Sep 06 2023

NETMANAGEIT

Intelligence Report

"Smishing Triad" Targeted USPS And US Citizens For Data Theft

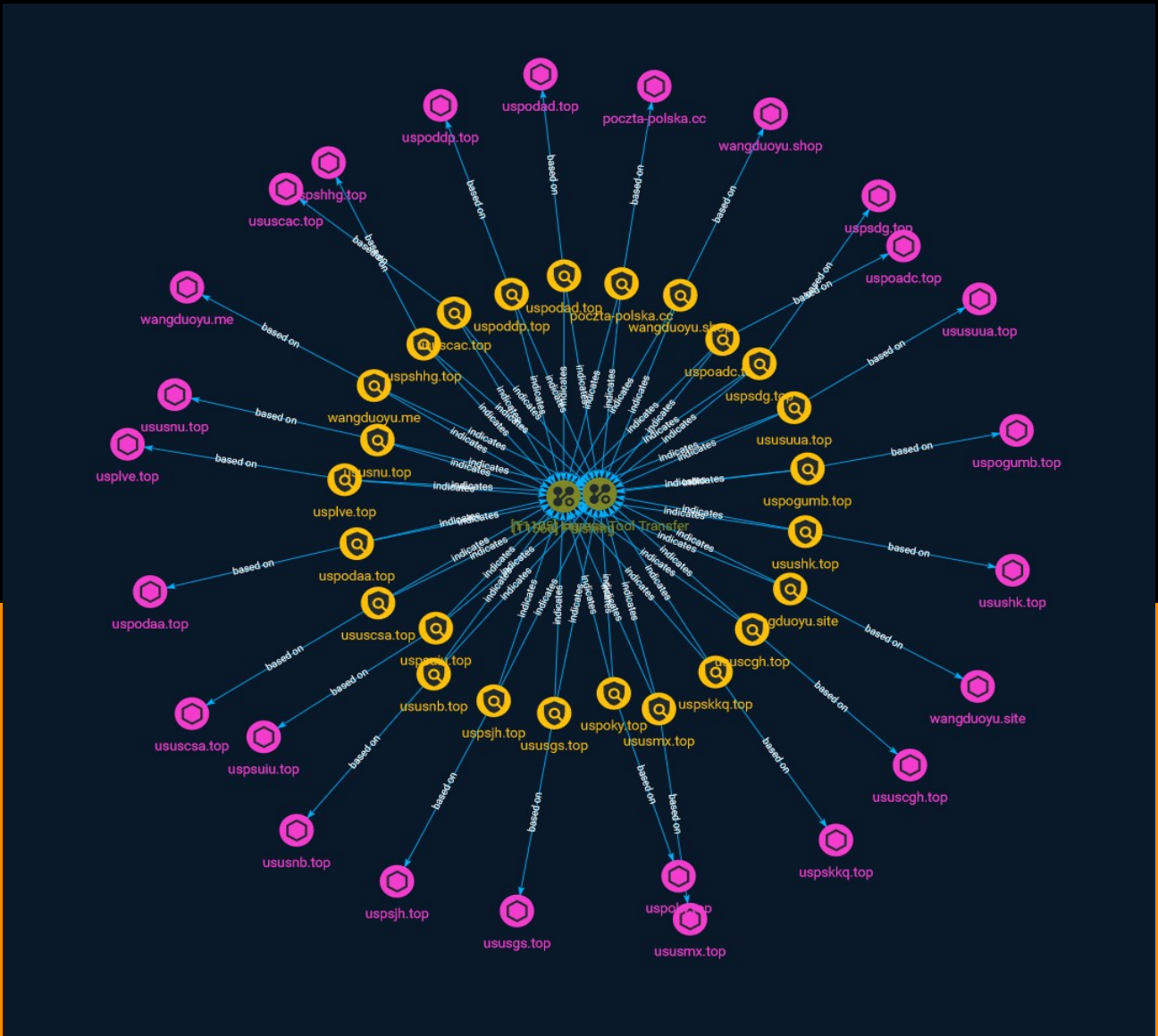

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Confidence

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

15 / 100

Indicator

Name
ususuua.top
Pattern Type
stix
Pattern
[domain-name:value = 'ususuua.top']
Name
ususmx.top
Pattern Type
stix
Pattern
[domain-name:value = 'ususmx.top']
Name
uspoddp.top

Pattern Type
stix
Pattern
[domain-name:value = 'uspoddp.top']
Name
ususnb.top
Pattern Type
stix
Pattern
[domain-name:value = 'ususnb.top']
Name
usplve.top
Pattern Type
stix
Pattern
[domain-name:value = 'usplve.top']
Name
wangduoyu.site

Pattern Type
stix
Pattern
[domain-name:value = 'wangduoyu.site']
Name
uspskkq.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspskkq.top']
Name
ususnu.top
Pattern Type
stix
Pattern
[domain-name:value = 'ususnu.top']
Name
uspodaa.top

Pattern Type
stix
Pattern
[domain-name:value = 'uspodaa.top']
Name
uspoky.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspoky.top']
Name
uspogumb.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspogumb.top']
Name
ususgs.top

Pattern Type
stix
Pattern
[domain-name:value = 'ususgs.top']
Name
uspoadc.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspoadc.top']
Name
poczta-polska.cc
Pattern Type
stix
Pattern
[domain-name:value = 'poczta-polska.cc']
Name
ususcgh.top

Pattern Type
stix
Pattern
[domain-name:value = 'ususcgh.top']
Name
wangduoyu.me
Pattern Type
stix
Pattern
[domain-name:value = 'wangduoyu.me']
Name
usushk.top
Pattern Type
stix
Pattern
[domain-name:value = 'usushk.top']
Name
uspshhg.top

Pattern Type
stix
Pattern
[domain-name:value = 'uspshhg.top']
Name
wangduoyu.shop
Pattern Type
stix
Pattern
[domain-name:value = 'wangduoyu.shop']
Name
uspsjh.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspsjh.top']
Name
uspodad.top

Pattern Type
stix
Pattern
[domain-name:value = 'uspodad.top']
Name
uspsdg.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspsdg.top']
Name
ususcsa.top
Pattern Type
stix
Pattern
[domain-name:value = 'ususcsa.top']
Name
ususcac.top

Pattern Type
stix
Pattern
[domain-name:value = 'ususcac.top']
Name
uspsuiu.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspsuiu.top']

Country

Name
Sweden
Name
Indonesia
Name
Poland
Name
United Kingdom of Great Britain and Northern Ireland
Name
Italy
Name
United States of America

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

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
uspshhg.top
uspoadc.top
ususnb.top
uspsdg.top
ususmx.top
usplve.top
usushk.top
ususcsa.top
uspsuiu.top
uspoky.top
wangduoyu.me
ususuua.top
ususgs.top

uspodaa.top
uspskkq.top
uspsjh.top
uspodad.top
uspogumb.top
uspoddp.top
wangduoyu.shop
ususnu.top
poczta-polska.cc
wangduoyu.site
ususcac.top
ususcgh.top

External References

- https://otx.alienvault.com/pulse/64f8ac7db00d8e26f15fa801
- https://www.resecurity.com/blog/article/smishing-triad-targeted-usps-and-us-citizens-for-data-theft