Sep 25 2023

NETMANAGEIT

Intelligence Report

From ScreenConnect to Hive Ransomware in 61 hours

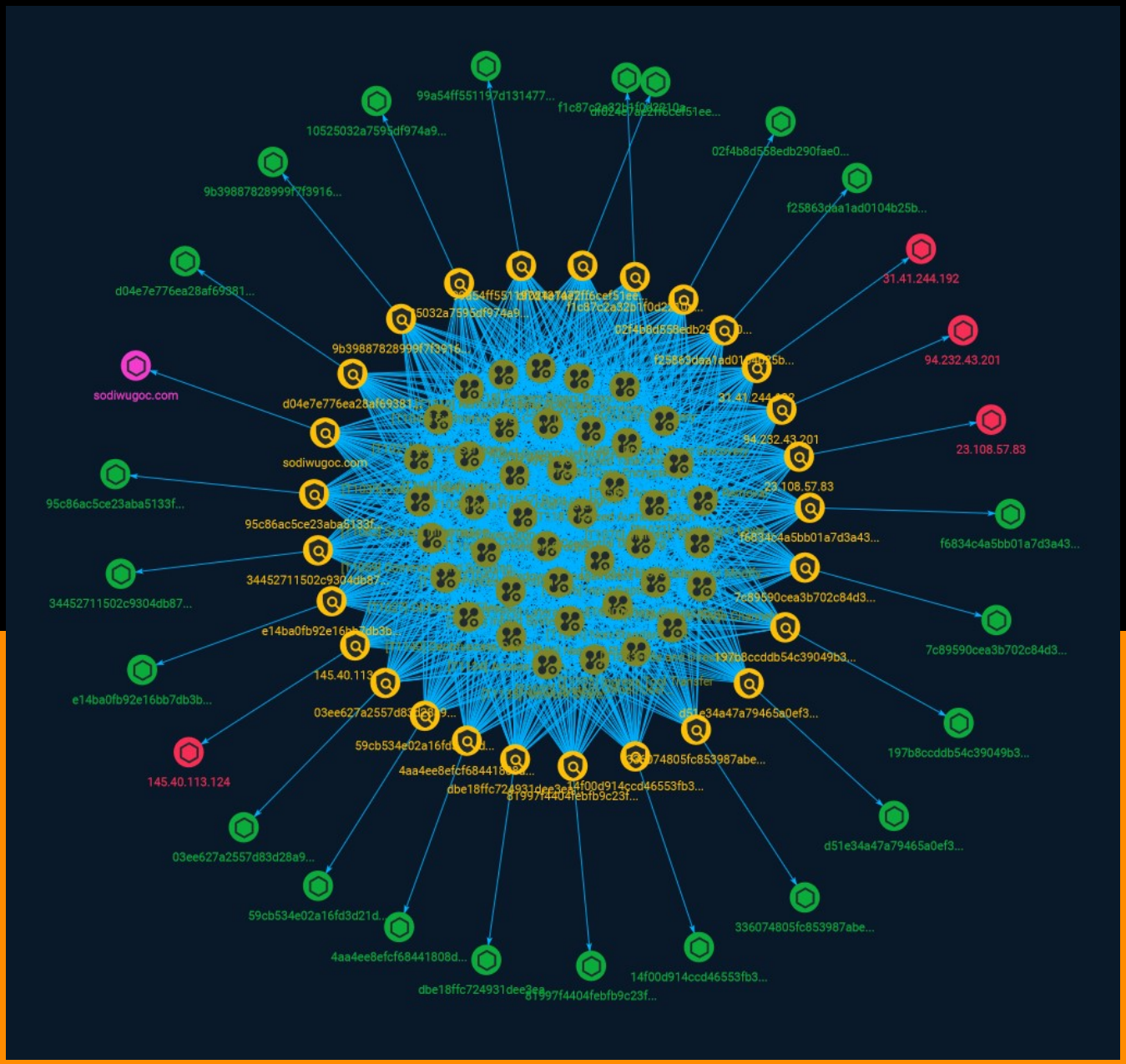

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In 2022, The DFIR Report observed an increase in the adversarial usage of Remote Management and Monitoring (RMM) tools. When compared to post-exploitation channels that heavily rely on terminals, such as Cobalt Strike or Metasploit, the graphical user interface provided by RMMs are more user friendly. With the popularity of SaaS (Software as a Service) models, many RMMs are further offered as cloud-based services. By having command & control channels rely on legitimate cloud services, adversaries make attribution and disruption more complex. Utilizing RMMs could also hinder detection (i.e. trusted domains & signed executables).

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
Windows Management Instrumentation
ID
T1047
Description
Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform

environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) (WinRM).(Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: MSDN WMI)(Citation: FireEye WMI 2015) An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

Input Capture

ID

T1056

Description

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

Name

Permission Groups Discovery

ID

T1069

Description

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

Name

Forced Authentication

ID

T1187

Description

Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept. The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. (Citation: Wikipedia Server Message Block) This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources. Web Distributed Authoring and Versioning (WebDAV) is also typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443. (Citation: Didier Stevens WebDAV Traffic) (Citation: Microsoft Managing WebDAV Security) Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB/WebDAV authentication. An adversary can send an attachment to a user through spearphishing that contains a resource link to an external server controlled by the adversary (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)), or place a specially crafted file on navigation path for privileged accounts (e.g. .SCF file placed on desktop) or on a publicly accessible share to be accessed by victim(s). When the user's system accesses the untrusted resource it will attempt authentication and send information, including the user's hashed credentials, over SMB to the adversary controlled server. (Citation: GitHub Hashjacking) With access to the credential hash, an adversary can perform off-line [Brute Force](https://attack.mitre.org/techniques/T1110) cracking to gain access to plaintext credentials. (Citation: Cylance Redirect to SMB) There are several different ways this can occur. (Citation: Osanda Stealing NetNTLM Hashes) Some specifics from in-the-wild use include: * A spearphishing attachment containing a document with a resource that is automatically loaded when the document is opened (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)). The document can include, for example, a request similar to `file[:]//[remote address]/Normal.dotm` to trigger the SMB request. (Citation: US-CERT APT Energy Oct 2017) * A modified .LNK or .SCF file with the icon filename pointing to an external reference such as `\\[remote address]\pic.png` that will force the system to load the resource when the icon is rendered to repeatedly gather credentials. (Citation: US-CERT APT Energy Oct 2017)

Name

Lateral Tool Transfer

ID

T1570

Description

Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e. [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation. Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) to connected network shares or with authenticated connections via [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001).(Citation: Unit42 LockerGoga 2019) Files can also be transferred using native or otherwise present tools on the victim system, such as scp, rsync, curl, sftp, and [ftp](https://attack.mitre.org/software/S0095).

Name

BITS Jobs

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

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

Scheduled Task/Job

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

Non-Standard Port

ID

T1571

Description

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data. Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change_rdp_port_conti)

Name

Exfiltration Over Alternative Protocol

ID

T1048

Description

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels. [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048) can be done using various common operating system utilities such as [Net](https://attack.mitre.org/software/S0039)/SMB or FTP.(Citation: Palo Alto OilRig Oct 2016) On macOS and Linux `curl` may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.(Citation: 20 macOS Common Tools and Techniques) Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive

information via the web console or [Cloud API](https://attack.mitre.org/techniques/T1059/009).

Name

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

Inhibit System Recovery

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery

options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

Name

System Network Configuration Discovery

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

Data Obfuscation

ID

T1001

Description

Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) 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). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Data Encrypted for Impact

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

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations. (Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with

native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

Name

Data from Local System

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Name

Create or Modify System Process

ID

T1543

Description

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

Name

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

System Services

ID

T1569

Description

Adversaries may abuse system services or daemons to execute commands or programs. Adversaries can execute malicious content by interacting with or creating services either locally or remotely. Many services are set to run at boot, which can aid in achieving persistence ([Create or Modify System Process](https://attack.mitre.org/techniques/T1543)), but adversaries can also abuse services for one-time or temporary execution.

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

Data from Network Shared Drive

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

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

Access Token Manipulation

ID

T1134

Description

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator

account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

Name

Remote Access Software

ID

T1219

Description

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, AnyDesk, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries.(Citation: Symantec Living off the Land) Remote access tools may be installed and used post-compromise as 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. Installation of many remote access tools may also include persistence (ex: the tool's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)). Admin tools such as TeamViewer have been used by several groups targeting institutions in countries of interest to the Russian state and criminal campaigns.(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy)

Name

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

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

Account Discovery

ID

T1087

Description

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

Name

System Owner/User Discovery

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

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

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Name

File and Directory Discovery

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

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather

detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

Domain Trust Discovery

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

Network Share Discovery

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.

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

e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c

Description

Delphi SHA256 of 39300863bcaad71e5d4efc9a1cae118440aa778f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c']

Name

02f4b8d558edb290fae03b8f1a7b412e988eab3738d11edb7d59890c784edb68

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '02f4b8d558edb290fae03b8f1a7b412e988eab3738d11edb7d59890c784edb68']

Name

14f00d914ccd46553fb30933fbe691e22e5197ad6a32bc076ba19935ebb7e5aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '14f00d914ccd46553fb30933fbe691e22e5197ad6a32bc076ba19935ebb7e5aa']

Name

d04e7e776ea28af69381e346a1bf86be5f5e4715003f7048783e7d1f049b1bd2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd04e7e776ea28af69381e346a1bf86be5f5e4715003f7048783e7d1f049b1bd2']

Name

23.108.57.83

Description

ISP: Leaseweb USA, Inc. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDTMh0tPqaLKJiMWBcOodgs5razgr4yqil5ujSzXTA0Jj9O19qwLFTNdrduGWFO9rIez69uEAF8LHdHM5RBP5fv5XVxNzTIjP8DfmxZhDL+chs7ridxX5pFFObiXOHCqfaeMjqHQhnECn3DZvJdbLK7Cz7CKPHn1FhkM3raswN+Ue8zgbNhbncZpvaslRcI9/a1clLo5qXuH0HOEFnw5JkQtRo5RGAoyrtmOQ2okh56OL6t087qBEgs6ixPdGDtPVJyTwPehC7ktyJzcMoHI8wx7cc2XnbsU6n0KFyfaezFJ9jJB2jZXRtum8Az+7Segv4RAcE8kCC7gW9bS3KiuZDX Fingerprint: b8:f4:62:e2:e2:66:48:7d:f4:b2:08:31:c6:f5:c5:cf 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 = '23.108.57.83']

Name

59cb534e02a16fd3d21d1ba5d34ee15e665d7a955751171249563d1192aa33e4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '59cb534e02a16fd3d21d1ba5d34ee15e665d7a955751171249563d1192aa33e4']

Name

df024e7ae2ff6cef51ee80d30f10f94233a5ddd62da22ecf3c6ab3ebc293264b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df024e7ae2ff6cef51ee80d30f10f94233a5ddd62da22ecf3c6ab3ebc293264b']

Name

d51e34a47a79465a0ef3916fe01fe667e8e4281ef3b676569e6a1a33419e51ea

Description

SHA256 of 21ef9f0a078dbc4e4c45be12f1cfaf8a3864dfa7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd51e34a47a79465a0ef3916fe01fe667e8e4281ef3b676569e6a1a33419e51ea']

Name

95c86ac5ce23aba5133f61ca0d2d637f74105fa05e88d232141f057a1df7dd8b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '95c86ac5ce23aba5133f61ca0d2d637f74105fa05e88d232141f057a1df7dd8b']

Name

31.41.244.192

Description

CC=RU ASN=AS57678 Cat Technologies Co. Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.41.244.192']

Name

dbe18ffc724931dee3ea99c75c9b4ea8e27b228e19508211689cc7c3249680d3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dbe18ffc724931dee3ea99c75c9b4ea8e27b228e19508211689cc7c3249680d3']

Name

10525032a7595df974a9649042acab0fda5c1e5a59297ad1709bbf463adb2e50

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10525032a7595df974a9649042acab0fda5c1e5a59297ad1709bbf463adb2e50']

Name

7c89590cea3b702c84d3b1a566705067d4bde1b97ecd160d553ff1380e0ef5a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c89590cea3b702c84d3b1a566705067d4bde1b97ecd160d553ff1380e0ef5a6']

Name

145.40.113.124

Description
CC=GB ASN=AS54825 PACKET
Pattern Type
stix
Pattern
[ipv4-addr:value = '145.40.113.124']
Name
f1c87c2a32b1f0d2210a12ebcb1d3146b54e3bb5db3fb97dbd81fe123d411632
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f1c87c2a32b1f0d2210a12ebcb1d3146b54e3bb5db3fb97dbd81fe123d411632']
Name
336074805fc853987abe6f7fe3ad97a6a6f3077a16391fec744f671a015fbd7e
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '336074805fc853987abe6f7fe3ad97a6a6f3077a16391fec744f671a015fbd7e']

Name

sodiwugoc.com

Pattern Type

stix

Pattern

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

Name

94.232.43.201

Description

ISP: XHOST INTERNET SOLUTIONS LP **OS:** Windows Server 2012 R2 (build 6.3.9600) ---------- Hostnames: ---------- Domains: ---------- Services: **135:** ``` Microsoft RPC Endpoint Mapper d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 94.232.43.201:1025 ncalrpc: WindowsShutdown ncacn_np: \\WIN-344VU98D3RU\PIPE\InitShutdown ncalrpc: WMsgKRpc08B2C0 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-344VU98D3RU\PIPE\InitShutdown ncalrpc: WMsgKRpc08B2C0 ncalrpc: WMsgKRpc08D531 ncalrpc: WMsgKRpc0E0A8E2 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-2a1bfa30232abbefab ncacn_np: \ \WIN-344VU98D3RU\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f2ebe85bcd8ea95873 ncalrpc: actkernel ncalrpc: umpo 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-2a1bfa30232abbefab ncacn_np: \ \WIN-344VU98D3RU\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f2ebe85bcd8ea95873 ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-f2ebe85bcd8ea95873 ncalrpc: actkernel ncalrpc: umpo ncacn_np: \

\WIN-344VU98D3RU\PIPE\srvsvc ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: actkernel ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: LRPC-c73c216fb8a451c076 ncacn_ip_tcp: 94.232.43.201:1026 ncacn_np: \\WIN-344VU98D3RU\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncalrpc: LRPC-c73c216fb8a451c076 ncacn_ip_tcp: 94.232.43.201:1026 ncacn_np: \
\WIN-344VU98D3RU\pipe\eventlog ncalrpc: eventlog abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: LRPC-c73c216fb8a451c076 ncacn_ip_tcp: 94.232.43.201:1026 ncacn_np: \
\WIN-344VU98D3RU\pipe\eventlog ncalrpc: eventlog 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-c73c216fb8a451c076 ncacn_ip_tcp: 94.232.43.201:1026 ncacn_np: \\WIN-344VU98D3RU\pipe\eventlog ncalrpc: eventlog f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 94.232.43.201:1026 ncacn_np: \
\WIN-344VU98D3RU\pipe\eventlog ncalrpc: eventlog 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-96e630b18ab712aca0 ncacn_np: \\WIN-344VU98D3RU\PIPE\srvsvc ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncacn_np: \
\WIN-344VU98D3RU\PIPE\srvsvc ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncacn_np: \\WIN-344VU98D3RU\PIPE\srvsvc ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server

endpoint ncacn_np: \\WIN-344VU98D3RU\PIPE\srvsvc ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncacn_np: \\WIN-344VU98D3RU\PIPE\srvsvc ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 94.232.43.201:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \ \WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: senssvc ncalrpc: OLE69701E990DC332FE0A178820C07E ncalrpc: IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-774565f74c10a88b8c b2507c30-b126-494a-92ac-ee32b6eeb039 version: v1.0 ncalrpc: LRPC-724ab8b01ddaaaf182 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncacn_np: \\WIN-344VU98D3RU\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT ncalrpc: LRPC-27bf7a2dfb544cd7c8 ncalrpc: OLEA890A90A8FD6583F41B60E2F4BA3 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-27bf7a2dfb544cd7c8 ncalrpc:

OLEA890A90A8FD6583F41B60E2F4BA3 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-64c0a2c4cf695e277c ncalrpc: LRPC-8d01945f096e6164e4 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-64c0a2c4cf695e277c ncalrpc: LRPC-8d01945f096e6164e4 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-64c0a2c4cf695e277c ncalrpc: LRPC-8d01945f096e6164e4 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-8d01945f096e6164e4 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-344VU98D3RU\PIPE\wkssvc ncalrpc: LRPC-c046e52e879f2431ac ncalrpc: DNSResolver eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-c046e52e879f2431ac ncalrpc: DNSResolver f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-c046e52e879f2431ac ncalrpc: DNSResolver 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 94.232.43.201:1028 ncalrpc: LRPC-df09f064bef8eafc2a 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 94.232.43.201:1028 ncalrpc: LRPC-df09f064bef8eafc2a ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 94.232.43.201:1028 ncalrpc: LRPC-df09f064bef8eafc2a 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 94.232.43.201:1028 ncalrpc: LRPC-df09f064bef8eafc2a 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 94.232.43.201:1028 ncalrpc: LRPC-df09f064bef8eafc2a 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 94.232.43.201:1029 6b5bdd1e-528c-422c-af8c-a4079be4fe48 version: v1.0 annotation: Remote Fw APIs protocol: [MS-FASP]: Firewall and Advanced Security Protocol provider: FwRemoteSvr.dll ncacn_ip_tcp: 94.232.43.201:1030 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 94.232.43.201:1034 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-344VU98D3RU\pipe\lsass 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0E0A8E2 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-cfc27752c3ab01a5dd ncalrpc: LRPC-cfc27752c3ab01a5dd ncalrpc: LRPC-cfc27752c3ab01a5dd ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 1 OS: Windows Server 2012 R2 Standard 9600 Software: Windows Server 2012 R2 Standard 6.3 Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode ``` ---------- **3389:** ``` Remote Desktop Protocol NTLM Info: OS: Windows 8.1/

Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-344VU98D3RU NetBIOS Domain Name: WIN-344VU98D3RU NetBIOS Computer Name: WIN-344VU98D3RU DNS Domain Name: WIN-344VU98D3RU FQDN: WIN-344VU98D3RU am Windows Server 2012R2 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 25 Sep 2023 02:08:44 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-344VU98D3RU NetBIOS Domain Name: WIN-344VU98D3RU NetBIOS Computer Name: WIN-344VU98D3RU DNS Domain Name: WIN-344VU98D3RU FQDN: WIN-344VU98D3RU ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.232.43.201']

Name

4aa4ee8efcf68441808d0055c26a24e5b8f32de89c6a7a0d9b742cce588213ed

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4aa4ee8efcf68441808d0055c26a24e5b8f32de89c6a7a0d9b742cce588213ed']

Name

99a54ff551197d131477152d3d27e38787ca949ffdbb041f15752767efe1e645

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99a54ff551197d131477152d3d27e38787ca949ffdbb041f15752767efe1e645']

Name

197b8ccddb54c39049b308a9a5037dc7bf7d3689bdc759504f3c36d483beb9d3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '197b8ccddb54c39049b308a9a5037dc7bf7d3689bdc759504f3c36d483beb9d3']

Name

34452711502c9304db8745510f96aa644481162c389f591147327f54d4ae3727

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '34452711502c9304db8745510f96aa644481162c389f591147327f54d4ae3727']

Name

f25863daa1ad0104b25b91581f7b1cc4f65ca63ff4d1bb956ecd3f9350e365a5

Description

Cabinet_Archive SHA256 of 1dd933817806728380fd1aee46d9f8d42251ea7f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f25863daa1ad0104b25b91581f7b1cc4f65ca63ff4d1bb956ecd3f9350e365a5']

Name

81997f4404febfb9c23f2f3939934513d499593750b4a4826c32878e05b83f30

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '81997f4404febfb9c23f2f3939934513d499593750b4a4826c32878e05b83f30']

Name

9b39887828999f7f3916262574c46b835d38f200fcd3c07c2bbe9a83c9f935a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9b39887828999f7f3916262574c46b835d38f200fcd3c07c2bbe9a83c9f935a9']

Name

f6834c4a5bb01a7d3a43b11a4792f8149714e4d1b271810f79772e50b6395615

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6834c4a5bb01a7d3a43b11a4792f8149714e4d1b271810f79772e50b6395615']

Name

03ee627a2557d83d28a90857678966709ec24582434a5d2f0653012b088276d1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '03ee627a2557d83d28a90857678966709ec24582434a5d2f0653012b088276d1']

Domain-Name

Value
sodiwugoc.com

StixFile

Value
dbe18ffc724931dee3ea99c75c9b4ea8e27b228e19508211689cc7c3249680d3
95c86ac5ce23aba5133f61ca0d2d637f74105fa05e88d232141f057a1df7dd8b
df024e7ae2ff6cef51ee80d30f10f94233a5ddd62da22ecf3c6ab3ebc293264b
f6834c4a5bb01a7d3a43b11a4792f8149714e4d1b271810f79772e50b6395615
81997f4404febfb9c23f2f3939934513d499593750b4a4826c32878e05b83f30
02f4b8d558edb290fae03b8f1a7b412e988eab3738d11edb7d59890c784edb68
d51e34a47a79465a0ef3916fe01fe667e8e4281ef3b676569e6a1a33419e51ea
59cb534e02a16fd3d21d1ba5d34ee15e665d7a955751171249563d1192aa33e4
4aa4ee8efcf68441808d0055c26a24e5b8f32de89c6a7a0d9b742cce588213ed
10525032a7595df974a9649042acab0fda5c1e5a59297ad1709bbf463adb2e50
99a54ff551197d131477152d3d27e38787ca949ffdbb041f15752767efe1e645
7c89590cea3b702c84d3b1a566705067d4bde1b97ecd160d553ff1380e0ef5a6
d04e7e776ea28af69381e346a1bf86be5f5e4715003f7048783e7d1f049b1bd2

14f00d914ccd46553fb30933fbe691e22e5197ad6a32bc076ba19935ebb7e5aa

f1c87c2a32b1f0d2210a12ebcb1d3146b54e3bb5db3fb97dbd81fe123d411632

34452711502c9304db8745510f96aa644481162c389f591147327f54d4ae3727

197b8ccddb54c39049b308a9a5037dc7bf7d3689bdc759504f3c36d483beb9d3

e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c

03ee627a2557d83d28a90857678966709ec24582434a5d2f0653012b088276d1

9b39887828999f7f3916262574c46b835d38f200fcd3c07c2bbe9a83c9f935a9

f25863daa1ad0104b25b91581f7b1cc4f65ca63ff4d1bb956ecd3f9350e365a5

336074805fc853987abe6f7fe3ad97a6a6f3077a16391fec744f671a015fbd7e

IPv4-Addr

Value
31.41.244.192
145.40.113.124
23.108.57.83
94.232.43.201

External References

- https://otx.alienvault.com/pulse/6511e0f479ad8c13d57d2253
- https://thedfirreport.com/2023/09/25/from-screenconnect-to-hive-ransomware-in-61-hours/