Jul 03 2023

NETMANAGEIT

Intelligence Report

PindOS: New JavaScript Dropper Delivering Bumblebee and IcedID

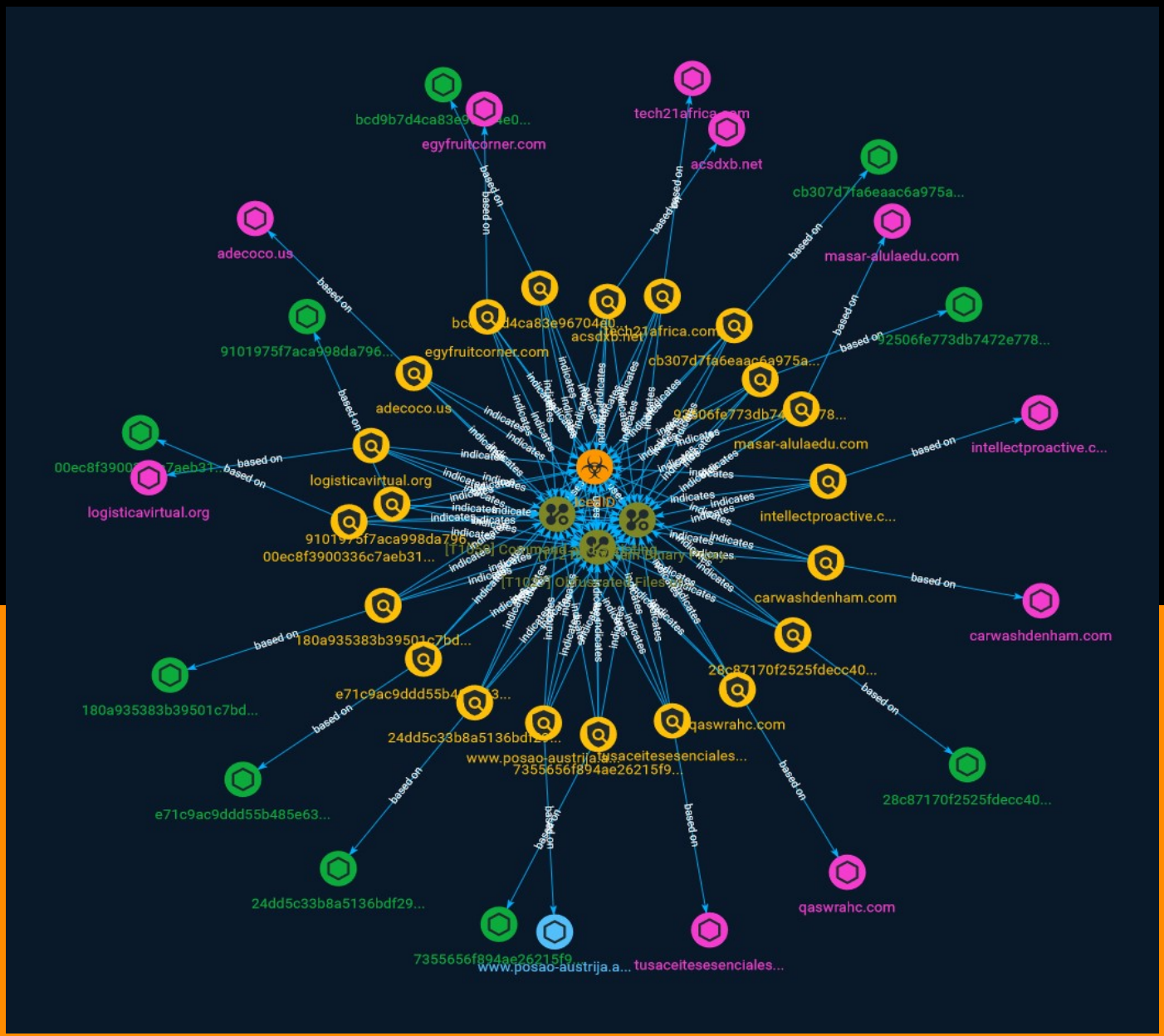

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new strain of Bumblebee and IcedID, a modular banking malware designed to steal financial information, has been spotted in the wild.

Confidence

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

15 / 100

Indicator

Name
e71c9ac9ddd55b485e636840da150db5cd2791d0681123457bd40623acd8311c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e71c9ac9ddd55b485e636840da150db5cd2791d0681123457bd40623acd8311c']
Name
tech21africa.com
Pattern Type
stix
Pattern
[domain-name:value = 'tech21africa.com']
Name

tusaceitesesenciales.com

Pattern Type

stix

Pattern

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

Name

www.posao-austrija.at

Pattern Type

stix

Pattern

[hostname:value = 'www.posao-austrija.at']

Name

adecoco.us

Pattern Type

stix

Pattern

[domain-name:value = 'adecoco.us']

Name

9101975f7aca998da796fc15a63b36ab8aa0fe0aed0b186aaed06a3383d5f226

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9101975f7aca998da796fc15a63b36ab8aa0fe0aed0b186aaed06a3383d5f226']

Name

92506fe773db7472e7782dbb5403548323e65a9eb2e4c15f9ac65ee6c4bd908b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '92506fe773db7472e7782dbb5403548323e65a9eb2e4c15f9ac65ee6c4bd908b']

Name

carwashdenham.com

Pattern Type

stix

Pattern

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

Name

00ec8f3900336c7aeb31fef4d111ee6e33f12ad451bc5119d3e50ad80b2212b0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '00ec8f3900336c7aeb31fef4d111ee6e33f12ad451bc5119d3e50ad80b2212b0']

Name

bcd9b7d4ca83e96704e00e378728db06291e8e2b50d68db22efd1f8974d1ca91

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bcd9b7d4ca83e96704e00e378728db06291e8e2b50d68db22efd1f8974d1ca91']

Name

7355656f894ae26215f979b953c8fa237dc39af857a6b27754a93adb1823f3b6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7355656f894ae26215f979b953c8fa237dc39af857a6b27754a93adb1823f3b6']

Name

acsdxb.net

Pattern Type

stix

Pattern

[domain-name:value = 'acsdxb.net']

Name

intellectproactive.com

Pattern Type

stix

Pattern

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

Name

180a935383b39501c7bdf2745b3a334841f01a7df9d063fecca587b5cc3f5e7a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '180a935383b39501c7bdf2745b3a334841f01a7df9d063fecca587b5cc3f5e7a']

Name

cb307d7fa6eaac6a975ad64ff966ff6b0b0fdd59109246c2f6f5e8d50a33e93c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cb307d7fa6eaac6a975ad64ff966ff6b0b0fdd59109246c2f6f5e8d50a33e93c']

Name

28c87170f2525fdecc4092fb347acd9b8350ed65e0fd584ce9fc001fd237d523

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '28c87170f2525fdecc4092fb347acd9b8350ed65e0fd584ce9fc001fd237d523']

Name

logisticavirtual.org

Pattern Type
stix
Pattern
[domain-name:value = 'logisticavirtual.org']
Name
masar-alulaedu.com
Pattern Type
stix
Pattern
[domain-name:value = 'masar-alulaedu.com']
Name
24dd5c33b8a5136bdf29d0c07cf56ef0e33a285bb12696a8ff65e4065cb18359
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '24dd5c33b8a5136bdf29d0c07cf56ef0e33a285bb12696a8ff65e4065cb18359']
Name

egyfruitcorner.com

Pattern Type

stix

Pattern

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

Name

qaswrahc.com

Pattern Type

stix

Pattern

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

Malware

Name
IcedID

Description
[IcedID](https://attack.mitre.org/software/S0483) is a modular banking malware designed to steal financial information that has been observed in the wild since at least 2017. [IcedID](https://attack.mitre.org/software/S0483) has been downloaded by [Emotet](https://attack.mitre.org/software/S0367) in multiple campaigns.(Citation: IBM IcedID November 2017)(Citation: Juniper IcedID June 2020)

Attack-Pattern

Name
Obfuscated Files or Information
ID
T1027
Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

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

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)

Domain-Name

Value
qaswrahc.com
egyfruitcorner.com
intellectproactive.com
masar-alulaedu.com
carwashdenham.com
tusaceitesesenciales.com
logisticavirtual.org
acsdxb.net
adecoco.us
tech21africa.com

StixFile

Value
24dd5c33b8a5136bdf29d0c07cf56ef0e33a285bb12696a8ff65e4065cb18359
180a935383b39501c7bdf2745b3a334841f01a7df9d063fecca587b5cc3f5e7a
92506fe773db7472e7782dbb5403548323e65a9eb2e4c15f9ac65ee6c4bd908b
bcd9b7d4ca83e96704e00e378728db06291e8e2b50d68db22efd1f8974d1ca91
9101975f7aca998da796fc15a63b36ab8aa0fe0aed0b186aaed06a3383d5f226
7355656f894ae26215f979b953c8fa237dc39af857a6b27754a93adb1823f3b6
00ec8f3900336c7aeb31fef4d111ee6e33f12ad451bc5119d3e50ad80b2212b0
28c87170f2525fdecc4092fb347acd9b8350ed65e0fd584ce9fc001fd237d523
e71c9ac9ddd55b485e636840da150db5cd2791d0681123457bd40623acd8311c
cb307d7fa6eaac6a975ad64ff966ff6b0b0fdd59109246c2f6f5e8d50a33e93c

Hostname

Value
www.posao-austrija.at

External References

- https://otx.alienvault.com/pulse/64a2e37e2ed3cb6e66de1d49
- https://www.deepinstinct.com/blog/pindos-new-javascript-dropper-delivering-bumblebee-and-icedid