May 02 2024

NETMANAGEIT

Intelligence Report

Phishing Campaigns Targeting USPS See as Much Web Traffic as the USPS Itself

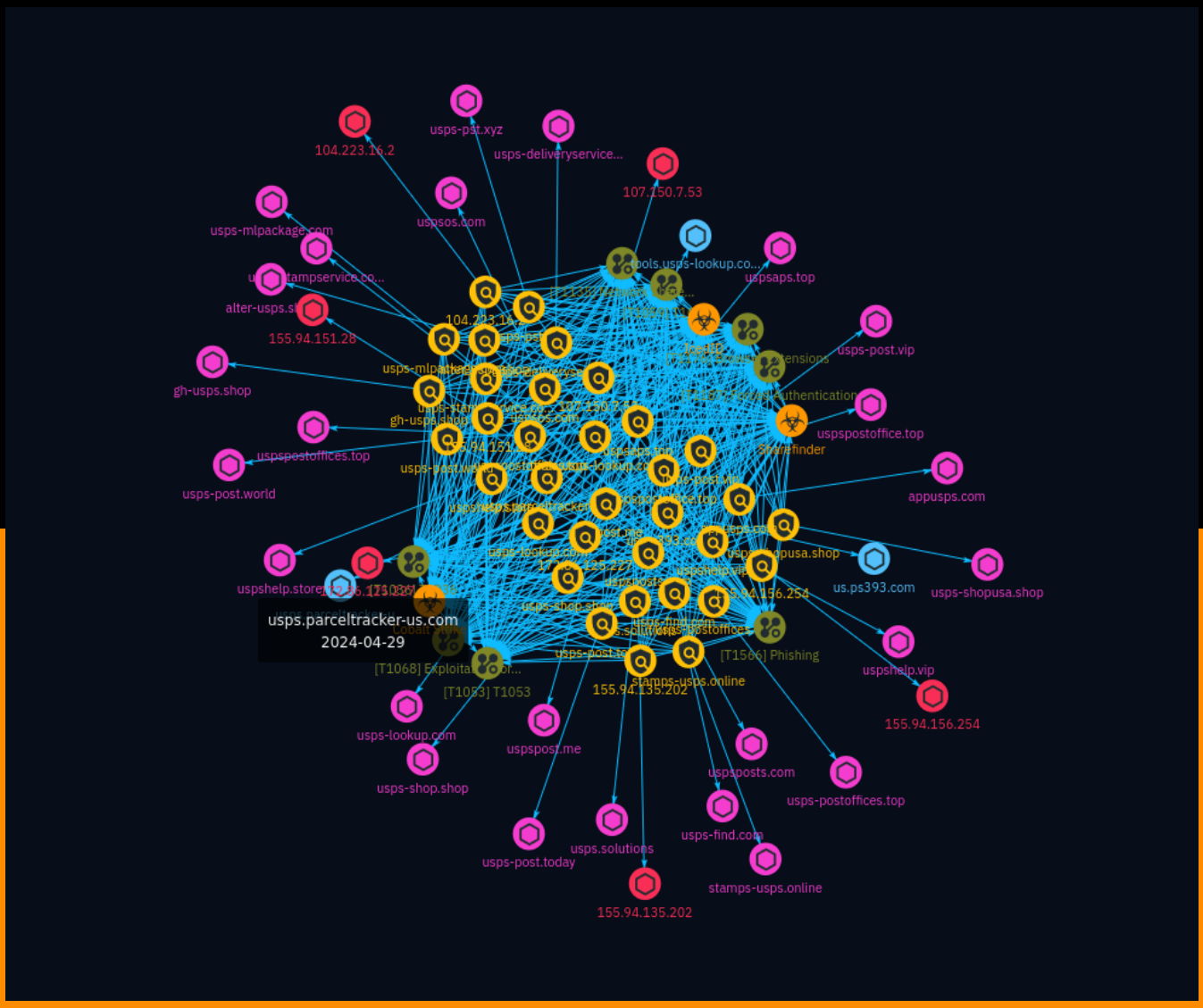

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Following the 2023 holiday season, Akamai researchers uncovered a significant amount of highly likely malicious activity and domains purporting to be associated with the United States Postal Service (USPS). Akamai researchers compared five months of DNS traffic to the legitimate domain, usps.com, with DNS traffic to illegitimate combosquatted domain names.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
usps.parceltracker-us.com
Pattern Type
stix
Pattern
[hostname:value = 'usps.parceltracker-us.com']
Name
us.ps393.com
Pattern Type
stix
Pattern
[hostname:value = 'us.ps393.com']
Name
tools.usps-lookup.com

Pattern Type
stix
Pattern
[hostname:value = 'tools.usps-lookup.com']
Name
uspsposts.com
Pattern Type
stix
Pattern
[domain-name:value = 'uspsposts.com']
Name
uspspostoffices.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspspostoffices.top']
Name
uspspostoffice.top

Pattern Type
stix
Pattern
[domain-name:value = 'uspspostoffice.top']
Name
uspspost.me
Pattern Type
stix
Pattern
[domain-name:value = 'uspspost.me']
Name
uspsos.com
Pattern Type
stix
Pattern
[domain-name:value = 'uspsos.com']
Name
uspshelp.vip

Pattern Type
stix
Pattern
[domain-name:value = 'uspshelp.vip']
Name
uspshelp.store
Pattern Type
stix
Pattern
[domain-name:value = 'uspshelp.store']
Name
uspsaps.top
Pattern Type
stix
Pattern
[domain-name:value = 'uspsaps.top']
Name
usps.solutions

Pattern Type
stix
Pattern
[domain-name:value = 'usps.solutions']
Name
usps-stampservice.com
Pattern Type
stix
Pattern
[domain-name:value = 'usps-stampservice.com']
Name
usps-shopusa.shop
Pattern Type
stix
Pattern
[domain-name:value = 'usps-shopusa.shop']
Name
usps-shop.shop

Pattern Type
stix
Pattern
[domain-name:value = 'usps-shop.shop']
Name
usps-pst.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'usps-pst.xyz']
Name
usps-postoffices.top
Pattern Type
stix
Pattern
[domain-name:value = 'usps-postoffices.top']
Name
usps-post.world

Pattern Type
stix
Pattern
[domain-name:value = 'usps-post.world']
Name
usps-post.vip
Pattern Type
stix
Pattern
[domain-name:value = 'usps-post.vip']
Name
usps-post.today
Pattern Type
stix
Pattern
[domain-name:value = 'usps-post.today']
Name
usps-mlpackage.com

Pattern Type
stix
Pattern
[domain-name:value = 'usps-mlpackage.com']
Name
usps-find.com
Pattern Type
stix
Pattern
[domain-name:value = 'usps-find.com']
Name
usps-lookup.com
Pattern Type
stix
Pattern
[domain-name:value = 'usps-lookup.com']
Name
usps-deliveryservice.icu

Pattern Type
stix
Pattern
[domain-name:value = 'usps-deliveryservice.icu']
Name
stamps-usps.online
Pattern Type
stix
Pattern
[domain-name:value = 'stamps-usps.online']
Name
gh-usps.shop
Pattern Type
stix
Pattern
[domain-name:value = 'gh-usps.shop']
Name
appusps.com

Pattern Type
stix
Pattern
[domain-name:value = 'appusps.com']
Name
172.86.125.227
Description
CC=US
Pattern Type
stix
Pattern
[ipv4-addr:value = '172.86.125.227']
Name
alter-usps.shop
Pattern Type
stix
Pattern
[domain-name:value = 'alter-usps.shop']

Name

155.94.156.254

Description

ISP: QuadraNet Enterprises LLC **OS:** - ---------- Services: **25:** ``` 220 skeltontribute.com ESMTP service ready 250-skeltontribute.com says hello 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250-8BITMIME 250-AUTH CRAM-MD5 250-AUTH=CRAM-MD5 250-XACK 250-SIZE 0 250-VERP 250 DSN ``` ---------- **53:** ``` ``` ---------- **53:** ``` ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Fri, 26 Apr 2024 20:12:43 GMT Server: Apache Content-Length: 2775 Connection: close Content-Type: text/html; charset=UTF-8 ``` ---------- **3128:** ``` HTTP/1.1 400 Bad Request Server: squid/3.5.20 Mime-Version: 1.0 Date: Mon, 29 Apr 2024 13:18:16 GMT Content-Type: text/html;charset=utf-8 Content-Length: 3510 X-Squid-Error: ERR_INVALID_URL 0 Vary: Accept-Language Content-Language: en Connection: close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '155.94.156.254']

Name

155.94.151.28

Description

CC=US ASN=AS30092 AS-30092

Pattern Type

stix

Pattern

[ipv4-addr:value = '155.94.151.28']

Name

107.150.7.53

Description

CC=US ASN=AS30092 AS-30092

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.150.7.53']

Name

155.94.135.202

Description

ISP: QuadraNet Enterprises LLC **OS:** - ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Sat, 27 Apr 2024 04:36:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '155.94.135.202']

Name

104.223.16.2

Description

CC=US ASN=AS30092 AS-30092

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.223.16.2']

Malware

Name
Sharefinder

Name
Cobalt Strike

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Name
IcedID

Description
[IcedID](https://attack.mitre.org/software/S0483) is a modular banking malware designed to steal financial information that has been observed in the wild since at least 2017. [IcedID](https://attack.mitre.org/software/S0483) has been downloaded by [Emotet]

(https://attack.mitre.org/software/S0367) in multiple campaigns.(Citation: IBM IcedID November 2017)(Citation: Juniper IcedID June 2020)

Attack-Pattern

Name

Forced Authentication

ID

T1187

Description

Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept. The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. (Citation: Wikipedia Server Message Block) This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources. Web Distributed Authoring and Versioning (WebDAV) is also typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443. (Citation: Didier Stevens WebDAV Traffic) (Citation: Microsoft Managing WebDAV Security) Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB/WebDAV authentication. An adversary can send an attachment to a user through spearphishing that contains a resource link to an external server controlled by the adversary (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)), or place a specially crafted file on navigation path for privileged accounts (e.g. .SCF file placed on desktop) or on a publicly accessible share to be accessed by victim(s). When the user's system accesses the untrusted resource it will attempt authentication and send information, including the user's hashed credentials, over SMB to the adversary controlled server. (Citation: GitHub Hashjacking) With access to the credential hash, an adversary can

perform off-line [Brute Force](https://attack.mitre.org/techniques/T1110) cracking to gain access to plaintext credentials. (Citation: Cylance Redirect to SMB) There are several different ways this can occur. (Citation: Osanda Stealing NetNTLM Hashes) Some specifics from in-the-wild use include: * A spearphishing attachment containing a document with a resource that is automatically loaded when the document is opened (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)). The document can include, for example, a request similar to `file[:]//[remote address]/Normal.dotm` to trigger the SMB request. (Citation: US-CERT APT Energy Oct 2017) * A modified .LNK or .SCF file with the icon filename pointing to an external reference such as `\\[remote address]\pic.png` that will force the system to load the resource when the icon is rendered to repeatedly gather credentials. (Citation: US-CERT APT Energy Oct 2017)

Name

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET

InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

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

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name

or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions for [Command and Control](https://attack.mitre.org/tactics/TA0011). (Citation: Stantinko Botnet)(Citation: Chrome Extension C2 Malware) Adversaries may also use browser extensions to modify browser permissions and components, privacy settings,

and other security controls for [Defense Evasion](https://attack.mitre.org/tactics/TA0005). (Citation: Browers FriarFox)(Citation: Browser Adrozek)

Name

T1053

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

Network Share Discovery

ID

T1135

Description

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network. File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the `net view \\\\remotesystem` command. It can also be used to query shared drives on the local system using `net share`. For macOS, the `sharing -l` command lists all shared points used for smb services.

Hostname

Value
us.ps393.com
usps.parceltracker-us.com
tools.usps-lookup.com

Domain-Name

Value
uspsposts.com
uspspostoffices.top
uspspostoffice.top
uspspost.me
uspsos.com
uspshelp.vip
uspshelp.store
uspsaps.top
usps.solutions
usps-stampservice.com
usps-shopusa.shop
usps-shop.shop
usps-pst.xyz

usps-postoffices.top

usps-post.world

usps-post.vip

usps-post.today

usps-mlpackage.com

usps-lookup.com

usps-find.com

usps-deliveryservice.icu

stamps-usps.online

gh-usps.shop

appusps.com

alter-usps.shop

IPv4-Addr

Value
172.86.125.227
155.94.156.254
107.150.7.53
155.94.151.28
155.94.135.202
104.223.16.2

External References

- https://www.akamai.com/blog/security-research/2024/apr/phishing-usps-malicious-domains-traffic-equal-to-legitimate-traffic
- https://otx.alienvault.com/pulse/662ff1ec26bd06238df792e8