Jul 17 2023

NETMANAGEIT

Intelligence Report

CVE-2023-36884 - Microsoft Office and Windows HTML Remote Code Execution

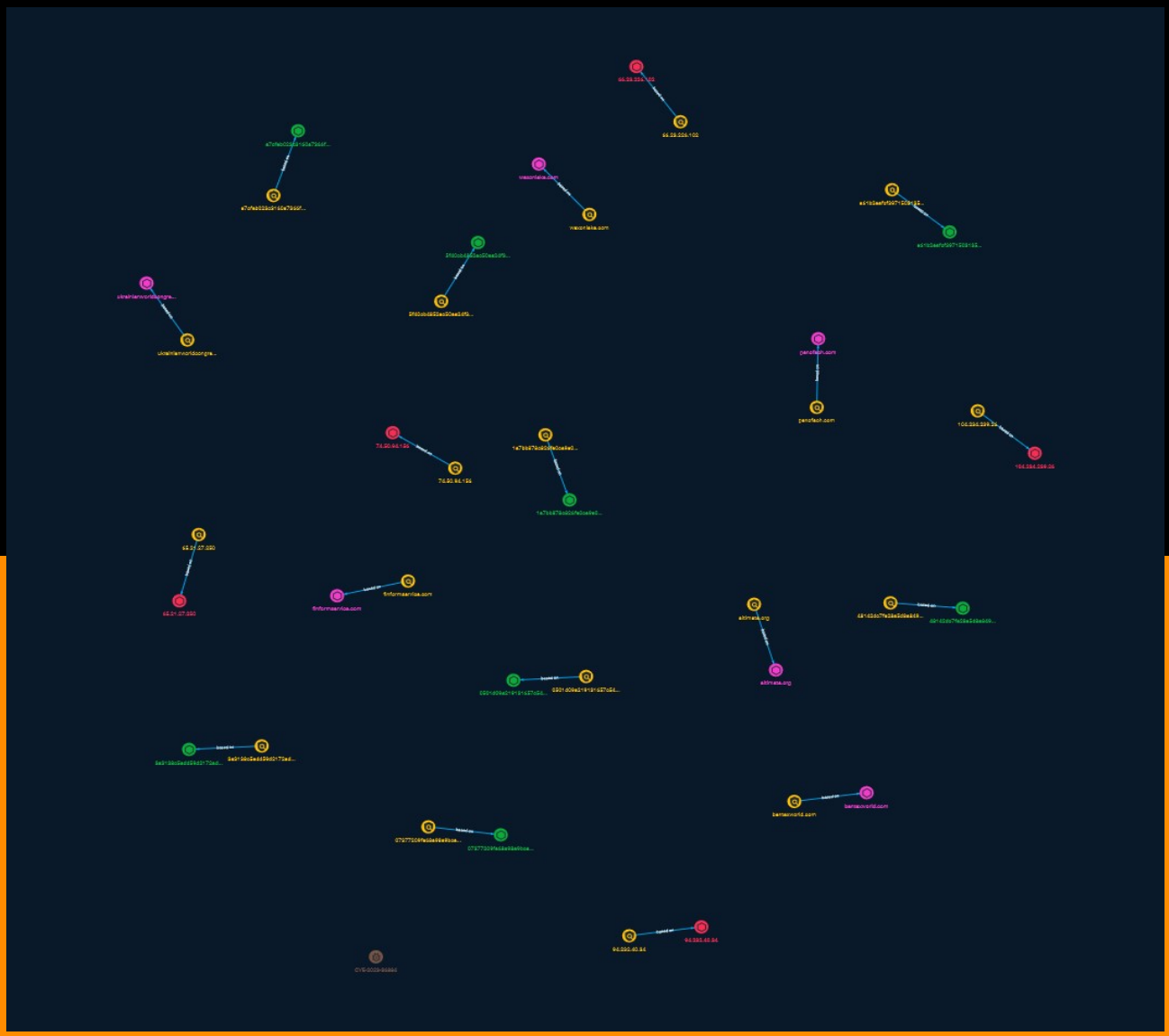

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers at Unit42 have published a threat analysis of CVE-2023-36884, a Microsoft Office and Windows HTML remote code vulnerability of important severity.

Confidence

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

15 / 100

Indicator

Name
wexonlake.com
Pattern Type
stix
Pattern
[domain-name:value = 'wexonlake.com']
Name
3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97']
Name

66.23.226.102

Pattern Type

stix

Pattern

[ipv4-addr:value = '66.23.226.102']

Name

48142dc7fe28a5d8a849fff11cb8206912e8382314a2f05e72abad0978b27e90

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '48142dc7fe28a5d8a849fff11cb8206912e8382314a2f05e72abad0978b27e90']

Name

ukrainianworldcongress.info

Pattern Type

stix

Pattern

[domain-name:value = 'ukrainianworldcongress.info']

Name
104.234.239.26
Pattern Type
stix
Pattern
[ipv4-addr:value = '104.234.239.26']
Name
bentaxworld.com
Pattern Type
stix
Pattern
[domain-name:value = 'bentaxworld.com']
Name
65.21.27.250
Pattern Type
stix
Pattern
[ipv4-addr:value = '65.21.27.250']

Name
finformservice.com
Pattern Type
stix
Pattern
[domain-name:value = 'finformservice.com']
Name
5f40cb4852ec50ee24f3cd951a172c725d02012d17dd645b6ce22d324aa140ad
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5f40cb4852ec50ee24f3cd951a172c725d02012d17dd645b6ce22d324aa140ad']
Name
altimata.org
Pattern Type
stix
Pattern

[domain-name:value = 'altimata.org']

Name

penofach.com

Pattern Type

stix

Pattern

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

Name

e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539']

Name

74.50.94.156

Pattern Type

stix

Pattern

[ipv4-addr:value = '74.50.94.156']

Name

94.232.40.34

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.232.40.34']

Name

1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f354930f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f354930f']

Name

0501d09a219131657c54dba71faf2b9d793e466f2c7fdf6b0b3c50ec5b866b2a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0501d09a219131657c54dba71faf2b9d793e466f2c7fdf6b0b3c50ec5b866b2a']

Name

07377209fe68a98e9bca310d9749daa4eb79558e9fc419cf0b02a9e37679038d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07377209fe68a98e9bca310d9749daa4eb79558e9fc419cf0b02a9e37679038d']

Name

a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f

Description

Rtf.Exploit.CVE_2017_0199-6335035-0

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f']
```

Vulnerability

Name
CVE-2023-36884

Domain-Name

Value
wexonlake.com
bentaxworld.com
finformservice.com
penofach.com
altimata.org
ukrainianworldcongress.info

StixFile

Value
1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f354930f
e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539
48142dc7fe28a5d8a849fff11cb8206912e8382314a2f05e72abad0978b27e90
3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97
5f40cb4852ec50ee24f3cd951a172c725d02012d17dd645b6ce22d324aa140ad
07377209fe68a98e9bca310d9749daa4eb79558e9fc419cf0b02a9e37679038d
0501d09a219131657c54dba71faf2b9d793e466f2c7fdf6b0b3c50ec5b866b2a
a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f

IPv4-Addr

Value
104.234.239.26
65.21.27.250
66.23.226.102
94.232.40.34
74.50.94.156

External References

- https://otx.alienvault.com/pulse/64b54e8c239d4457494dd91f
- https://unit42.paloaltonetworks.com/cve-2023-36884-rce/