Jul 12 2023

NETMANAGEIT

Intelligence Report

Loader activity for Formbook "QM18"

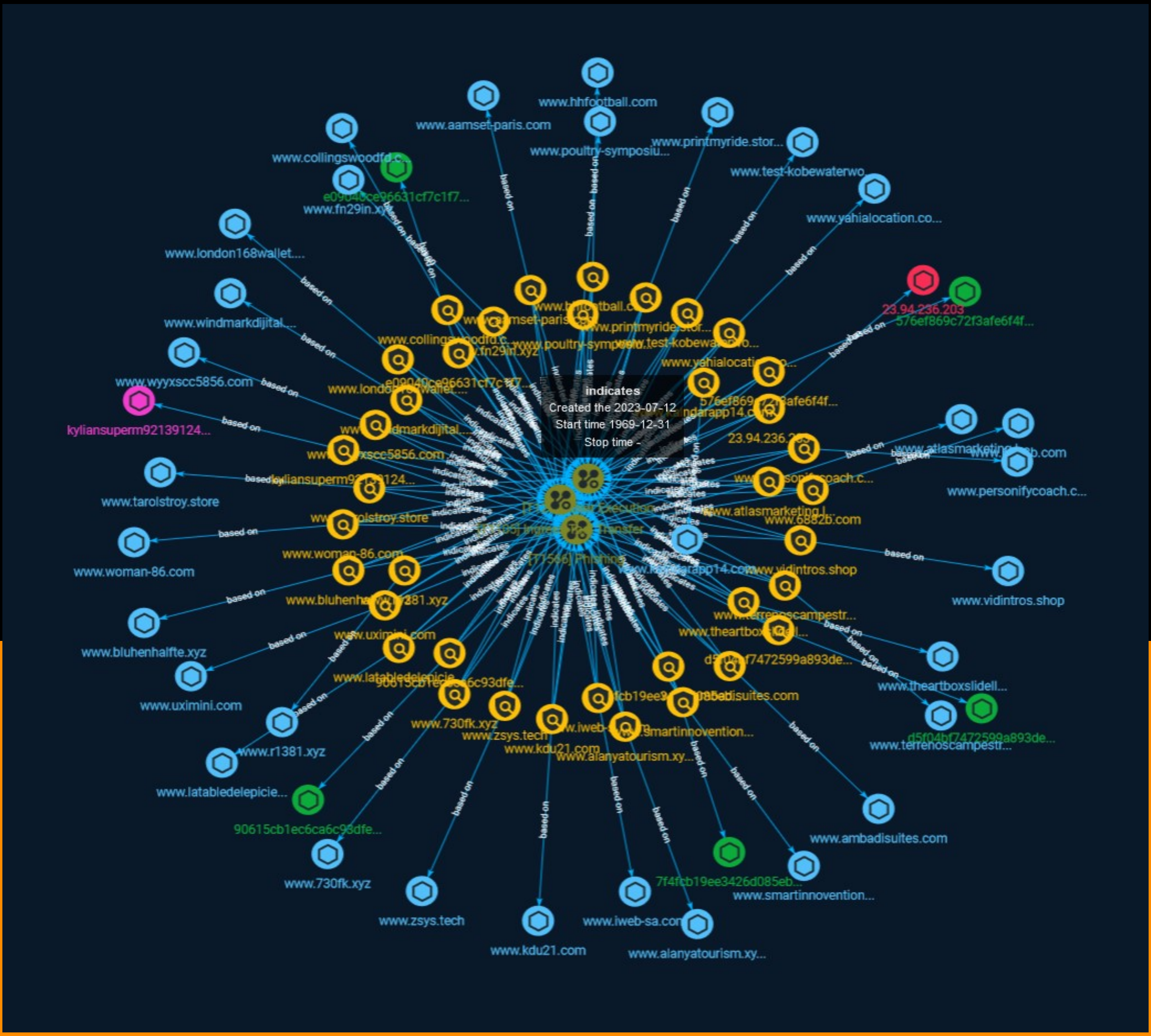

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Loader activity for Formbook QM18

Confidence

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

15 / 100

Indicator

Name
www.fn29in.xyz
Pattern Type
stix
Pattern
[hostname:value = 'www.fn29in.xyz']
Name
e09040ce96631cf7c1f7be6de48f961540e6fb8db97859c9fa7ae35f7fa9d930
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e09040ce96631cf7c1f7be6de48f961540e6fb8db97859c9fa7ae35f7fa9d930']
Name

7f4fcb19ee3426d085eb36f0f27d8fd3d0242d0aa057daa9f4d8a7cd68576045

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7f4fcb19ee3426d085eb36f0f27d8fd3d0242d0aa057daa9f4d8a7cd68576045']

Name

www.yahialocation.com

Pattern Type

stix

Pattern

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

Name

www.zsys.tech

Pattern Type

stix

Pattern

[hostname:value = 'www.zsys.tech']

Name
www.personifycoach.com
Pattern Type
stix
Pattern
[hostname:value = 'www.personifycoach.com']
Name
www.latabledelepicier.com
Pattern Type
stix
Pattern
[hostname:value = 'www.latabledelepicier.com']
Name
www.730fk.xyz
Pattern Type
stix
Pattern
[hostname:value = 'www.730fk.xyz']

Name

23.94.236.203

Description

ISP: ColoCrossing **OS:** None ------------------------- Hostnames: - 23-94-236-203-host.colocrossing.com ------------------------- Domains: - colocrossing.com ------------------------- Services: **80:** ``` HTTP/1.1 200 OK Date: Sun, 09 Jul 2023 08:09:11 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.1.17 Last-Modified: Thu, 06 Apr 2023 08:57:36 GMT ETag: "1443-5f8a719956000" Accept-Ranges: bytes Content-Length: 5187 Content-Type: text/html ``` ------------------ **443:** ``` HTTP/1.1 200 OK Date: Sun, 09 Jul 2023 05:18:28 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.1.17 Last-Modified: Thu, 06 Apr 2023 08:57:36 GMT ETag: "1443-5f8a719956000" Accept-Ranges: bytes Content-Length: 5187 Content-Type: text/html ``` HEARTBLEED: 2023/07/09 05:18:47 23.94.236.203:443 - SAFE ------------------ **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.94.236.203']

Name

www.windmarkdijital.xyz

Pattern Type

stix

Pattern

[hostname:value = 'www.windmarkdijital.xyz']

Name

www.iweb-sa.com

Pattern Type

stix

Pattern

[hostname:value = 'www.iweb-sa.com']

Name

576ef869c72f3afe6f4f5101f27aeb0d479cae8e5d348eea4e43e8af8252dfd0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '576ef869c72f3afe6f4f5101f27aeb0d479cae8e5d348eea4e43e8af8252dfd0']

Name

www.tarolstroy.store

Pattern Type

stix

Pattern

[hostname:value = 'www.tarolstroy.store']

Name

www.ambadisuites.com

Pattern Type

stix

Pattern

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

Name

www.wyyxscc5856.com

Pattern Type

stix

Pattern

[hostname:value = 'www.wyyxscc5856.com']

Name

www.london168wallet.monster

Pattern Type

stix

Pattern

[hostname:value = 'www.london168wallet.monster']

Name

www.kdu21.com

Pattern Type

stix

Pattern

[hostname:value = 'www.kdu21.com']

Name

www.poultry-symposium.com

Description

FormBook

Pattern Type

stix

Pattern

[hostname:value = 'www.poultry-symposium.com']

Name

www.terrenoscampestres.com

Pattern Type

stix

Pattern

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

Name

www.alanyatourism.xyz

Pattern Type

stix

Pattern

[hostname:value = 'www.alanyatourism.xyz']

Name

www.hhfootball.com

Pattern Type

stix

Pattern

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

Name

www.smartinnoventions.com

Pattern Type

stix

Pattern

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

Name

www.bluhenhalfte.xyz

Pattern Type

stix

Pattern

[hostname:value = 'www.bluhenhalfte.xyz']

Name

www.test-kobewaterworks.com

Pattern Type

stix

Pattern

[hostname:value = 'www.test-kobewaterworks.com']

Name

www.atlasmarketing.life

Pattern Type

stix

Pattern

[hostname:value = 'www.atlasmarketing.life']

Name

www.uximini.com

Pattern Type

stix

Pattern

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

Name

www.6882b.com

Pattern Type

stix

Pattern

[hostname:value = 'www.6882b.com']

Name

www.vidintros.shop

Pattern Type

stix

Pattern

[hostname:value = 'www.vidintros.shop']

Name

www.collingswoodfd.com

Pattern Type

stix

Pattern

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

Name

www.kalndarapp14.com

Pattern Type

stix

Pattern

[hostname:value = 'www.kalndarapp14.com']

Name

www.woman-86.com

Pattern Type

stix

Pattern

[hostname:value = 'www.woman-86.com']

Name

www.printmyride.store

Pattern Type

stix

Pattern

[hostname:value = 'www.printmyride.store']

Name

90615cb1ec6ca6c93dfe44f414c0d00db4e200c5011304df2c652182b4b593e3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90615cb1ec6ca6c93dfe44f414c0d00db4e200c5011304df2c652182b4b593e3']

Name

kyliansuperm92139124.shop

Pattern Type

stix

Pattern

[domain-name:value = 'kyliansuperm92139124.shop']

Name

d5f04bf7472599a893de61a21acb464ee11a9b7fbb2a20e348309857ee321691

Description

SUSP_INDICATOR_RTF_MalVer_Objects

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd5f04bf7472599a893de61a21acb464ee11a9b7fbb2a20e348309857ee321691']

Name

www.r1381.xyz

Pattern Type

stix

Pattern
[hostname:value = 'www.r1381.xyz']
Name
www.aamset-paris.com
Pattern Type
stix
Pattern
[hostname:value = 'www.aamset-paris.com']
Name
www.theartboxslidell.com
Pattern Type
stix
Pattern
[hostname:value = 'www.theartboxslidell.com']

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

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

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas)

Domain-Name

Value
kyliansuperm92139124.shop

StixFile

Value
90615cb1ec6ca6c93dfe44f414c0d00db4e200c5011304df2c652182b4b593e3
576ef869c72f3afe6f4f5101f27aeb0d479cae8e5d348eea4e43e8af8252dfd0
7f4fcb19ee3426d085eb36f0f27d8fd3d0242d0aa057daa9f4d8a7cd68576045
e09040ce96631cf7c1f7be6de48f961540e6fb8db97859c9fa7ae35f7fa9d930
d5f04bf7472599a893de61a21acb464ee11a9b7fbb2a20e348309857ee321691

Hostname

Value
www.6882b.com
www.uximini.com
www.windmarkdijital.xyz
www.ambadisuites.com
www.latabledelepicier.com
www.yahialocation.com
www.alanyatourism.xyz
www.atlasmarketing.life
www.poultry-symposium.com
www.zsys.tech
www.aamset-paris.com
www.terrenoscampestres.com
www.bluhenhalfte.xyz

www.vidintros.shop

www.iweb-sa.com

www.theartboxslidell.com

www.personifycoach.com

www.woman-86.com

www.collingswoodfd.com

www.tarolstroy.store

www.fn29in.xyz

www.hhfootball.com

www.kdu21.com

www.printmyride.store

www.smartinnoventions.com

www.kalndarapp14.com

www.test-kobewaterworks.com

www.730fk.xyz

www.wyyxscc5856.com

www.r1381.xyz

www.london168wallet.monster

IPv4-Addr

Value
23.94.236.203

External References

- https://otx.alienvault.com/pulse/64aec959f8017dda53219cd6
- https://isc.sans.edu/diary/rss/30020