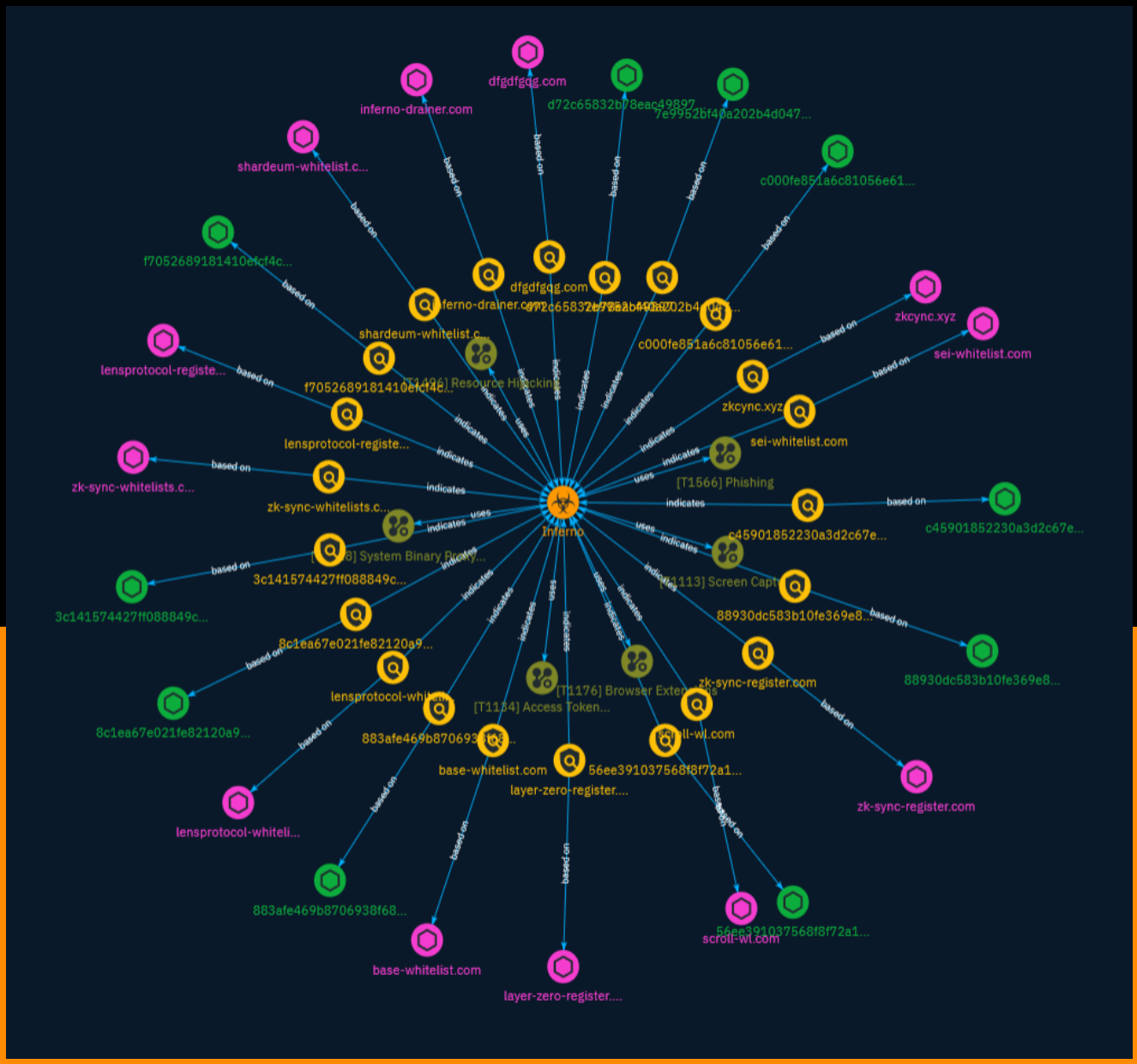
Jan 19 2024

NETMANAGEIT

# Intelligence Report

# Burnout: Inferno Drainer's multimillion-dollar scam scheme detailed



# Table of contents

## Overview



## Entities



## Observables

# External References

# Overview

## Description

A cybersecurity firm has uncovered details about a scam-as-a-service that stole more than $80m from cryptocurrency wallets worldwide in the last year. The project ceased activity in late November 2023, but its panel is still active. Group-IB believes its customers are probably active and in the search for new tools to steal cryptocurrencies from their victims.

## Confidence

*This value represents the confidence in the correctness of the data contained within this report.*

15 / 100

# Content

N/A

# Attack-Pattern

| Name |
| --- |
| Phishing |
| **ID** |
| T1566 |
| **Description** |
| Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth) |

**Name**

Browser Extensions

**ID**

T1176

**Description**

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

**Name**

Resource Hijacking

**ID**

T1496

**Description**

Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster. (Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR) Alternatively, they may engage in proxyjacking by selling use of the victims' network bandwidth and IP address to proxyware services.(Citation: Sysdig Proxyjacking)

**Name**

Access Token Manipulation

**ID**

T1134

**Description**

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to

make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

**Name**

System Binary Proxy Execution

**ID**

T1218

**Description**

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

**Name**

Screen Capture

## ID

T1113

## Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

# Indicator

| Name |
| --- |
| zk-sync-whitelists.com |
| **Pattern Type** |
| stix |
| **Pattern** |
| [domain-name:value = 'zk-sync-whitelists.com'] |
| **Name** |
| zkcync.xyz |
| **Pattern Type** |
| stix |
| **Pattern** |
| [domain-name:value = 'zkcync.xyz'] |
| **Name** |
| c000fe851a6c81056e617d3132bcdc741b8a9a715f59b3d0f304816ffc8f397c |

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = 'c000fe851a6c81056e617d3132bcdc741b8a9a715f59b3d0f304816ffc8f397c'] |
| **Name** |
| 56ee391037568f8f72a191635288afe7274cb7cb2439d1cdadc407be07b3925c |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '56ee391037568f8f72a191635288afe7274cb7cb2439d1cdadc407be07b3925c'] |
| **Name** |
| f7052689181410efcf4c857c8a0eeb8bf911ff9958a88884063edf5d43578437 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = 'f7052689181410efcf4c857c8a0eeb8bf911ff9958a88884063edf5d43578437'] |

| Name |
| --- |
| c45901852230a3d2c67eae5fdf7204ba6afb7432377ec25157d838b1663d5b96 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = 'c45901852230a3d2c67eae5fdf7204ba6afb7432377ec25157d838b1663d5b96'] |
| **Name** |
| layer-zero-register.com |
| **Pattern Type** |
| stix |
| **Pattern** |
| [domain-name:value = 'layer-zero-register.com'] |
| **Name** |
| lensprotocol-register.com |
| **Pattern Type** |
| stix |
| **Pattern** |

[domain-name:value = 'lensprotocol-register.com']

**Name**

scroll-wl.com

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'scroll-wl.com']

**Name**

8c1ea67e021fe82120a99d3bc33c92dec4845f5af94f192e17104e14ca04ecee

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '8c1ea67e021fe82120a99d3bc33c92dec4845f5af94f192e17104e14ca04ecee']

**Name**

88930dc583b10fe369e8f3ec632c819d54c6cc6a812087eba17b9b7db6a86cba

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '88930dc583b10fe369e8f3ec632c819d54c6cc6a812087eba17b9b7db6a86cba']

**Name**

base-whitelist.com

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'base-whitelist.com']

**Name**

7e9952bf40a202b4d047ea5157e5c67930667d29749dcecfd20df0fc1a40f276

**Description**

compromised_site_redirector_fromcharcode

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '7e9952bf40a202b4d047ea5157e5c67930667d29749dcecfd20df0fc1a40f276']

**Name**

sei-whitelist.com

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'sei-whitelist.com']

**Name**

3c141574427ff088849cebd2fde1bde711158020be7edb496bcf41b8c10d5231

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '3c141574427ff088849cebd2fde1bde711158020be7edb496bcf41b8c10d5231']

**Name**

d72c65832b78eac498973efbc617486ea981cb6a2efe477e2887ac4142a50c1e

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'd72c65832b78eac498973efbc617486ea981cb6a2efe477e2887ac4142a50c1e']

| Name |
| --- |
| 883afe469b8706938f681b78750974b5daa373befe51f91eba6e9cb0a18d8238 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '883afe469b8706938f681b78750974b5daa373befe51f91eba6e9cb0a18d8238'] |
| **Name** |
| shardeum-whitelist.com |
| **Pattern Type** |
| stix |
| **Pattern** |
| [domain-name:value = 'shardeum-whitelist.com'] |
| **Name** |
| inferno-drainer.com |
| **Pattern Type** |
| stix |
| **Pattern** |

[domain-name:value = 'inferno-drainer.com']

**Name**

lensprotocol-whitelist.com

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'lensprotocol-whitelist.com']

**Name**

dfgdfgqg.com

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'dfgdfgqg.com']

**Name**

zk-sync-register.com

**Pattern Type**

stix

**Pattern**

```
[domain-name:value = 'zk-sync-register.com']
```

# Malware

| Name |
| --- |
| Inferno |

# Domain-Name

| Value |
| --- |
| inferno-drainer.com |
| sei-whitelist.com |
| layer-zero-register.com |
| lensprotocol-whitelist.com |
| zk-sync-register.com |
| lensprotocol-register.com |
| shardeum-whitelist.com |
| scroll-wl.com |
| zk-sync-whitelists.com |
| zkcync.xyz |
| base-whitelist.com |
| dfgdfgqg.com |

# StixFile

| Value |
| --- |
| 88930dc583b10fe369e8f3ec632c819d54c6cc6a812087eba17b9b7db6a86cba |
| c000fe851a6c81056e617d3132bcdc741b8a9a715f59b3d0f304816ffc8f397c |
| 56ee391037568f8f72a191635288afe7274cb7cb2439d1cdadc407be07b3925c |
| 3c141574427ff088849cebd2fde1bde711158020be7edb496bcf41b8c10d5231 |
| 7e9952bf40a202b4d047ea5157e5c67930667d29749dcecfd20df0fc1a40f276 |
| 8c1ea67e021fe82120a99d3bc33c92dec4845f5af94f192e17104e14ca04ecee |
| f70526891814l0efcf4c857c8a0eeb8bf911ff9958a88884063edf5d43578437 |
| c45901852230a3d2c67eae5fdf7204ba6afb7432377ec25157d838b1663d5b96 |
| d72c65832b78eac498973efbc617486ea981cb6a2efe477e2887ac4142a50c1e |
| 883afe469b8706938f681b78750974b5daa373befe51f91eba6e9cb0a18d8238 |

# External References

- https://otx.alienvault.com/pulse/65a90b0cfd7d892f1197f724