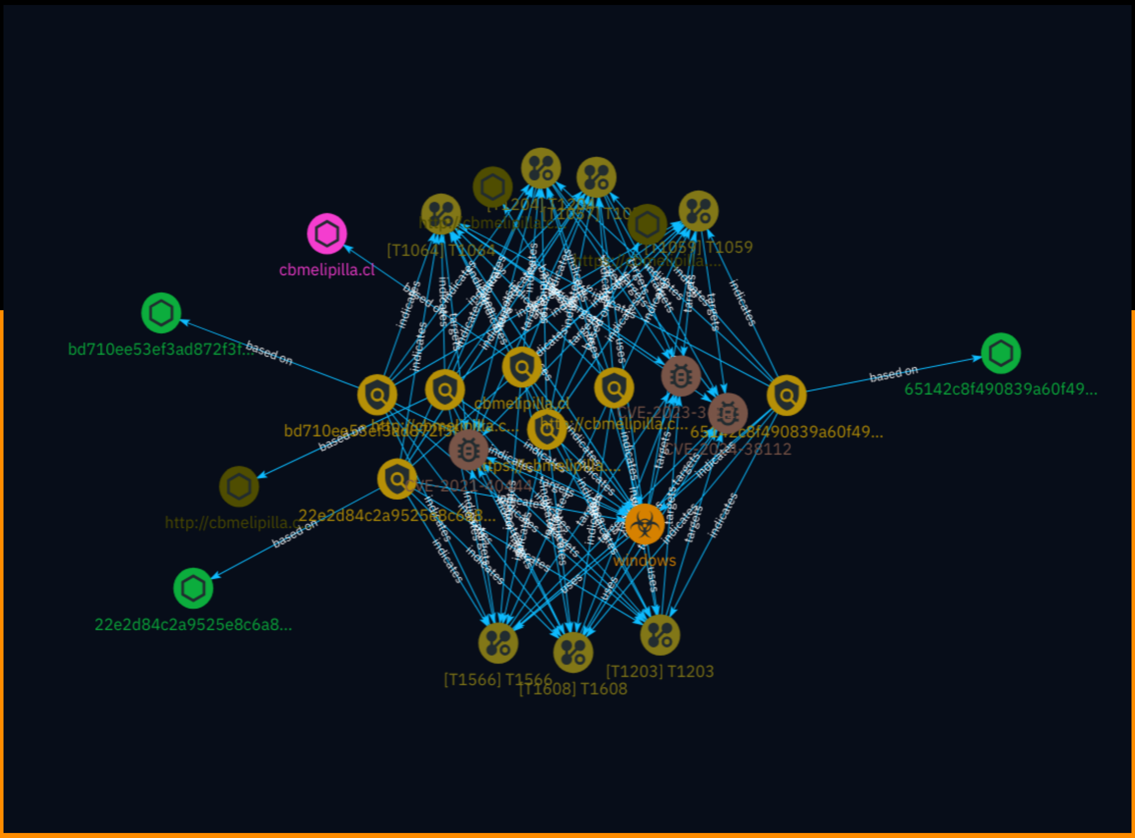
Jul 11 2024

NETMANAGEIT

# Intelligence Report

# Resurrecting Internet Explorer: Threat Actors Using Zero-day Tricks in Internet Shortcut File to Lure Victims (CVE-2024-38112)



# Table of contents

## Overview

- Description 4
- Confidence 4
- Content 5

## Entities

- Attack-Pattern 6
- Indicator 12
- Malware 15
- indicates 16
- targets 21
- based-on 24
- uses 25

## Observables

- Domain-Name 26
- StixFile 27

## External References

- External References 28

# Overview

## Description

Check Point Research discovered threat actors leveraging novel techniques to execute malicious code on Windows systems by exploiting Internet Explorer's vulnerabilities. The attackers utilized specially crafted .url files that, when opened, would launch IE and visit attacker-controlled URLs. Additionally, they employed a trick to hide the .hta extension, tricking victims into executing malicious code disguised as a PDF file. This campaign has been active since January 2023, targeting various industries and utilizing multiple MITRE ATT&CK techniques.

## Confidence

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

100 / 100

# Content

N/A

# Attack-Pattern

**Name**

T1057

**ID**

T1057

**Description**

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Administrator or otherwise elevated access may provide better process details. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via `/proc`. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes. (Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

**Name**

T1064

| ID |
|---|
| T1064 |

| Description |
|---|
| **This technique has been deprecated. Please use [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) where appropriate.** Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and [PowerShell](https://attack.mitre.org/techniques/T1086) but could also be in the form of command-line batch scripts. Scripts can be embedded inside Office documents as macros that can be set to execute when files used in [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), where adversaries will rely on macros being allowed or that the user will accept to activate them. Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit (Citation: Metasploit_Ref), Veil (Citation: Veil_Ref), and PowerSploit (Citation: Powersploit) are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell. (Citation: Alperovitch 2014) |

| Name |
|---|
| T1566 |

| 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**

T1204

**ID**

T1204

**Description**

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary; running malicious JavaScript in their browser, allowing adversaries to [Steal Web Session

Cookie](https://attack.mitre.org/techniques/T1539)s; or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204).(Citation: Talos Roblox Scam 2023)(Citation: Krebs Discord Bookmarks 2023) For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

**Name**

T1059

**ID**

T1059

**Description**

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

| Name |
|---|
| T1608 |

| ID |
|---|
| T1608 |

| Description |
|---|
| Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert) |

| Name |
|---|
| T1203 |

## ID

T1203

## Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

# Indicator

**Name**

http://cbmelipilla.cl/te/test1.html!x-usc:http://cbmelipilla.cl/te/test1.html

**Pattern Type**

stix

**Pattern**

[url:value = 'http://cbmelipilla.cl/te/test1.html!x-usc:http://cbmelipilla.cl/te/test1.html']

**Name**

bd710ee53ef3ad872f3f0678117050608a8e073c87045a06a86fb4a7f0e4eff0

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'bd710ee53ef3ad872f3f0678117050608a8e073c87045a06a86fb4a7f0e4eff0']

**Name**

22e2d84c2a9525e8c6a825fb53f2f30621c5e6c68b1051432b1c5c625ae46f8c

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '22e2d84c2a9525e8c6a825fb53f2f30621c5e6c68b1051432b1c5c625ae46f8c']

**Name**

cbmelipilla.cl

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'cbmelipilla.cl']

**Name**

http://cbmelipilla.cl/te/test1.html

**Pattern Type**

stix

**Pattern**

[url:value = 'http://cbmelipilla.cl/te/test1.html']

**Name**

https://cbmelipilla.cl/te/Books_A0UJKO.pdf%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80.hta

**Pattern Type**

stix

**Pattern**

[url:value = 'https://cbmelipilla.cl/te/Books_A0UJKO.pdf%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80%E2%A0%80.hta']

**Name**

65142c8f490839a60f4907ab8f28dd9db4258e1cfab2d48e89437ef2188a6e94

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '65142c8f490839a60f4907ab8f28dd9db4258e1cfab2d48e89437ef2188a6e94']

# Malware

| Name |
|---|
| windows |

# indicates

| Name |
|---|
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |

| |
|---|
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |

| |
|---|
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

| |
|---|
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |
| **Name** |
| |

# targets

| Name |
|---|
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |
| |
| Name |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

# based-on

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

| Name |
|---|
| |

# uses

| Name |
|---|
|  |

| Name |
|---|
|  |

| Name |
|---|
|  |

| Name |
|---|
|  |

# Domain-Name

| Value |
|---|
| cbmelipilla.cl |

# StixFile

| Value |
|---|
| bd710ee53ef3ad872f3f0678117050608a8e073c87045a06a86fb4a7f0e4eff0 |
| 22e2d84c2a9525e8c6a825fb53f2f30621c5e6c68b1051432b1c5c625ae46f8c |
| 65142c8f490839a60f4907ab8f28dd9db4258e1cfab2d48e89437ef2188a6e94 |

# External References

- https://research.checkpoint.com/2024/resurrecting-internet-explorer-threat-actors-using-zero-day-tricks-in-internet-shortcut-file-to-lure-victims-cve-2024-38112/
- https://otx.alienvault.com/pulse/668e5353bb297021f2c812f9