Jul 11 2023

NETMANAGEIT

Intelligence Report

It’s Raining Phish and Scams – How Cloudflare Pages.dev and Workers.dev Domains Get Abused

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Recently, Trustwave observed more than 3,000 phishing emails containing phishing URLs abusing services at workers.dev and pages.dev domains.

Confidence

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

15 / 100

Indicator

Name
http://sondakikatokathaberleri.name.tr/hash/demo/mailer.php
Pattern Type
stix
Pattern
[url:value = 'http://sondakikatokathaberleri.name.tr/hash/demo/mailer.php']
Name
flexjobs-10.pages.dev
Pattern Type
stix
Pattern
[hostname:value = 'flexjobs-10.pages.dev']
Name
https://helpsana.ro/wp-hash/1/index4.php

Pattern Type

stix

Pattern

[url:value = 'https://helpsana.ro/wp-hash/1/index4.php']

Name

safe-cash98.pages.dev

Pattern Type

stix

Pattern

[hostname:value = 'safe-cash98.pages.dev']

Name

https://tutu57tututut.000webhostapp.com/don.php

Pattern Type

stix

Pattern

[url:value = 'https://tutu57tututut.000webhostapp.com/don.php']

Name

https://ancient-salad-4674.mmrctliacetgliue504.workers.dev/87c03eda-fdd4-4125-bf73-1b161178699a

Pattern Type

stix

Pattern

[url:value = 'https://ancient-salad-4674.mmrctliacetgliue504.workers.dev/87c03eda-fdd4-4125-bf73-1b161178699a']

Name

net-cash375.pages.dev

Pattern Type

stix

Pattern

[hostname:value = 'net-cash375.pages.dev']

Name

safe-cash90.pages.dev

Pattern Type

stix

Pattern

[hostname:value = 'safe-cash90.pages.dev']

Name
http://a211a49a8bb35.pages.dev/
Pattern Type
stix
Pattern
[url:value = 'http://a211a49a8bb35.pages.dev/']
Name
https://1-d0asfasfjhasfa7979352jhasf.pages.dev/
Pattern Type
stix
Pattern
[url:value = 'https://1-d0asfasfjhasfa7979352jhasf.pages.dev/']
Name
moneypro105.pages.dev
Pattern Type
stix
Pattern
[hostname:value = 'moneypro105.pages.dev']

Name
https://3f303073.45564355zezdfxc56e667.pages.dev/qrdcxw52463f86302yh72-fe4367z
Pattern Type
stix
Pattern
[url:value = 'https://3f303073.45564355zezdfxc56e667.pages.dev/qrdcxw52463f86302yh72-fe4367z']
Name
helpsana.ro
Pattern Type
stix
Pattern
[domain-name:value = 'helpsana.ro']
Name
sondakikatokathaberleri.name.tr
Pattern Type
stix
Pattern

[domain-name:value = 'sondakikatokathaberleri.name.tr']

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Attack-Pattern

Name
Malicious Link
ID
T1204.001
Description
An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). Links may also lead users to download files that require execution via [Malicious File](https://attack.mitre.org/techniques/T1204/002).
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)

Domain-Name

Value
sondakikatokathaberleri.name.tr
helpsana.ro

Hostname

Value
flexjobs-10.pages.dev
moneypro105.pages.dev
safe-cash98.pages.dev
net-cash375.pages.dev
safe-cash90.pages.dev

Url

Value
https://ancient-salad-4674.mmrctliacetgliue504.workers.dev/87c03eda-fdd4-4125-bf73-1b161178699a
http://sondakikatokathaberleri.name.tr/hash/demo/mailer.php
http://a211a49a8bb35.pages.dev/
https://1-d0asfasfjhasfa7979352jhasf.pages.dev/
https://tutu57tututut.000webhostapp.com/don.php
https://3f303073.45564355zezdfxc56e667.pages.dev/qrdcxw52463f86302yh72-fe4367z
https://helpsana.ro/wp-hash/1/index4.php

External References

- https://otx.alienvault.com/pulse/64ad7e4942c59b3fc4fbb6e1
- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/its-raining-phish-and-scams-how-cloudflare-pages-dev-and-workers-dev-domains-get-abused/