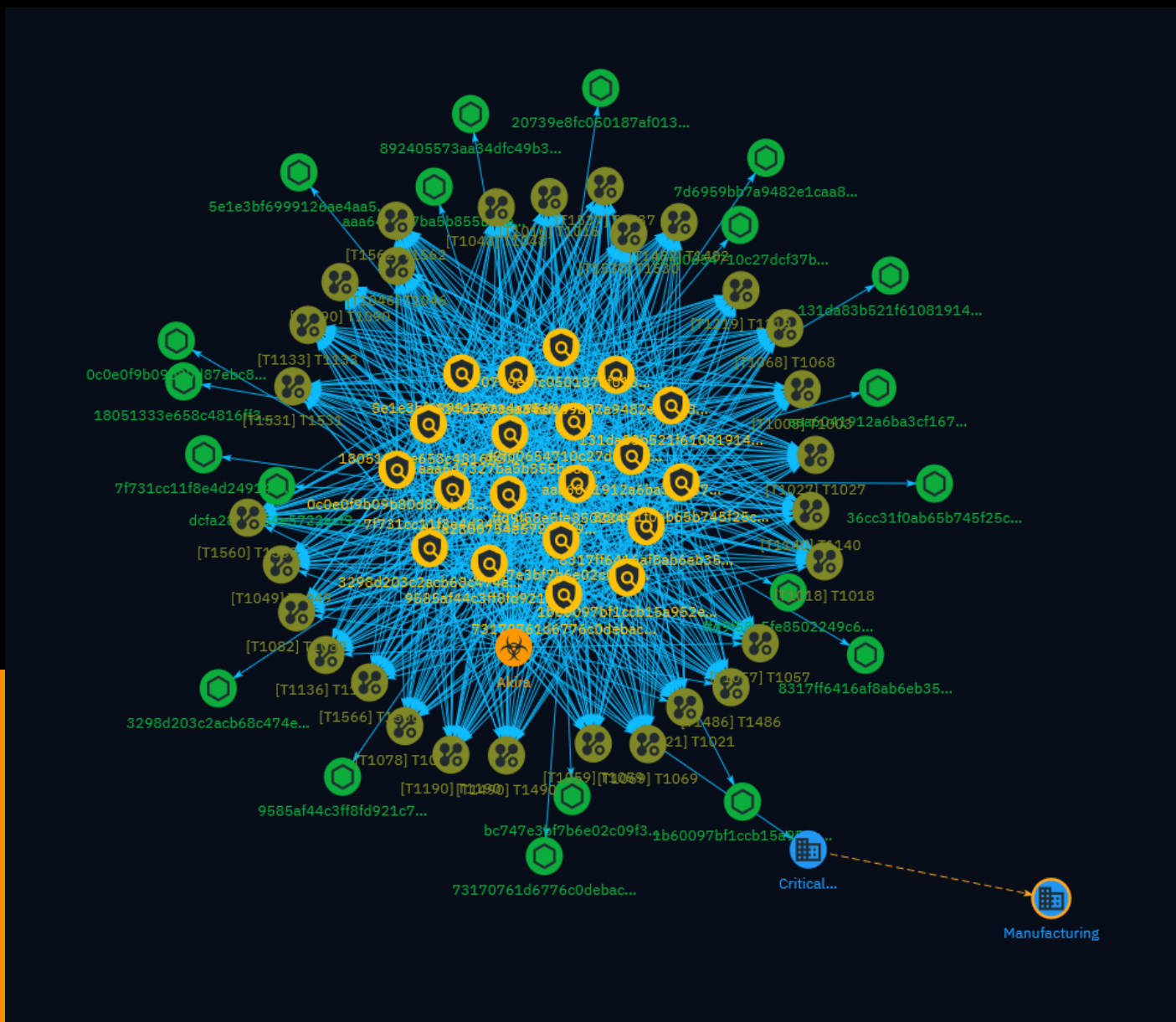


# NETMANAGEIT

## Intelligence Report

# #StopRansomware: Akira Ransomware



# Table of contents

---

## Overview

---

● Description	4
● Confidence	4
● Content	5

---

## Entities

---

● Indicator	6
● Malware	15
● Attack-Pattern	16
● Sector	37

---

## Observables

---

● StixFile	38
------------	----



## External References

- External References

40

# Overview

## Description

The CISA cybersecurity and Infrastructure Security Agency (CISA) is working with the European Union to prevent the release of the Akira ransomware, a type of ransomware that locks people out of their computers and demands a ransom.

## Confidence

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

100 / 100

# Content

N/A

# Indicator

**Name**

ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc

**Pattern Type**

stix

**Pattern**

```
[file:hashes!'SHA-256' =  
'ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc']
```

**Name**

dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e

**Pattern Type**

stix

**Pattern**

```
[file:hashes!'SHA-256' =  
'dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e']
```

**Name**

d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'd2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca']

**Name**

bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138

**Description**

ConventionEngine\_Keyword\_Bot

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138']

**Name**

aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9

**Description**

dbgdetect\_files

**Pattern Type**

stix

**Pattern**

[file:hashes:'SHA-256' =  
'aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9']

**Name**

aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d

**Pattern Type**

stix

**Pattern**

[file:hashes:'SHA-256' =  
'aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d']

**Name**

9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065

**Pattern Type**

stix

**Pattern**

[file:hashes:'SHA-256' =  
'9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065']



**Name**

892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0

**Description**

Nullsoft\_NSIS

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0']

**Name**

8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694']

**Name**

7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be

**Description**

ConventionEngine\_Term\_Copy

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be']

**Name**

7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4']

**Name**

73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf']

**Name**

5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32']

**Name**

36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c

**Description**

InnoSetupInstaller

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c']

**Name**

3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75']

**Name**

20739e8fc050187af013e2499718895e4c980699ccaf046b2f96b12497e61959

**Description**

SHA256 of 7a647af3c112ad805296a22b2a276e7c

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'20739e8fc050187af013e2499718895e4c980699ccaf046b2f96b12497e61959']

**Name**

1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386']

**Name**

18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88

**Description**

SLF:Trojan:PowerShell/PSExploitCredAPI.A

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88']

**Name**

131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07']

**Name**

0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d

**Pattern Type**

stix

**Pattern**

[file:hashes:'SHA-256' =  
'0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d']

# Malware

**Name**

Akira

# Attack-Pattern

## Name

T1490

## ID

T1490

## Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](<https://attack.mitre.org/techniques/T1485>) and [Data Encrypted for Impact](<https://attack.mitre.org/techniques/T1486>).(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable\_notif\_synology\_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: \* `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` \* [Windows Management Instrumentation](<https://attack.mitre.org/techniques/T1047>) can be used to delete volume shadow copies - `wmic shadowcopy delete` \* `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` \* `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` \* `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](<https://attack.mitre.org/techniques/T1561>) to delete



backup firmware images and reformat the file system, then [System Shutdown/Reboot] (<https://attack.mitre.org/techniques/T1529>) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

**Name**

T1046

**ID**

T1046

**Description**

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021) Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well. Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host’s registered services on the network. For example, adversaries can use a mDNS query (such as ``dns-sd -B _ssh._tcp .``) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

**Name**

T1018

**ID**

T1018

**Description**

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or `net view` using [Net](https://attack.mitre.org/software/S0039). Adversaries may also analyze data from local host files (ex: `C:\Windows\System32\Drivers\etc\hosts` or `/etc/hosts`) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment. Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network (e.g. `show cdp neighbors`, `show arp`).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

**Name**

T1136

**ID**

T1136

**Description**

Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system. Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

**Name**

T1537

**ID**

T1537

**Description**

Adversaries may exfiltrate data by transferring the data, including backups of cloud environments, to another cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection. A defender who is monitoring for large transfers to outside the cloud environment through normal file transfers or over command and control channels may not be watching for data transfers to another account within the same cloud provider. Such transfers may utilize existing cloud provider APIs and the internal address space of the cloud provider to blend into normal traffic or avoid data transfers over external network interfaces. Incidents have been observed where adversaries have created backups of cloud instances and transferred them to separate accounts.(Citation: DOJ GRU Indictment Jul 2018)

**Name**

T1486

**ID**

T1486

**Description**

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](<https://attack.mitre.org/techniques/T1222>) or [System

Shutdown/Reboot](<https://attack.mitre.org/techniques/T1529>), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack 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: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](<https://attack.mitre.org/techniques/T1491/001>), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted. (Citation: Rhino S3 Ransomware Part 1)

**Name**

T1531

**ID**

T1531

**Description**

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](<https://attack.mitre.org/techniques/T1529>) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019) In Windows, [Net](<https://attack.mitre.org/software/S0039>) utility, `Set-LocalUser`` and `Set-ADAccountPassword`` [PowerShell](<https://attack.mitre.org/techniques/T1059/001>) cmdlets may be used by adversaries to modify user accounts. In Linux, the `passwd`` utility may be used to change passwords. Accounts could also be disabled by Group Policy. Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](<https://attack.mitre.org/techniques/T1485>) and [Defacement](<https://attack.mitre.org/techniques/T1491>), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](<https://attack.mitre.org/techniques/T1486>) objective.

**Name**

T1068

**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**

T1078

**ID**

T1078

**Description**

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials 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, network devices, and remote desktop.(Citation: volexity\_0day\_sophos\_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

**Name**

T1048

**ID**

T1048

**Description**

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels. [Exfiltration Over Alternative Protocol](<https://attack.mitre.org/techniques/T1048>) can be done using various common operating system utilities such as

[Net](https://attack.mitre.org/software/S0039)/SMB or FTP.(Citation: Palo Alto OilRig Oct 2016) On macOS and Linux `curl` may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.(Citation: 20 macOS Common Tools and Techniques) Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive information via the web console or [Cloud API](https://attack.mitre.org/techniques/T1059/009).

**Name**

T1057

**ID**

T1057

**Description**

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via `/proc`. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show\_processes\_cisco\_cmd)

**Name**

T1049

**ID**

T1049

**Description**

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](<https://attack.mitre.org/software/S0104>), "net use," and "net session" with [Net](<https://attack.mitre.org/software/S0039>). In Mac and Linux, [netstat](<https://attack.mitre.org/software/S0104>) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

**Name**

T1482

**ID**

T1482

**Description**

Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.(Citation: Microsoft Trusts) Domain trusts allow the users of the trusted domain to access resources in the



trusting domain. The information discovered may help the adversary conduct [SID-History Injection](<https://attack.mitre.org/techniques/T1134/005>), [Pass the Ticket](<https://attack.mitre.org/techniques/T1550/003>), and [Kerberoasting](<https://attack.mitre.org/techniques/T1558/003>). (Citation: AdSecurity Forging Trust Tickets) (Citation: Harmj0y Domain Trusts) Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP. (Citation: Harmj0y Domain Trusts) The Windows utility [Nltest](<https://attack.mitre.org/software/S0359>) is known to be used by adversaries to enumerate domain trusts. (Citation: Microsoft Operation Wilysupply)

**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**

T1090

**ID**

T1090

**Description**

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](<https://attack.mitre.org/software/S0040>), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

**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**

T1016

**ID**

T1016

**Description**

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. `show ip route`, `show ip interface`). (Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion ) Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

**Name**

T1021

**ID**

T1021

**Description**

Adversaries may use [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP). (Citation: SSH Secure Shell) (Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](<https://attack.mitre.org/techniques/T1072>) and other administrative programs) may utilize [Remote Services](<https://attack.mitre.org/techniques/T1021>) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](<https://attack.mitre.org/techniques/T1021/005>) to send the screen and control buffers and [SSH](<https://attack.mitre.org/techniques/T1021/004>) for secure file transfer. (Citation: Remote Management MDM macOS) (Citation: Kickstart Apple Remote Desktop commands) (Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data. (Citation: FireEye 2019 Apple Remote Desktop) (Citation: Lockboxx ARD 2019) (Citation: Kickstart Apple Remote Desktop commands)

**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**

T1219

**ID**

T1219

**Description**

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land) (Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Remote access software may be installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary controlled system. Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access. Installation of many remote access software may also include persistence (e.g., the software's installation routine creates a [Windows Service](<https://attack.mitre.org/techniques/T1543/003>)).

**Name**

T1190

**ID**

T1190

**Description**

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion] (<https://attack.mitre.org/techniques/T1211>). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](<https://attack.mitre.org/techniques/T1611>), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

**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**

T1140

**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**

T1082

**ID**

T1082

**Description**



An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](<https://attack.mitre.org/techniques/T1082>) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](<https://attack.mitre.org/software/S0096>) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) on network devices to gather detailed system information (e.g. `show version`). (Citation: US-CERT-TA18-106A) [System Information Discovery](<https://attack.mitre.org/techniques/T1082>) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment. (Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine. (Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virtual Machine API)

**Name**

T1530

**ID**

T1530

**Description**

Adversaries may access data from cloud storage. Many IaaS providers offer solutions for online data object storage such as Amazon S3, Azure Storage, and Google Cloud Storage. Similarly, SaaS enterprise platforms such as Office 365 and Google Workspace provide cloud-based document storage to users through services such as OneDrive and Google Drive, while SaaS application providers such as Slack, Confluence, Salesforce, and Dropbox may provide cloud storage solutions as a peripheral or primary use case of their platform. In some cases, as with IaaS-based cloud storage, there exists no overarching application (such as SQL or Elasticsearch) with which to interact with the stored objects: instead, data from these solutions is retrieved directly through the [Cloud API](<https://attack.mitre.org/>)

techniques/T1059/009). In SaaS applications, adversaries may be able to collect this data directly from APIs or backend cloud storage objects, rather than through their front-end application or interface (i.e., [Data from Information Repositories](https://attack.mitre.org/techniques/T1213)). Adversaries may collect sensitive data from these cloud storage solutions. Providers typically offer security guides to help end users configure systems, though misconfigurations are a common problem.(Citation: Amazon S3 Security, 2019) (Citation: Microsoft Azure Storage Security, 2019)(Citation: Google Cloud Storage Best Practices, 2019) There have been numerous incidents where cloud storage has been improperly secured, typically by unintentionally allowing public access to unauthenticated users, overly-broad access by all users, or even access for any anonymous person outside the control of the Identity Access Management system without even needing basic user permissions. This open access may expose various types of sensitive data, such as credit cards, personally identifiable information, or medical records.(Citation: Trend Micro S3 Exposed PII, 2017)(Citation: Wired Magecart S3 Buckets, 2019)(Citation: HIPAA Journal S3 Breach, 2017)(Citation: Rclone-mega-extortion\_05\_2021) Adversaries may also obtain then abuse leaked credentials from source repositories, logs, or other means as a way to gain access to cloud storage objects.

**Name**

T1069

**ID**

T1069

**Description**

Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions. Adversaries may attempt to discover group permission settings in many different ways. This data may provide the adversary with information about the compromised environment that can be used in follow-on activity and targeting.(Citation: CrowdStrike BloodHound April 2018)

**Name**

T1133

**ID**

T1133

**Description**

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](<https://attack.mitre.org/techniques/T1021/006>) and [VNC](<https://attack.mitre.org/techniques/T1021/005>) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

**Name**

T1003

**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.

# Sector

**Name**

Critical Infrastructure

**Description**

Private entities working to transform raw materials into manufactured products (Chemicals, metal etc.).

**Name**

Manufacturing

**Description**

Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.

# StixFile

## Value

ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc

dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e

d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca

bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138

aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9

aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d

9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065

892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0

8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694

7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be

7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4

73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf

5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32

**TLP:CLEAR**

36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c

3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75

20739e8fc050187af013e2499718895e4c980699ccaf046b2f96b12497e61959

1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386

18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88

131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07

0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d

# External References

- 
- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>
- 
- <https://otx.alienvault.com/pulse/662275c281f26134a0a89e72>