Feb 01 2024

NETMANAGEIT

Intelligence Report

‘Tis the Season for Tax Hax

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Proofpoint researchers recently identified the return of TA576, a cybercriminal threat actor that uses tax-themed lures specifically targeting accounting and finance organizations. This actor is typically only active the first few months of the year during U.S. tax season, generally targeting organizations in North America with low-volume email campaigns.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

https://uploadfile2024.web.app/2023-FILES-MY1040-w2.zip

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** uploadfile2024.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://uploadfile2024.web.app/2023-FILES-MY1040-w2.zip']

Name

https://sacmuo.web.app/

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human':

'5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** sacmuo.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://sacmuo.web.app/']

Name

https://g3w2host.web.app/G3w2

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** g3w2host.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://g3w2host.web.app/G3w2']

Name

https://redirectit1.web.app/

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** redirectit1.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://redirectit1.web.app/']

Name

https://files-accl.zohopublic.eu/public/workdrive-public/download/dcyo813923950520542f6bba4f49d89fddf2d?x-cli-msg=%7B%22isFileOwner%22%3Afalse%2C%22version%22%3A%221.0%22%7D

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 25181 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Computers & Internet - **Domain Age:** {'human': '8 years ago', 'timestamp': 1455080400, 'iso': '2016-02-10T00:00:00-05:00'} - **IPQS: Domain:** files-accl.zohopublic.eu - **IPQS: IP Address:** 185.230.212.169

Pattern Type

stix

Pattern

[url:value = 'https://files-accl.zohopublic.eu/public/workdrive-public/download/dcyo813923950520542f6bba4f49d89fddf2d?x-cli-msg=%7B%22isFileOwner%22%3Afalse%2C%22version%22%3A%221.0%22%7D']

Name

https://2023-w2.web.app/2023-w2.zip

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** 2023-w2.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://2023-w2.web.app/2023-w2.zip']

Name

bvillegas@mountain-alliance.com

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 2 - **Overall Score:** 3 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** True - **Honeypot:** False - **Deliverability:** medium - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** True - **Timed Out:** False - **Suspect:** True - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** bvillegas@mountain-alliance.com - **Domain Age:** {'human': '1 week ago', 'timestamp': 1705956836, 'iso': '2024-01-22T15:53:56-05:00'} - **First Seen:** {'human': '2 days ago', 'timestamp': 1706650045, 'iso': '2024-01-30T16:27:25-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'bvillegas@mountain-alliance.com']

Name

charitytechw.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 week ago', 'timestamp': 1706032275, 'iso': '2024-01-23T12:51:15-05:00'} - **IPQS: Domain:** charitytechw.com - **IPQS: IP Address:** 104.21.35.77

Pattern Type

stix

Pattern

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

Name

https://charitytechw.com/Knitste12

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1

week ago', 'timestamp': 1706032275, 'iso': '2024-01-23T12:51:15-05:00'} - **IPQS: Domain:** charitytechw.com - **IPQS: IP Address:** 172.67.215.224

Pattern Type

stix

Pattern

[url:value = 'https://charitytechw.com/Knitste12']

Name

https://charitytechw.com/sew1.exe

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 week ago', 'timestamp': 1706032275, 'iso': '2024-01-23T12:51:15-05:00'} - **IPQS: Domain:** charitytechw.com - **IPQS: IP Address:** 104.21.35.77

Pattern Type

stix

Pattern

[url:value = 'https://charitytechw.com/sew1.exe']

Name

193.142.146.101

Description

- **Zip Code:** N/A - **ISP:** ColocationX - **ASN:** 208046 - **Organization:** ColocationX - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** 193.142.146.101 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.37850189 - **Longitude:** 4.89998007

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.142.146.101']

Name

f6c901d8959b26428c5fbb9b0c4a18be2057bb4d22e85bfe2442c0a8744a9ff6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6c901d8959b26428c5fbb9b0c4a18be2057bb4d22e85bfe2442c0a8744a9ff6']

Name

https://uploadfile2024.web.app/2023-FILES-MY1040-w2.zip

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** uploadfile2024.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://uploadfile2024.web.app/2023-FILES-MY1040-w2.zip']

Name

https://sacmuo.web.app/

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** sacmuo.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://sacmuo.web.app/']

Name

https://g3w2host.web.app/G3w2

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** g3w2host.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://g3w2host.web.app/G3w2']

Name

https://redirectit1.web.app/

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** redirectit1.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://redirectit1.web.app/']

Name

https://files-accl.zohopublic.eu/public/workdrive-public/download/dcyo813923950520542f6bba4f49d89fddf2d?x-cli-msg=%7B%22isFileOwner%22%3Afalse%2C%22version%22%3A%221.0%22%7D

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 25181 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Computers & Internet - **Domain Age:** {'human': '8 years ago', 'timestamp': 1455080400, 'iso': '2016-02-10T00:00:00-05:00'} - **IPQS: Domain:** files-accl.zohopublic.eu - **IPQS: IP Address:** 185.230.212.169

Pattern Type

stix

Pattern

[url:value = 'https://files-accl.zohopublic.eu/public/workdrive-public/download/dcyo813923950520542f6bba4f49d89fddf2d?x-cli-msg=%7B%22isFileOwner%22%3Afalse%2C%22version%22%3A%221.0%22%7D']

Name

https://2023-w2.web.app/2023-w2.zip

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 5491 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Hosting - **Domain Age:** {'human': '5 years ago', 'timestamp': 1546985104, 'iso': '2019-01-08T17:05:04-05:00'} - **IPQS: Domain:** 2023-w2.web.app - **IPQS: IP Address:** 199.36.158.100

Pattern Type

stix

Pattern

[url:value = 'https://2023-w2.web.app/2023-w2.zip']

Name

bvillegas@mountain-alliance.com

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 2 - **Overall Score:** 3 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** True - **Honeypot:** False - **Deliverability:** medium - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** True - **Timed Out:** False - **Suspect:** True - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** bvillegas@mountain-alliance.com - **Domain Age:** {'human': '1 week ago', 'timestamp': 1705956836, 'iso': '2024-01-22T15:53:56-05:00'} - **First Seen:** {'human': '2 days ago', 'timestamp': 1706650045, 'iso': '2024-01-30T16:27:25-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'bvillegas@mountain-alliance.com']

Name

charitytechw.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 week ago', 'timestamp': 1706032275, 'iso': '2024-01-23T12:51:15-05:00'} - **IPQS: Domain:** charitytechw.com - **IPQS: IP Address:** 104.21.35.77

Pattern Type

stix

Pattern

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

Name

https://charitytechw.com/Knitste12

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 week ago', 'timestamp': 1706032275, 'iso': '2024-01-23T12:51:15-05:00'} - **IPQS: Domain:** charitytechw.com - **IPQS: IP Address:** 172.67.215.224

Pattern Type

stix

Pattern

[url:value = 'https://charitytechw.com/Knitste12']

Name

https://charitytechw.com/sew1.exe

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 week ago', 'timestamp': 1706032275, 'iso': '2024-01-23T12:51:15-05:00'} - **IPQS: Domain:** charitytechw.com - **IPQS: IP Address:** 104.21.35.77

Pattern Type

stix

Pattern

[url:value = 'https://charitytechw.com/sew1.exe']

Name

193.142.146.101

Description

- **Zip Code:** N/A - **ISP:** ColocationX - **ASN:** 208046 - **Organization:** ColocationX - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** 193.142.146.101 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.37850189 - **Longitude:** 4.89998007

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.142.146.101']

Name

f6c901d8959b26428c5fbb9b0c4a18be2057bb4d22e85bfe2442c0a8744a9ff6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6c901d8959b26428c5fbb9b0c4a18be2057bb4d22e85bfe2442c0a8744a9ff6']

Malware

Name
Parallax RAT

Name
Parallax RAT

Intrusion-Set

Name
TA576

Name
TA576

Attack-Pattern

Name
T1193
ID
T1193
Name
Command and Scripting Interpreter
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

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

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

Masquerading

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/

T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

OS Credential Dumping

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Name

T1193

ID

T1193

Name

Command and Scripting Interpreter

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

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

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

Masquerading

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/

T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

OS Credential Dumping

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Country

Name
United States

Name
United States

Sector

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

Url

Value
https://uploadfile2024.web.app/2023-FILES-MY1040-w2.zip
https://sacmuo.web.app/
https://g3w2host.web.app/G3w2
https://redirectit1.web.app/
https://files-accl.zohopublic.eu/public/workdrive-public/download/dcyo813923950520542f6bba4f49d89fddf2d?x-cli-msg=%7B%22isFileOwner%22%3Afalse%2C%22version%22%3A%221.0%22%7D
https://2023-w2.web.app/2023-w2.zip
https://charitytechw.com/sew1.exe
https://charitytechw.com/Knitste12
https://uploadfile2024.web.app/2023-FILES-MY1040-w2.zip
https://sacmuo.web.app/
https://g3w2host.web.app/G3w2
https://redirectit1.web.app/

https://files-accl.zohopublic.eu/public/workdrive-public/download/dcyo813923950520542f6bba4f49d89fddf2d?x-cli-msg=%7B%22isFileOwner%22%3Afalse%2C%22version%22%3A%221.0%22%7D

https://2023-w2.web.app/2023-w2.zip

https://charitytechw.com/sew1.exe

https://charitytechw.com/Knitste12

Domain-Name

Value
charitytechw.com
charitytechw.com

Email-Addr

Value
bvillegas@mountain-alliance.com
bvillegas@mountain-alliance.com

StixFile

Value
f6c901d8959b26428c5fbb9b0c4a18be2057bb4d22e85bfe2442c0a8744a9ff6
f6c901d8959b26428c5fbb9b0c4a18be2057bb4d22e85bfe2442c0a8744a9ff6

IPv4-Addr

Value
193.142.146.101
193.142.146.101

External References

- https://www.proofpoint.com/us/blog/threat-insight/security-brief-tis-season-tax-hax
- https://otx.alienvault.com/pulse/65ba14e48f88c2ec9e697449