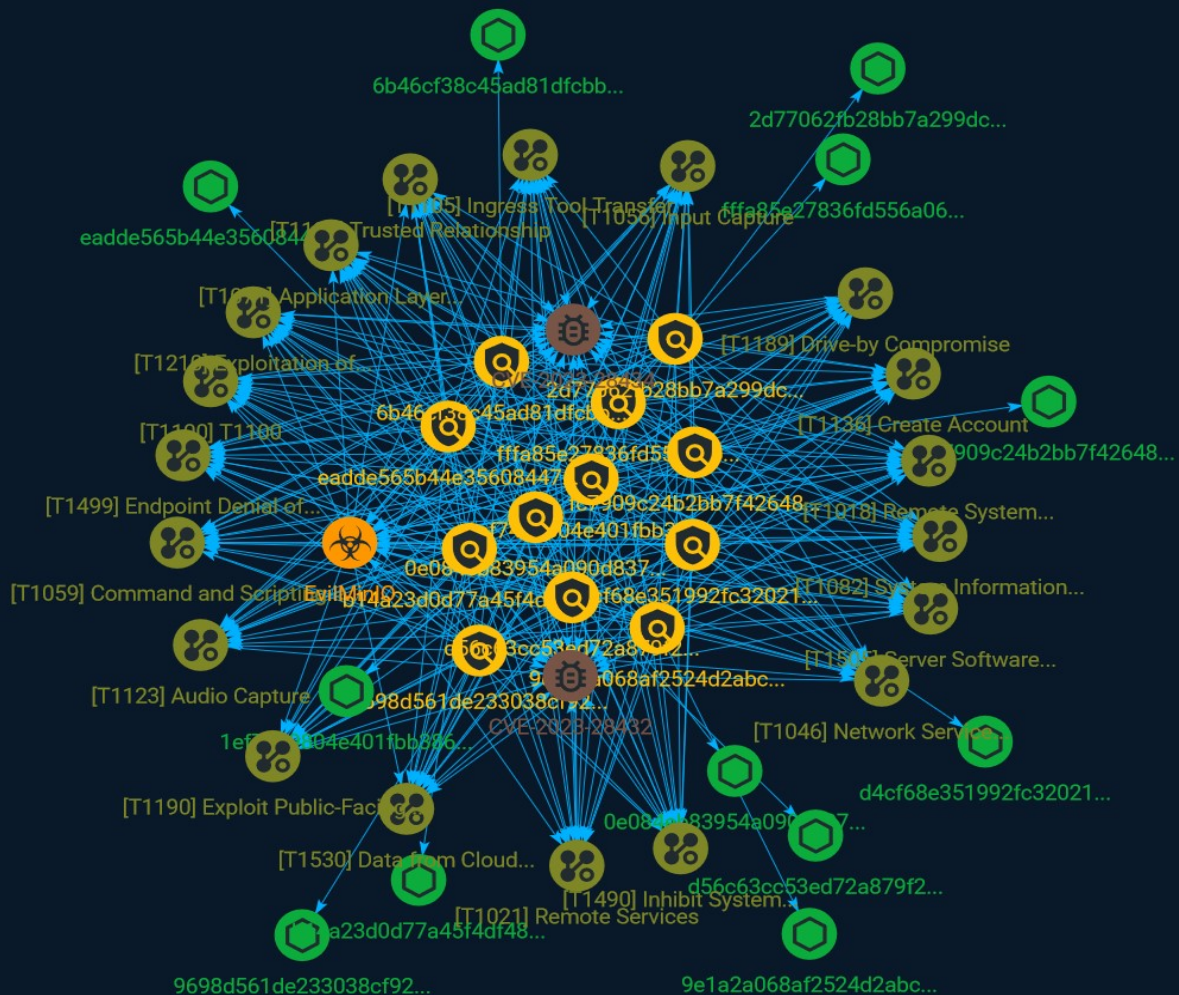




NETMANAGEIT

# Intelligence Report

## New Attack Vector In The Cloud: Attackers caught exploiting Object Storage Services



# Table of contents

---

## Overview

---

● Description	4
● Confidence	4

---

---

## Entities

---

● Indicator	5
● Malware	10
● Vulnerability	11
● Attack-Pattern	12

---

---

## Observables

---

● StixFile	26
------------	----

---



## External References

- External References

27

# Overview

## Description

A new attack vector in the cloud is being exploited by attackers using non-native object storage services, according to Security Joes' Incident Response (IR).

## Confidence

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

15 / 100

# Indicator

**Name**

1ef7419804e401fbb3860862c2b2fbc1ec3c4650fe24fb44f787f81acf6ad65b

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'1ef7419804e401fbb3860862c2b2fbc1ec3c4650fe24fb44f787f81acf6ad65b']

**Name**

0e084eb83954a090d83730b157f20549cf90b9d0206f5fd0bbcff009788eeafd

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'0e084eb83954a090d83730b157f20549cf90b9d0206f5fd0bbcff009788eeafd']

**Name**

ffa85e27836fd556a06660ac0ad76a35ef02687652a81194821c538e847d58f

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'ffa85e27836fd556a06660ac0ad76a35ef02687652a81194821c538e847d58f']

**Name**

9e1a2a068af2524d2abc48c1edf46de8cfa3329d3688164db5969bc1914377fc

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'9e1a2a068af2524d2abc48c1edf46de8cfa3329d3688164db5969bc1914377fc']

**Name**

eadde565b44e35608447b056761ba172b608b796418ab1244607dc17d21f05e3

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'eadde565b44e35608447b056761ba172b608b796418ab1244607dc17d21f05e3']

**Name**

fc7909c24b2bb7f42648c605deacb3ae4f9574b95a562dd165e5e9aca2cc7d74

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'fc7909c24b2bb7f42648c605deacb3ae4f9574b95a562dd165e5e9aca2cc7d74']

**Name**

9698d561de233038cf922b0de4a0bbb8e5723c800b4bc04c7ac82d92cb715dfd

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'9698d561de233038cf922b0de4a0bbb8e5723c800b4bc04c7ac82d92cb715dfd']

**Name**

6b46cf38c45ad81dfcbbd77a1b196c5dea147088f6dab1b1920a508d61bb03ed

**Pattern Type**

stix

**Pattern**

[file:hashes:'SHA-256' =  
'6b46cf38c45ad81dfcbbd77a1b196c5dea147088f6dab1b1920a508d61bb03ed']

**Name**

d4cf68e351992fc32021c75820f7d2a858796dd9dc245b7fbbf2cef8656081b2

**Pattern Type**

stix

**Pattern**

[file:hashes:'SHA-256' =  
'd4cf68e351992fc32021c75820f7d2a858796dd9dc245b7fbbf2cef8656081b2']

**Name**

b14a23d0d77a45f4df4889b0c2d239fb118f9d16f944571a8b4d08603d16fb41

**Pattern Type**

stix

**Pattern**

[file:hashes:'SHA-256' =  
'b14a23d0d77a45f4df4889b0c2d239fb118f9d16f944571a8b4d08603d16fb41']

**Name**



2d77062fb28bb7a299dcb8fa4ed62503d19ea6b8bd14e4f7ec78c54b9d08f052

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'2d77062fb28bb7a299dcb8fa4ed62503d19ea6b8bd14e4f7ec78c54b9d08f052']

**Name**

d56c63cc53ed72a879f224ab85019db5fc2c30e8f193c1147975d46e3f5d913a

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'd56c63cc53ed72a879f224ab85019db5fc2c30e8f193c1147975d46e3f5d913a']

# Malware

Name
------

EvilMinIO
-----------

# Vulnerability

**Name**

CVE-2023-28434

**Name**

CVE-2023-28432

# Attack-Pattern

## Name

T1100

## ID

T1100

## Name

Endpoint Denial of Service

## ID

T1499

## Description

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes (Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction (Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion. (Citation: Symantec DDoS October 2014) An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the system used to provide the service. These layers include the Operating Systems (OS),

server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform DoS attacks against endpoint resources, several aspects apply to multiple methods, including IP address spoofing and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016) In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.(Citation: ArsTechnica Great Firewall of China) For attacks attempting to saturate the providing network, see [Network Denial of Service](<https://attack.mitre.org/techniques/T1498>).

**Name**

Create Account

**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**

Data from Cloud Storage

**ID**

T1530

**Description**

Adversaries may access data from improperly secured cloud storage. Many cloud service providers offer solutions for online data object storage such as Amazon S3, Azure Storage, and Google Cloud Storage. These solutions differ from other storage solutions (such as SQL or Elasticsearch) in that there is no overarching application. Data from these solutions can be retrieved directly using the cloud provider's APIs. In other cases, SaaS application providers such as Slack, Confluence, and Salesforce also provide cloud storage solutions as a peripheral use case of their platform. These cloud objects can be extracted directly from their associated application.(Citation: EA Hacked via Slack - June 2021)(Citation: SecureWorld - How Secure Is Your Slack Channel - Dec 2021)(Citation: HackerNews - 3 SaaS App Cyber Attacks - April 2022)(Citation: Dark Clouds\_Usernix\_Mulazzani\_08\_2011)

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**

Trusted Relationship

**ID**

T1199

**Description**

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network. Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) used by the other party for access to internal network systems may be compromised and used. (Citation: CISA IT Service Providers) In Office 365 environments, organizations may grant Microsoft partners or resellers delegated administrator permissions. By compromising a partner or reseller account, an adversary may be able to leverage existing delegated administrator relationships or send new delegated administrator offers to clients in order to gain administrative control over the victim tenant.(Citation: Office 365 Delegated Administration)

**Name**

Server Software Component

**ID**

T1505

**Description**

Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity\_0day\_sophos\_FW)

**Name**

Audio Capture

**ID**

T1123

**Description**

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

**Name**

Exploitation of Remote Services

**ID**

T1210

**Description**

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. 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. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources. There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169) Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

**Name**

Input Capture

**ID**

T1056

**Description**

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

**Name**

Inhibit System Recovery

**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**

Remote System Discovery

**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**

Exploit Public-Facing Application

**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**

Ingress Tool Transfer

**ID**

T1105

**Description**

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](<https://attack.mitre.org/software/S0095>). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](<https://attack.mitre.org/techniques/T1570>)). Files can also be transferred using various [Web Service](<https://attack.mitre.org/techniques/T1102>)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as ``copy``, ``finger``, [certutil](<https://attack.mitre.org/software/S0160>), and [PowerShell](<https://attack.mitre.org/techniques/T1059/001>) commands such as ``IEX(New-Object Net.WebClient).downloadString()`` and ``Invoke-WebRequest``. On Linux and macOS systems, a variety of utilities also exist, such as ``curl``, ``scp``, ``sftp``, ``tftp``, ``rsync``, ``finger``, and ``wget``. (Citation: t1105\_lolbas)

**Name**

Network Service Discovery

**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**

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**

Drive-by Compromise

**ID**

T1189

**Description**

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: \* A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting \* Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary \* Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) \* Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute,

typically searching versions of the browser and plugins for a potentially vulnerable version. \* The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. \* In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

**Name**

Remote Services

**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**

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**

System Information Discovery

**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)

# StixFile

## Value

6b46cf38c45ad81dfcbbd77a1b196c5dea147088f6dab1b1920a508d61bb03ed

d4cf68e351992fc32021c75820f7d2a858796dd9dc245b7fbbf2cef8656081b2

eadde565b44e35608447b056761ba172b608b796418ab1244607dc17d21f05e3

0e084eb83954a090d83730b157f20549cf90b9d0206f5fd0bbcff009788eeafd

9698d561de233038cf922b0de4a0bbb8e5723c800b4bc04c7ac82d92cb715dfd

ffa85e27836fd556a06660ac0ad76a35ef02687652a81194821c538e847d58f

9e1a2a068af2524d2abc48c1edf46de8cfa3329d3688164db5969bc1914377fc

2d77062fb28bb7a299dcb8fa4ed62503d19ea6b8bd14e4f7ec78c54b9d08f052

b14a23d0d77a45f4df4889b0c2d239fb118f9d16f944571a8b4d08603d16fb41

1ef7419804e401fbb3860862c2b2fbc1ec3c4650fe24fb44f787f81acf6ad65b

d56c63cc53ed72a879f224ab85019db5fc2c30e8f193c1147975d46e3f5d913a

fc7909c24b2bb7f42648c605deacb3ae4f9574b95a562dd165e5e9aca2cc7d74

# External References

- 
- <https://otx.alienvault.com/pulse/64f8a28ed26db043a3a49b8f>
- 
- <https://www.securityjoes.com/post/new-attack-vector-in-the-cloud-attackers-caught-exploiting-object-storage-services>