Mar 29 2024

NETMANAGEIT

Intelligence Report

Most prevalent malware files

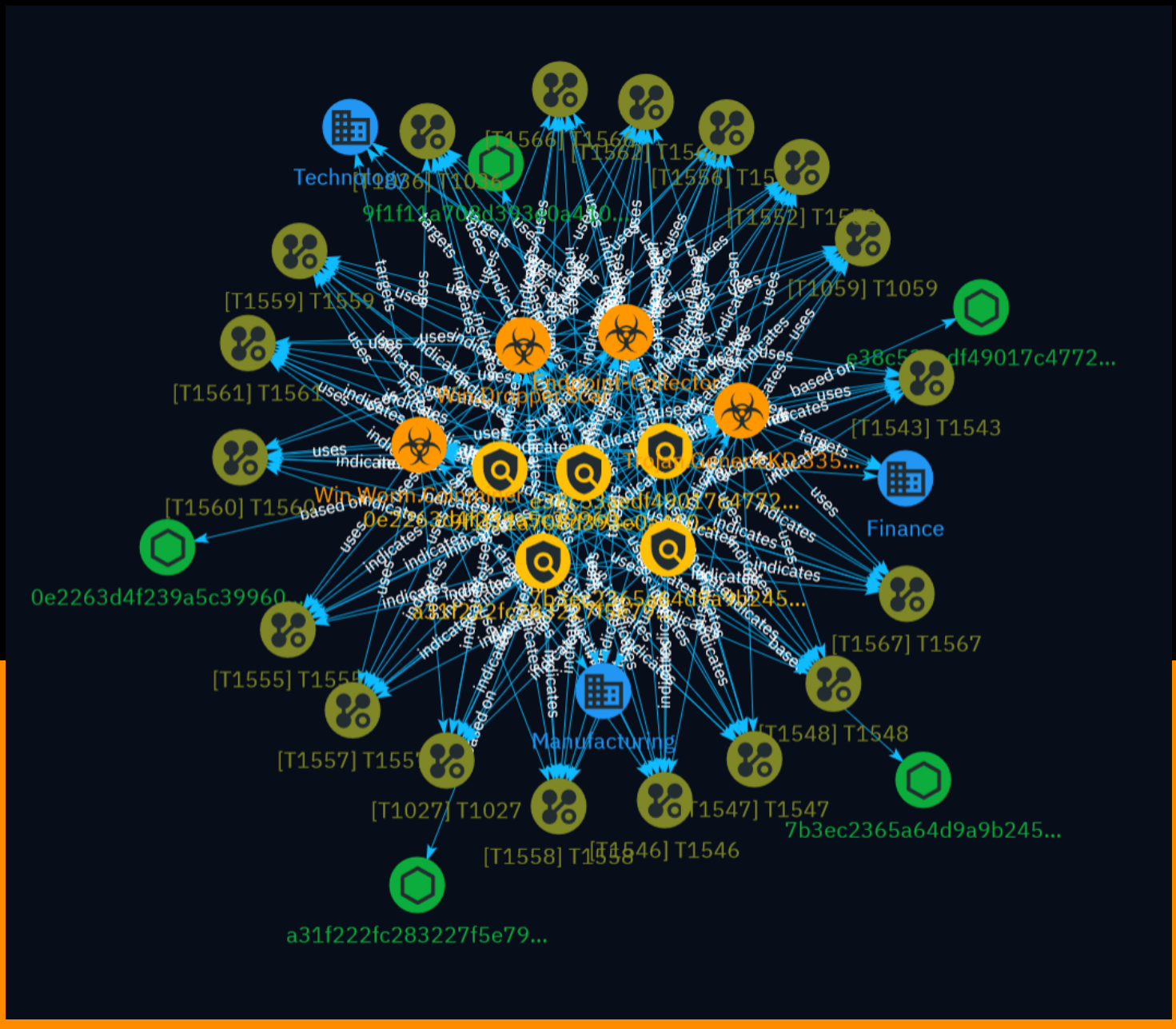

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Most prevalent malware files from Talos telemetry over the past week

Confidence

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

100 / 100

Content

N/A

Indicator

Name

e38c53aedf49017c47725e4912fc7560e1c8ece2633c05057b22fd4a8ed28eb3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e38c53aedf49017c47725e4912fc7560e1c8ece2633c05057b22fd4a8ed28eb3']

Name

a31f222fc283227f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a31f222fc283227f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91']

Name

9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507']

Name

7b3ec2365a64d9a9b2452c22e82e6d6ce2bb6dbc06c6720951c9570a5cd46fe5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7b3ec2365a64d9a9b2452c22e82e6d6ce2bb6dbc06c6720951c9570a5cd46fe5']

Name

0e2263d4f239a5c39960ffa6b6b688faa7fc3075e130fe0d4599d5b95ef20647

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'0e2263d4f239a5c39960ffa6b6b688faa7fc3075e130fe0d4599d5b95ef20647']
```

Malware

Name
Win.Dropper.Scar
Name
Trojan.GenericKD.33515991
Name
Win.Worm.Coinminer
Name
Endpoint-Collector

Attack-Pattern

Name
T1556
ID
T1556
Description
Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using [Valid Accounts](https://attack.mitre.org/techniques/T1078). Adversaries may maliciously modify a part of this process to either reveal credentials or bypass authentication mechanisms. Compromised credentials or access may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop.
Name
T1546
ID

T1546

Description

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events. (Citation: Backdooring an AWS account)(Citation: Varonis Power Automate Data Exfiltration) (Citation: Microsoft DART Case Report 001) Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked. (Citation: FireEye WMI 2015)(Citation: Malware Persistence on OS X)(Citation: amnesia malware) Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

Name

T1559

ID

T1559

Description

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern. Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange] (https://attack.mitre.org/techniques/T1559/002) or [Component Object Model](https://attack.mitre.org/techniques/T1559/001). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.(Citation: Linux IPC) Higher level

execution mediums, such as those of [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) to facilitate remote IPC execution.(Citation: Fireeye Hunting COM June 2019)

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

T1027

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

T1566

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

T1548

ID

T1548

Description

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

Name

T1560

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Name

T1552

ID

T1552

Description

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](https://attack.mitre.org/techniques/T1552/003)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://attack.mitre.org/techniques/T1552/002)), or other specialized files/artifacts (e.g. [Private Keys](https://attack.mitre.org/techniques/T1552/004)).

Name

T1558

ID

T1558

Description

Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as “realms”, there are three basic participants: client, service, and Key Distribution Center (KDC).(Citation: ADSecurity Kerberos Ring Decoder) Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to enable unauthorized access. On Windows, the built-in `klist` utility can be used to list and analyze cached Kerberos tickets.(Citation: Microsoft Klist) Linux systems on Active Directory domains store Kerberos credentials locally in the credential cache file referred to as the "ccache". The credentials are stored in the ccache file while they remain valid and generally while a user's session lasts.(Citation: MIT ccache) On modern Redhat Enterprise Linux systems, and derivative distributions, the System Security Services Daemon (SSSD) handles Kerberos tickets. By default SSSD maintains a copy of the ticket database that can be found in `/var/lib/sss/secrets/secrets.ldb` as well as the corresponding key located in `/var/lib/sss/secrets/.secrets.mkey`. Both files require root access to read. If an adversary is able to access the database and key, the credential cache Kerberos blob can be extracted and converted into a usable Kerberos ccache file that adversaries may use for [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). The ccache file may also be converted into a Windows format using tools such as Kekeo.(Citation: Linux Kerberos Tickets)(Citation: Brining MimiKatz to Unix)(Citation: Kekeo) Kerberos tickets on macOS are stored in a standard ccache format, similar to Linux. By default, access to these ccache entries is federated through the KCM daemon process via the Mach RPC protocol, which uses the caller's environment to determine access. The storage location for these ccache entries is influenced by the `/etc/krb5.conf` configuration file and the `KRB5CCNAME` environment variable which can specify to save them to disk or keep them protected via the KCM daemon. Users can interact with ticket storage using `kinit`, `klist`, `ktutil`, and `kcc` built-in binaries or via Apple's native Kerberos framework. Adversaries can use open source tools to interact with the ccache files directly or to use the Kerberos framework to call lower-level APIs for extracting the user's TGT or Service Tickets.(Citation: SpectorOps Bifrost Kerberos macOS 2019)(Citation: macOS kerberos framework MIT)

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) 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

T1567

ID

T1567

Description

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service

providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Name

T1555

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

T1562

ID

T1562

Description

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down.

These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

Name

T1547

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

T1561

ID

T1561

Description

Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources. With direct write access to a disk, adversaries may attempt to overwrite portions of disk data. Adversaries may opt to wipe arbitrary portions of disk data and/or wipe disk structures like the master boot record (MBR). A complete wipe of all disk sectors may be attempted. To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disks may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Novetta Blockbuster Destructive Malware) On network devices, adversaries may wipe configuration files and other data from the device using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `erase`.(Citation: erase_cmd_cisco)

Name

T1543

ID

T1543

Description

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons) Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect. Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.(Citation: OSX Malware Detection)

Name

T1557

ID

T1557

Description

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or replay attacks ([Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212)). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.(Citation: Rapid7 MiTM Basics) For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.(Citation: ttint_rat)(Citation: dns_changer_trojans)(Citation: ad_blocker_with_miner) Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials and session cookies. (Citation: volexity_0day_sophos_FW) [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)s can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.(Citation: mitm_tls_downgrade_att)(Citation: taxonomy_downgrade_att_tls)(Citation: tlseminar_downgrade_att) Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://attack.mitre.org/techniques/T1562) and/or in support of a [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

Sector

Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Technology
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.
Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

StixFile

Value
e38c53aedf49017c47725e4912fc7560e1c8ece2633c05057b22fd4a8ed28eb3
a31f222fc283227f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91
9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507
7b3ec2365a64d9a9b2452c22e82e6d6ce2bb6dbc06c6720951c9570a5cd46fe5
0e2263d4f239a5c39960ffa6b6b688faa7fc3075e130fe0d4599d5b95ef20647

External References

- https://blog.talosintelligence.com/threat-source-newsletter-enter-the-substitute-teacher/
- https://otx.alienvault.com/pulse/6606bcbdb712ff97f8369bd8