Jul 31 2023

NETMANAGEIT

Intelligence Report

Out of the Sandbox: WikiLoader Digs Sophisticated Evasion

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Proofpoint researchers identified a new malware we call WikiLoader. It was first identified in December 2022 being delivered by TA544, an actor that typically uses Ursnif malware to target Italian organizations. Proofpoint observed multiple subsequent campaigns, the majority of which targeted Italian organizations.

Confidence

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

15 / 100

Indicator

Name
www.p-e-c.nl
Pattern Type
stix
Pattern
[hostname:value = 'www.p-e-c.nl']
Name
inspiration-canopee.fr
Pattern Type
stix
Pattern
[domain-name:value = 'inspiration-canopee.fr']
Name
9386ccb677bde1c51ca3336d02fea66f9489913f2241caa77def71d09464d937

Description

!#HSTR:Donoff.mx

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9386ccb677bde1c51ca3336d02fea66f9489913f2241caa77def71d09464d937']

Name

1106e4b7392f471a740ec96f9e6a603fe28f74b32eef7b456801a833f13727fc

Description

!#HSTR:Donoff.mx

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1106e4b7392f471a740ec96f9e6a603fe28f74b32eef7b456801a833f13727fc']

Name

studiolegalecarduccimacuzzi.it

Pattern Type

stix

Pattern

[domain-name:value = 'studiolegalecarduccimacuzzi.it']

Name

www.astrolabecommunication.fr

Pattern Type

stix

Pattern

[hostname:value = 'www.astrolabecommunication.fr']

Name

sunniznuhqan.com

Pattern Type

stix

Pattern

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

Name

ee008ff7b30d4fce17c5b07ed2d6a0593dc346f899eff3441d8fb3c190ef0e0e

Description

!#HSTR:Donoff.mx

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ee008ff7b30d4fce17c5b07ed2d6a0593dc346f899eff3441d8fb3c190ef0e0e']

Name

a599666949f022de7ccc7edb3d31360e38546be22ad2227d4390364b42f43cfd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a599666949f022de7ccc7edb3d31360e38546be22ad2227d4390364b42f43cfd']

Name

86966795bbd054104844cdab7efcafb0b1879a10aae5c0fefbbc83d1ebccbc98

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '86966795bbd054104844cdab7efcafb0b1879a10aae5c0fefbbc83d1ebccbc98']

Name

9782f11930910c7d24dea71a7a21f40f19623b214cb1848bf9f4d49b858c8379

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9782f11930910c7d24dea71a7a21f40f19623b214cb1848bf9f4d49b858c8379']

Name

www.ilfungodilacco.it

Pattern Type

stix

Pattern

[hostname:value = 'www.ilfungodilacco.it']

Name

0e518e2627350ec0ab61fce3713644726eb3916563199187ef244277281cd35b

Description

#Lowfi:Lua:Mampa:95!ml

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '0e518e2627350ec0ab61fce3713644726eb3916563199187ef244277281cd35b']
Name
6e494eb76d75ee02b28e370ab667bcbcdc6f5143ad522090f4b8244eb472d447
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6e494eb76d75ee02b28e370ab667bcbcdc6f5143ad522090f4b8244eb472d447']
Name
95125db52cdc7870b35c3762bad0ea18944aaed9503c3f69b30beb6ca7bae7e7
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '95125db52cdc7870b35c3762bad0ea18944aaed9503c3f69b30beb6ca7bae7e7']

Name
8d4701f33c05851f41eedb98bfff0569b7f4fae3352e2081f01b3add0a97936c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8d4701f33c05851f41eedb98bfff0569b7f4fae3352e2081f01b3add0a97936c']
Name
a2ed8e1d23d2032909c8ad264231bc244c113a4b40786a9bc9df3418cc915405
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a2ed8e1d23d2032909c8ad264231bc244c113a4b40786a9bc9df3418cc915405']
Name
osteopathe-claudia-grimand.fr
Pattern Type
stix
Pattern

[domain-name:value = 'osteopathe-claudia-grimand.fr']

Name

1eb5d4ae5114979908bfbf8a617b2084b101e9eda92532cf81b2a527c27d91a5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1eb5d4ae5114979908bfbf8a617b2084b101e9eda92532cf81b2a527c27d91a5']

Name

2505b1471e26a303d59e5fc5f0118729a9eead489ffc6574ea2a7746e5db722d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2505b1471e26a303d59e5fc5f0118729a9eead489ffc6574ea2a7746e5db722d']

Name

nikotta.com

Pattern Type

stix

Pattern

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

Name

69a6476d6f7b312cc0d994767801826273741 7e02ebfe168f8d17babed24d657

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '69a6476d6f7b312cc0d994767801826273741 7e02ebfe168f8d17babed24d657']

Name

0b02cfe16ac73f2e7dc52eaf3b93279b7d02b3d64d061782dfed0c55ab621a8e

Description

SUSP_XORed_Mozilla

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0b02cfe16ac73f2e7dc52eaf3b93279b7d02b3d64d061782dfed0c55ab621a8e']

Name

d49c2e47c8e14cc01f0a362293c613ea9604e532ff77b879d69895473dfbeb03

Description

invalid_trailer_structure

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd49c2e47c8e14cc01f0a362293c613ea9604e532ff77b879d69895473dfbeb03']

Name

9a74befc4a4dab4c5032d64fcf9723b67e73ae9d5280fb9fb54f225febba03fe

Description

invalid_trailer_structure

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a74befc4a4dab4c5032d64fcf9723b67e73ae9d5280fb9fb54f225febba03fe']

Name

46c2e0ffadf801900fbff964ba2af5e24fee3209d1011bb46529ba779ff79e93

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '46c2e0ffadf801900fbff964ba2af5e24fee3209d1011bb46529ba779ff79e93']

Name

bbe1eb4a211c3ebaf885b7584fc0936b9289b4d4f4a7fc7556cc870de1ff0724

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bbe1eb4a211c3ebaf885b7584fc0936b9289b4d4f4a7fc7556cc870de1ff0724']

Name

44abd30e18e88e832a65a29ce56c9c570d7f0a3b93158e5059722d89782a750c

Description

#Lowfi:Lua:Mampa:95!ml

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44abd30e18e88e832a65a29ce56c9c570d7f0a3b93158e5059722d89782a750c']

Name

1e5035723637c2f4a26d984e29d17cf164f3846f82eb0b7667efa132a2ea0187

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e5035723637c2f4a26d984e29d17cf164f3846f82eb0b7667efa132a2ea0187']

Name

tournadre.dc1-mtp.fr

Pattern Type

stix

Pattern

[hostname:value = 'tournadre.dc1-mtp.fr']

Name

f88526be804223cae5b4314b9bc0f01c24352caa7ec2c7a2f8b6b54c2e902acc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f88526be804223cae5b4314b9bc0f01c24352caa7ec2c7a2f8b6b54c2e902acc']

Name

2c44c1312a4c99e689979863e7c82c474395d6f46485bd19d0ee26fc3fa52279

Description

!#HSTR:Donoff.mx

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2c44c1312a4c99e689979863e7c82c474395d6f46485bd19d0ee26fc3fa52279']

Name

eaa1be7a91c4f1370d2ad566f8625e3e5bb7c58d99a9e2e3a80e83ce80904e11

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eaa1be7a91c4f1370d2ad566f8625e3e5bb7c58d99a9e2e3a80e83ce80904e11']

Name
www.centrograndate.it
Pattern Type
stix
Pattern
[hostname:value = 'www.centrograndate.it']
Name
1d1e2c0946cd4e22fff380a3b6adf38e7c8b3f2947db7787d00f7d9db988dad2
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1d1e2c0946cd4e22fff380a3b6adf38e7c8b3f2947db7787d00f7d9db988dad2']
Name
www.bbpline.com
Pattern Type
stix
Pattern

[hostname:value = 'www.bbpline.com']

Name

d16c5485f3f01fe0d0ce9387e9c92b561ef4d42f0a22dde77f18a424079c87cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd16c5485f3f01fe0d0ce9387e9c92b561ef4d42f0a22dde77f18a424079c87cd']

Name

e0a1ffff9d5c6eaaa2e57548d8db2febbe89441a76f58feae8256ab69f64c88b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e0a1ffff9d5c6eaaa2e57548d8db2febbe89441a76f58feae8256ab69f64c88b']

Name

vivalisme.fr

Pattern Type

stix

Pattern

[domain-name:value = 'vivalisme.fr']

Name

www.yourbed.it

Pattern Type

stix

Pattern

[hostname:value = 'www.yourbed.it']

Name

27070a66fc07ff721a16c4945d4ec1ca1a1f870d64e52ed387b499160a03d490

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '27070a66fc07ff721a16c4945d4ec1ca1a1f870d64e52ed387b499160a03d490']

Name

9feb868d39b13e395396ea86ddbf05c4820dd476b58b6b437eff1e0b91e2615c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9feb868d39b13e395396ea86ddbf05c4820dd476b58b6b437eff1e0b91e2615c']

Name

18a088a190263275172a28d387103e83b8940e51e96cb518ed41a1960c772bba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '18a088a190263275172a28d387103e83b8940e51e96cb518ed41a1960c772bba']

Intrusion-Set

Name
TA544

Attack-Pattern

Name
TA0005
ID
TA0005
Name
Data Encoding
ID
T1132
Description
Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.
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

User Execution

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, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). 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

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation:

GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations. (Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

Country

Name
Italy

Domain-Name

Value
inspiration-canopee.fr
nikotta.com
sunniznuhqan.com
osteopathe-claudia-grimand.fr
vivalisme.fr
studiolegalecarduccimacuzzi.it

StixFile

Value
1eb5d4ae5114979908bfbf8a617b2084b101e9eda92532cf81b2a527c27d91a5
1106e4b7392f471a740ec96f9e6a603fe28f74b32eef7b456801a833f13727fc
e0a1ffff9d5c6eaaa2e57548d8db2febbe89441a76f58feae8256ab69f64c88b
46c2e0ffadf801900fbff964ba2af5e24fee3209d1011bb46529ba779ff79e93
d49c2e47c8e14cc01f0a362293c613ea9604e532ff77b879d69895473dfbeb03
9a74befc4a4dab4c5032d64fcf9723b67e73ae9d5280fb9fb54f225febba03fe
a2ed8e1d23d2032909c8ad264231bc244c113a4b40786a9bc9df3418cc915405
0e518e2627350ec0ab61fce3713644726eb3916563199187ef244277281cd35b
eaa1be7a91c4f1370d2ad566f8625e3e5bb7c58d99a9e2e3a80e83ce80904e11
9feb868d39b13e395396ea86ddbf05c4820dd476b58b6b437eff1e0b91e2615c
bbe1eb4a211c3ebaf885b7584fc0936b9289b4d4f4a7fc7556cc870de1ff0724
f88526be804223cae5b4314b9bc0f01c24352caa7ec2c7a2f8b6b54c2e902acc
1d1e2c0946cd4e22fff380a3b6adf38e7c8b3f2947db7787d00f7d9db988dad2

44abd30e18e88e832a65a29ce56c9c570d7f0a3b93158e5059722d89782a750c

0b02cfe16ac73f2e7dc52eaf3b93279b7d02b3d64d061782dfed0c55ab621a8e

18a088a190263275172a28d387103e83b8940e51e96cb518ed41a1960c772bba

2c44c1312a4c99e689979863e7c82c474395d6f46485bd19d0ee26fc3fa52279

27070a66fc07ff721a16c4945d4ec1ca1a1f870d64e52ed387b499160a03d490

6e494eb76d75ee02b28e370ab667bcbcdc6f5143ad522090f4b8244eb472d447

2505b1471e26a303d59e5fc5f0118729a9eead489ffc6574ea2a7746e5db722d

a599666949f022de7ccc7edb3d31360e38546be22ad2227d4390364b42f43cfd

ee008ff7b30d4fce17c5b07ed2d6a0593dc346f899eff3441d8fb3c190ef0e0e

1e5035723637c2f4a26d984e29d17cf164f3846f82eb0b7667efa132a2ea0187

9386ccb677bde1c51ca3336d02fea66f9489913f2241caa77def71d09464d937

d16c5485f3f01fe0d0ce9387e9c92b561ef4d42f0a22dde77f18a424079c87cd

8d4701f33c05851f41eedb98bfff0569b7f4fae3352e2081f01b3add0a97936c

95125db52cdc7870b35c3762bad0ea18944aaed9503c3f69b30beb6ca7bae7e7

86966795bbd054104844cdab7efcafb0b1879a10aae5c0fefbbc83d1ebccbc98

9782f11930910c7d24dea71a7a21f40f19623b214cb1848bf9f4d49b858c8379

69a6476d6f7b312cc0d994767801826273741 7e02ebfe168f8d17babed24d657

Hostname

Value
tournadre.dc1-mtp.fr
www.p-e-c.nl
www.bbpline.com
www.centrograndate.it
www.ilfungodilacco.it
www.yourbed.it
www.astrolabecommunication.fr

External References

- https://otx.alienvault.com/pulse/64c7eb61c9323f2856396c98
- https://www.proofpoint.com/us/blog/threat-insight/out-sandbox-wikiloader-digs-sophisticated-evasion