stp x28, x27, [var_60h]!
0x1000056bc      fa6701a9      stp x26, x25, [var_10h]
0x1000056c0      f85f02a9      stp x24, x23, [var_20h]
0x1000056c4      f65703a9      stp x22, x21, [var_30h]
0x1000056c8      f44f04a9      stp x20, x19, [var_40h]
0x1000056cc      fd7b05a9      stp x29, x30, [var_50h]
0x1000056d0      ff4333d1      sub sp, sp, 0xcd0
0x1000056d4      1f2003d5      nop
0x1000056d8      88492558      ldr x8, reloc.__stack_chk_guard
0x1000056dc      080140f9      ldr x8, [x8]
0x1000056e0      e86706f9      str x8, [var_cc8h]
0x1000056e4      a1e12850      adr x1, sym._vmdumper_1
0x1000056e8      1f2003d5      nop
0x1000056ec      e0232191      add x0, var_848h
0x1000056f0      02108052      mov w2, 0x80
```

The discovered samples use "test" as a hardcoded password for execution, inviting speculation that the threat remains in its development stages. It is unclear if the samples are intended for actual deployment or are merely proof-of-concept.

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 concern 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 engineering, 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 the victim to then launch the malware.

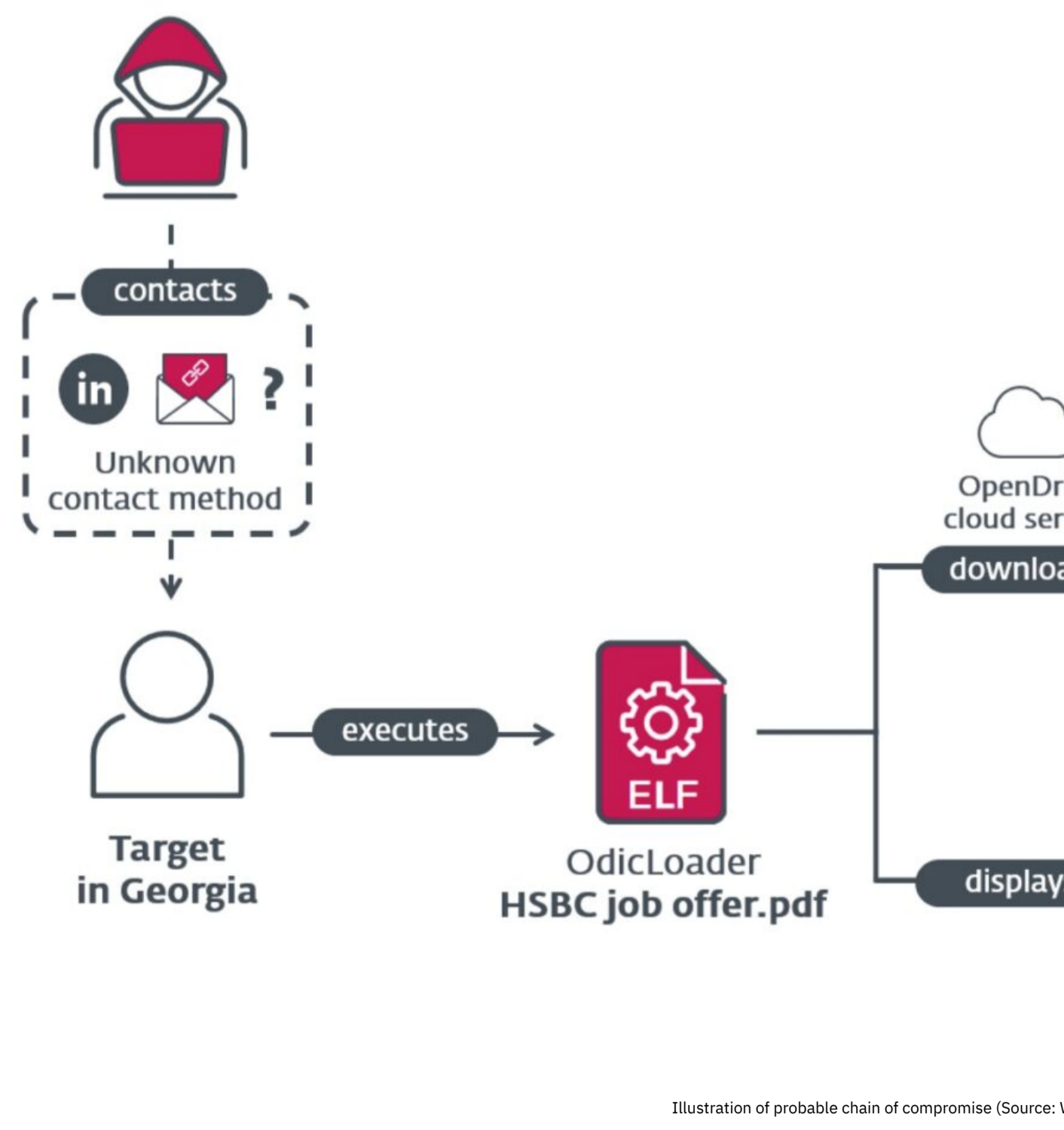


Illustration of probable chain of compromise (Source: Vortex)

The use of this backdoor and other common artifacts have resulted in [researchers](#) linking Operation DreamJob to [Smooth Operator](#) – the recent supply chain attack on the Linux-based malware attack attributed to Lazarus is evidence of how threat actors are continuing to grow their arsenal and tactics, expanding their reach.

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 4th 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](#)
- [Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool](#)
- [Enterprise Security Essentials | Top 15 Most Routinely Exploited Vulnerabilities 2022](#)