Jun 10 2023

NETMANAGEIT

Intelligence Report

#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

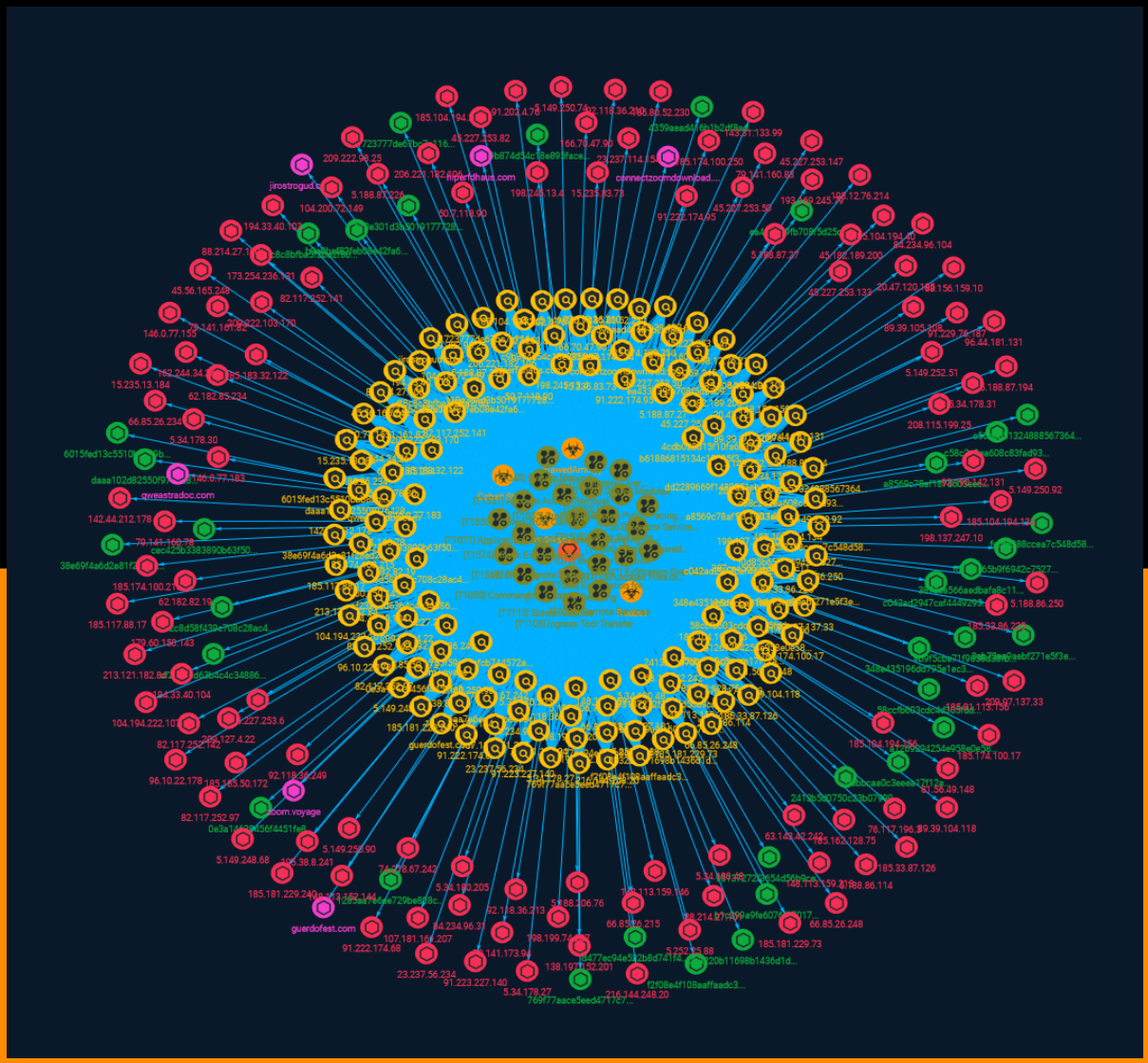

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The FBI and the US National Security Agency (CISA) have issued a joint cybersecurity advisory, warning about the threat posed by ransomware and other cyber-threats, including this year's #StopRansomware on CL0P ransomware gang.

Confidence

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

15 / 100

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name

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

Name

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto

their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Proxy

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

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel

itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry]

(https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

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

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

Exfiltration Over Other Network Medium

ID

T1011

Description

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to

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

Name

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

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

Account Access Removal

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

Event Triggered Execution

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

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

Shared Modules

ID

T1129

Description

Adversaries may execute malicious payloads via loading shared modules. The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in NTDLL.dll and is part of the Windows [Native API](https://attack.mitre.org/techniques/T1106) which is called from functions like `CreateProcess`, `LoadLibrary`, etc. of the Win32 API.(Citation: Wikipedia Windows Library Files) The module loader can load DLLs: * via specification of the (fully-qualified or relative) DLL pathname in the IMPORT directory; * via EXPORT forwarded to another DLL, specified with (fully-qualified or relative) pathname (but without extension); * via an NTFS junction or symlink program.exe.local with the fully-qualified or relative pathname of a directory containing the DLLs specified in the IMPORT

directory or forwarded EXPORTs; * via `<file name="filename.extension" loadFrom="fully-qualified or relative pathname">` in an embedded or external "application manifest". The file name refers to an entry in the IMPORT directory or a forwarded EXPORT. Adversaries may use this functionality as a way to execute arbitrary payloads on a victim system. For example, malware may execute share modules to load additional components or features.

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

Remote Service Session Hijacking

ID

T1563

Description

Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service. Adversaries may commandeer these sessions to carry out actions on remote systems. [Remote Service Session Hijacking](https://attack.mitre.org/techniques/T1563) differs from use of [Remote Services](https://attack.mitre.org/techniques/T1021) because it hijacks an existing session rather than creating a new

session using [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: RDP Hijacking Medium)(Citation: Breach Post-mortem SSH Hijack)

Name

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Name

System Network Connections Discovery

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

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Indicator

Name
5.188.87.27
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.188.87.27']
Name
148.113.159.146
Pattern Type
stix
Pattern
[ipv4-addr:value = '148.113.159.146']
Name
185.183.32.122

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.183.32.122']

Name

a8569c78af187d603eecdc5faec860458919349eef51091893b705f466340ecd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8569c78af187d603eecdc5faec860458919349eef51091893b705f466340ecd']

Name

7d5f59ae3cfcb744572ab2242e3da49640113aaf

Description

Detects the LEMURLOOT ASP.NET scripts

Pattern Type

yara

Pattern

rule M_Webshell_LEMURLOOT_1 { meta: disclaimer = "This rule is meant for hunting and is not tested to run in a production environment" description = "Detects the LEMURLOOT ASP.NET scripts" md5 = "b69e23cd45c8ac71652737ef44e15a34" sample = "cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45x" date = "2023/06/01" version = "1" strings: $head = "<%@ Page" $s1 = "X-siLock-Comment" $s2 = "X-siLock-Step" $s3 = "Health Check Service" $s4 = /pass, \"[a-z0-9]{8}-[a-z0-9]{4}/ $s5 = "attachment;filename={0}" condition: filesize > 5KB and filesize < 10KB and (($head in (0..50) and 2 of ($s*)) or (3 of ($s*))) }

Name

15.235.83.73

Pattern Type

stix

Pattern

[ipv4-addr:value = '15.235.83.73']

Name

2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5']

Name

cec425b3383890b63f5022054c396f6d510fae436041add935cd6ce42033f621

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cec425b3383890b63f5022054c396f6d510fae436041add935cd6ce42033f621']

Name

b61886815134c10105f35b6a45d77150f5f90a7f

Description

Detects indicators of compromise in MOVEit Transfer exploitation.

Pattern Type

yara

Pattern

rule MOVEit_Transfer_exploit_webshell_aspx { meta: date = "2023-06-01" description = "Detects indicators of compromise in MOVEit Transfer exploitation." author = "Ahmet Payaslioglu - Binalyze DFIR Lab" hash1 = "44d8e68c7c4e04ed3adacb5a88450552" hash2 = "a85299f78ab5dd05e7f0f11ecea165ea" reference1 = "https://www.reddit.com/r/msp/comments/13xjs1y/tracking_emerging_moveit_transfer_critical/" reference2 = "https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/" reference3 = "https://gist.github.com/JohnHammond/44ce8556f798b7f6a7574148b679c643" verdict = "dangerous" mitre = "T1505.003" platform = "windows" search_context = "filesystem" strings: $a1 = "MOVEit.DMZ" $a2 = "Request.Headers[\"X-siLock-Comment\"]" $a3 = "Delete FROM users WHERE RealName='Health Check Service'" $a4 = "set[\"Username\"]" $a5 = "INSERT INTO users (Username, LoginName, InstID, Permission, RealName" $a6 =

"Encryption.OpenFileForDecryption(dataFilePath, siGlobs.FileSystemFactory.Create()" $a7 = "Response.StatusCode = 404;" condition: filesize < 10KB and all of them }

Name

92.118.36.213

Description

ISP: Alviva Holding Limited **OS:** None ---------- Hostnames: - qweastradoc.com ---------- Domains: - qweastradoc.com ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 27 Jan 2023 15:38:38 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 213 Connection: keep-alive Vary: Accept-Encoding ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sat, 04 Feb 2023 00:17:10 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 213 Connection: keep-alive Vary: Accept-Encoding ``` HEARTBLEED: 2023/02/04 00:18:55 92.118.36.213:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.118.36.213']

Name

82.117.252.141

Pattern Type

stix

Pattern

[ipv4-addr:value = '82.117.252.141']

Name
c042ad2947caf4449295a51f9d640d722b5a6ec6957523ebf68cddb87ef3545c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c042ad2947caf4449295a51f9d640d722b5a6ec6957523ebf68cddb87ef3545c']
Name
45.227.253.6
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.227.253.6']
Name
91.222.174.95
Pattern Type
stix
Pattern

[ipv4-addr:value = '91.222.174.95']

Name

5.34.180.48

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.34.180.48']

Name

62.182.85.234

Pattern Type

stix

Pattern

[ipv4-addr:value = '62.182.85.234']

Name

208.115.199.25

Pattern Type

stix

Pattern

[ipv4-addr:value = '208.115.199.25']

Name

74.218.67.242

Pattern Type

stix

Pattern

[ipv4-addr:value = '74.218.67.242']

Name

50.7.118.90

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.7.118.90']

Name

185.104.194.156

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.104.194.156']

Name

2c8d58f439c708c28ac4ad4a0e9f93046cf076fc6e5ab1088e8943c0909acbc4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2c8d58f439c708c28ac4ad4a0e9f93046cf076fc6e5ab1088e8943c0909acbc4']

Name

45.227.253.133

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.227.253.133']

Name

5.188.206.76

Description

ISP: KREZ 999 EOOD **OS:** Debian ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7 Key type: ssh-rsa Key:

AAAAB3NzaC1yc2EAAAADAQABAAABAQDoygGzKBR8GALTBBhsA/uRBO4f0G7zmHOphKxy1MHkJhUAJ2UUP4uER7O7mFsP1u0dnau+aEug8cngirlcsdsEMvM7SZXXz6giCPZZW4vs3KT/ADzVy7oPPXPl8teyZ/ppCA2HSEm44tAI4fZM4wpuRG3yKowcy9R9l8sffclzhtP2jxNparuSwKdn/8n+Xcyf32b/scNytjUN/2f8g7OqjXIiLbJtgWzS97p9euDONQHzWGz/jVml8LfKQ8uFEnEyFsE7CuVu50UNbPzCZta+eTqu0w84H+OYzBt+IOAQhVDIn53riNbdp8gb3IKfrXqcADLEIDVoIaSZ+6au7cEr Fingerprint: c0:a6:29:2f:31:ac:31:5b:ce:d8:2c:05:47:d0:f0:e0 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.188.206.76']

Name

209.222.103.170

Description

CC=US ASN=AS23470 RELIABLESITE

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.222.103.170']

Name

198.137.247.10

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.137.247.10']

Name

92.118.36.249

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.118.36.249']

Name

23.237.114.154

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.237.114.154']

Name

63.143.42.242

Pattern Type

stix

Pattern

[ipv4-addr:value = '63.143.42.242']

Name

146.0.77.183

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.0.77.183']

Name

dd2289669f1488351eb455d3650b2e051a453a5f

Description

Detects indicators of compromise in MOVEit Transfer exploitation.

Pattern Type

yara

Pattern

rule MOVEit_Transfer_exploit_webshell_dll { meta: date = "2023-06-01" description = "Detects indicators of compromise in MOVEit Transfer exploitation." author = "Djordje Lukic - Binalyze DFIR Lab" hash1 = "7d7349e51a9bdcdd8b5daeeefe6772b5" hash2 = "2387be2afe2250c20d4e7a8c185be8d9" reference1 = "https://www.reddit.com/r/msp/comments/13xjs1y/tracking_emerging_moveit_transfer_critical/" reference2 = "https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/" reference3 = "https://gist.github.com/JohnHammond/44ce8556f798b7f6a7574148b679c643" verdict = "dangerous" mitre = "T1505.003" platform = "windows" search_context = "filesystem" strings: $a1 = "human2.aspx" wide $a2 = "Delete FROM users WHERE RealName='Health Check Service'" wide $a3 = "X-siLock-Comment" wide condition: uint16(0) == 0x5A4D and filesize < 20KB and all of them }

Name

1285aa7e6ee729be808c46c069e30a9ee9ce34287151076ba81a0bea0508ff7e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1285aa7e6ee729be808c46c069e30a9ee9ce34287151076ba81a0bea0508ff7e']

Name

110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286']

Name

348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d']

Name

209.127.4.22

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.127.4.22']

Name

45.227.253.50

Pattern Type
stix
Pattern
[ipv4-addr:value = '45.227.253.50']
Name
88.214.27.101
Pattern Type
stix
Pattern
[ipv4-addr:value = '88.214.27.101']
Name
79.141.161.82
Pattern Type
stix
Pattern
[ipv4-addr:value = '79.141.161.82']
Name
93.190.142.131

Pattern Type
stix
Pattern
[ipv4-addr:value = '93.190.142.131']
Name
5.149.250.90
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.149.250.90']
Name
198.245.13.4
Pattern Type
stix
Pattern
[ipv4-addr:value = '198.245.13.4']
Name
d5bbcaa0c3eeea17f12a5cc3dbcaffff423d00562acb694561841bcfe984a3b7

Description

_7_Zip_Installer

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd5bbcaa0c3eeea17f12a5cc3dbcaffff423d00562acb694561841bcfe984a3b7']

Name

62.182.82.19

Description

ISP: Virtual Systems LLC **OS:** Ubuntu ---------- Hostnames: - host19.v-sys.org ---------- Domains: - v-sys.org ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQD5sdWmZUX7Qil4niRczdSUX3WBj6OvHEDRO/aD8jmjRWcHYVlN455arxmbE4de+7PfYVgERDrrZfkdSxuqebV4bgsyUlwRuzt07p0GySN+OGW+zMlE4dfAUe/Q8upMah6wqwG2hAdMrV8WcPH1jqM5F7LPhWYcaXHvHbU8y79UaEhdtve6coO8U1lsDpkM5YEQ4IhNGQ1ts1mjC948y2O9YIhESYJWwNxZ+YHLN+k+ZbVvNlEiwF/b83XklfkiLA1WJZjRTDfAxAvnLvk5NNALp5w82XaCfwlyVIiavRFsblr+CT/MxMlJjg6gKuSs7Wkrt21kHLYxIJ+F40zv958j19Wp5zk1Rs1AYp08nvlNOY1XF/1a9k5fZJONmxZqPlabGPM3pvSnsmMnJFn2+1obnKMwDqYBKi41XqgLgARiLXaWrBBYppeYQY4qHxj5jhW40LffL2UnxxJRKRxNcRBDLrGx7tbhDlHp+2nDj246mVWhWgicK7kgP5d0cInz790= Fingerprint: af:dd:f1:45:e6:69:04:22:78:48:6c:14:02:a2:12:72 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com

umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '62.182.82.19']

Name

89.39.105.108

Description

CC=NL ASN=AS49981 WorldStream B.V.

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.39.105.108']

Name

198.199.74.207

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.199.74.207']

Name

b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad']

Name

387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a

Description

SHA256 of 44d8e68c7c4e04ed3adacb5a88450552

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a']

Name

zoom.voyage

Pattern Type

stix

Pattern

[domain-name:value = 'zoom.voyage']

Name

connectzoomdownload.com

Pattern Type

stix

Pattern

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

Name

93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db']

Name
5.34.178.30
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.34.178.30']
Name
5.149.252.51
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.149.252.51']
Name
5.34.180.205
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.34.180.205']

Name

hiperfdhaus.com

Description

TrueBot

Pattern Type

stix

Pattern

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

Name

58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166']

Name

cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45

Description

SHA256 of b69e23cd45c8ac71652737ef44e15a34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45']

Name

ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a']

Name

66.85.26.215

Pattern Type

stix

Pattern

[ipv4-addr:value = '66.85.26.215']

Name
173.254.236.131
Pattern Type
stix
Pattern
[ipv4-addr:value = '173.254.236.131']
Name
185.104.194.134
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.104.194.134']
Name
195.38.8.241
Pattern Type
stix
Pattern
[ipv4-addr:value = '195.38.8.241']

Name
166.70.47.90
Pattern Type
stix
Pattern
[ipv4-addr:value = '166.70.47.90']
Name
185.162.128.75
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.162.128.75']
Name
qweastradoc.com
Pattern Type
stix
Pattern
[domain-name:value = 'qweastradoc.com']

Name
20.47.120.195
Pattern Type
stix
Pattern
[ipv4-addr:value = '20.47.120.195']
Name
84.234.96.31
Pattern Type
stix
Pattern
[ipv4-addr:value = '84.234.96.31']
Name
5.188.87.226
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.188.87.226']

Name

eb9f5cbe71f9658d38fb4a7aa101ad40534c4c93ee73ef5f6886d89159b0e2c2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eb9f5cbe71f9658d38fb4a7aa101ad40534c4c93ee73ef5f6886d89159b0e2c2']

Name

194.33.40.104

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.33.40.104']

Name

79.141.160.83

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.141.160.83']

Name

b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272']

Name

162.244.34.26

Pattern Type

stix

Pattern

[ipv4-addr:value = '162.244.34.26']

Name

5.34.178.31

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.34.178.31']

Name

107.181.161.207

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.181.161.207']

Name

45.227.253.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.227.253.82']

Name

81.56.49.148

Pattern Type

stix

Pattern

[ipv4-addr:value = '81.56.49.148']

Name

179.60.150.143

Pattern Type

stix

Pattern

[ipv4-addr:value = '179.60.150.143']

Name

45.182.189.200

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.182.189.200']

Name

d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899']

Name

ff8c8c8bfba5f2ba2f8003255949678df209dbff95e16f2f3c338cfa0fd1b885

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ff8c8c8bfba5f2ba2f8003255949678df209dbff95e16f2f3c338cfa0fd1b885']

Name

f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d']

Name

0e3a14638456f4451fe8d76fdc04e591fba942c2f16da31857ca66293a58a4c3

Description

dbgdetect_procs

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e3a14638456f4451fe8d76fdc04e591fba942c2f16da31857ca66293a58a4c3']

Name

185.174.100.250

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.174.100.250']

Name

148.113.159.213

Pattern Type

stix

Pattern

[ipv4-addr:value = '148.113.159.213']

Name

daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4']

Name

68.156.159.10

Pattern Type

stix

Pattern

[ipv4-addr:value = '68.156.159.10']

Name

79.141.173.94

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.141.173.94']

Name
206.221.182.106
Pattern Type
stix
Pattern
[ipv4-addr:value = '206.221.182.106']
Name
185.81.113.156
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.81.113.156']
Name
213.121.182.84
Pattern Type
stix
Pattern
[ipv4-addr:value = '213.121.182.84']

Name
193.169.245.79
Pattern Type
stix
Pattern
[ipv4-addr:value = '193.169.245.79']
Name
5.252.25.88
Description
CC=DE ASN=AS202422 G-Core Labs S.A.
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.252.25.88']
Name
146.0.77.155
Pattern Type
stix

Pattern

[ipv4-addr:value = '146.0.77.155']

Name

c58c2c2ea608c83fad9326055a8271d47d8246dc9cb401e420c0971c67e19cbf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c58c2c2ea608c83fad9326055a8271d47d8246dc9cb401e420c0971c67e19cbf']

Name

148.113.152.144

Description

CC=CA ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '148.113.152.144']

Name

c9b874d54c18e895face055eeb6faa2da7965a336d70303d0bd6047bec27a29d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c9b874d54c18e895face055eeb6faa2da7965a336d70303d0bd6047bec27a29d']

Name

76.117.196.3

Pattern Type

stix

Pattern

[ipv4-addr:value = '76.117.196.3']

Name

79.141.160.78

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.141.160.78']

Name

185.104.194.40

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.104.194.40']

Name

138.197.152.201

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC7MK7ZGMFUS/DuvrLJoXk7nFRS2uSjoW5es5Z56RGtDuA5 KL3MKq2btnH9X5xJH81EAEvwSsU78RKAFbibD5l9Z4/T6dsv+BbNGmRnCyr6SGo9X1uMO2sq9fcp +y5kAgRu7ZaSlSz5lDAMlZbqDbsgqPCxmJ2XpcPdlQdnmezoeFt3N1/P6OyMv+66kLjWadk1aGZz 7Ip5euQX/Djcpi30lD3I82WfxMqveSFvZJ6UtMf1v7PmVdjOluSTMzHyYq4Z+kHaz2naAqbg8mO2 mHpcRmDsDYxbikax6aJ6PN+uKFB/k/tx0NMZe9D6HHjiBNk9ucAmn1y7t50Wu8NKaIdt Fingerprint: 00:52:53:52:fe:3f:ee:f7:ed:66:35:a0:ad:c6:68:be Kex Algorithms: diffie-hellman-group1-sha1 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 31 Jan 2023 05:07:00 GMT Server: Apache/2.4.29 (Ubuntu) Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, OPTIONS Vary: Cookie,Accept-Encoding Set-Cookie:

sessionid=7f8pabhljrwwa022y6fbs6uzbdfdh9os; httponly; Path=/ Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '138.197.152.201']

Name

104.200.72.149

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.200.72.149']

Name

185.33.86.225

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.33.86.225']

Name
185.185.50.172
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.185.50.172']
Name
4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf']
Name
185.181.229.73
Pattern Type
stix
Pattern

[ipv4-addr:value = '185.181.229.73']

Name

66.85.26.234

Pattern Type

stix

Pattern

[ipv4-addr:value = '66.85.26.234']

Name

5.188.87.194

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.188.87.194']

Name

91.222.174.68

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.222.174.68']

Name

9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead']

Name

a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7']

Name

185.117.88.17

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.117.88.17']

Name

198.12.76.214

Description

CC=US ASN=AS36352 AS-COLOCROSSING

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.12.76.214']

Name

216.144.248.20

Pattern Type

stix

Pattern

[ipv4-addr:value = '216.144.248.20']

Name

88.214.27.100

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.214.27.100']

Name

fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f

Description

SHA256 of a85299f78ab5dd05e7f0f11ecea165ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f']

Name

5.149.248.68

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.149.248.68']

Name

92.118.36.210

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.118.36.210']

Name

5.188.86.114

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.188.86.114']

Name

142.44.212.178

Pattern Type

stix

Pattern

[ipv4-addr:value = '142.44.212.178']

Name

96.44.181.131

Pattern Type

stix

Pattern

[ipv4-addr:value = '96.44.181.131']

Name

91.223.227.140

Description

404 NOT FOUND

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.223.227.140']

Name

209.222.98.25

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.222.98.25']

Name

209.97.137.33

Description

CC=GB ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.97.137.33']

Name

82.117.252.142

Pattern Type

stix

Pattern

[ipv4-addr:value = '82.117.252.142']

Name

143.31.133.99

Pattern Type

stix

Pattern

[ipv4-addr:value = '143.31.133.99']

Name

0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9']

Name

15.235.13.184

Pattern Type

stix

Pattern

[ipv4-addr:value = '15.235.13.184']

Name
c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4']
Name
guerdofest.com
Pattern Type
stix
Pattern
[domain-name:value = 'guerdofest.com']
Name
91.202.4.76
Pattern Type
stix
Pattern

[ipv4-addr:value = '91.202.4.76']

Name

89.39.104.118

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.39.104.118']

Name

185.174.100.215

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.174.100.215']

Name

4cdb028d15f10fa6b37db1c90e2a1bda1797919d

Description

Detects the compiled DLLs generated from human2.aspx LEMURLOOT payloads.

Pattern Type

yara

Pattern

rule M_Webshell_LEMURLOOT_DLL_1 { meta: disclaimer = "This rule is meant for hunting and is not tested to run in a production environment" description = "Detects the compiled DLLs generated from human2.aspx LEMURLOOT payloads." sample = "c58c2c2ea608c83fad9326055a8271d47d8246dc9cb401e420c0971c67e19cbf" date = "2023/06/01" version = "1" strings: $net = "ASP.NET" $human = "Create_ASP_human2_aspx" $s1 = "X-siLock-Comment" wide $s2 = "X-siLock-Step3" wide $s3 = "X-siLock-Step2" wide $s4 = "Health Check Service" wide $s5 = "attachment; filename={0}" wide condition: uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and filesize < 15KB and $net and (($human and 2 of ($s*)) or (3 of ($s*))) }

Name

769f77aace5eed4717c7d3142989b53bd5bac9297a6e11b2c588c3989b397e6b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '769f77aace5eed4717c7d3142989b53bd5bac9297a6e11b2c588c3989b397e6b']

Name

194.33.40.103

Pattern Type

stix

Pattern

```
[ipv4-addr:value = '194.33.40.103']
```

Domain-Name

Value
hiperfdhaus.com
zoom.voyage
connectzoomdownload.com
jirostrogud.com
guerdofest.com
qweastradoc.com

StixFile

Value
c58c2c2ea608c83fad9326055a8271d47d8246dc9cb401e420c0971c67e19cbf
f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d
c042ad2947caf4449295a51f9d640d722b5a6ec6957523ebf68cddb87ef3545c
2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d
769f77aace5eed4717c7d3142989b53bd5bac9297a6e11b2c588c3989b397e6b
0e3a14638456f4451fe8d76fdc04e591fba942c2f16da31857ca66293a58a4c3
b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272
fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f
eb9f5cbe71f9658d38fb4a7aa101ad40534c4c93ee73ef5f6886d89159b0e2c2
387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a
4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf
3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409

c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4

b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad

cec425b3383890b63f5022054c396f6d510fae436041add935cd6ce42033f621

c9b874d54c18e895face055eeb6faa2da7965a336d70303d0bd6047bec27a29d

cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45

ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a

f2f08e4f108aaffaadc3d11bad24abdd625a77e0ee9674c4541b562c78415765

d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899

a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7

58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166

1285aa7e6ee729be808c46c069e30a9ee9ce34287151076ba81a0bea0508ff7e

110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286

2c8d58f439c708c28ac4ad4a0e9f93046cf076fc6e5ab1088e8943c0909acbc4

0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9

93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db

d5bbcaa0c3eeea17f12a5cc3dbcaffff423d00562acb694561841bcfe984a3b7

a8569c78af187d603eecdc5faec860458919349eef51091893b705f466340ecd

ff8c8c8bfba5f2ba2f8003255949678df209dbff95e16f2f3c338cfa0fd1b885

9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead

6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d

38e69f4a6d2e81f28ed2dc6df0daf31e73ea365bd2cfc90ebc31441404cca264

daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4

External References

- https://otx.alienvault.com/pulse/648107945daaa56965c6b5f1
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a