Jan 19 2024

NETMANAGEIT

Intelligence Report

Detailed Analysis of DarkGate; Investigating new top-trend backdoor malware

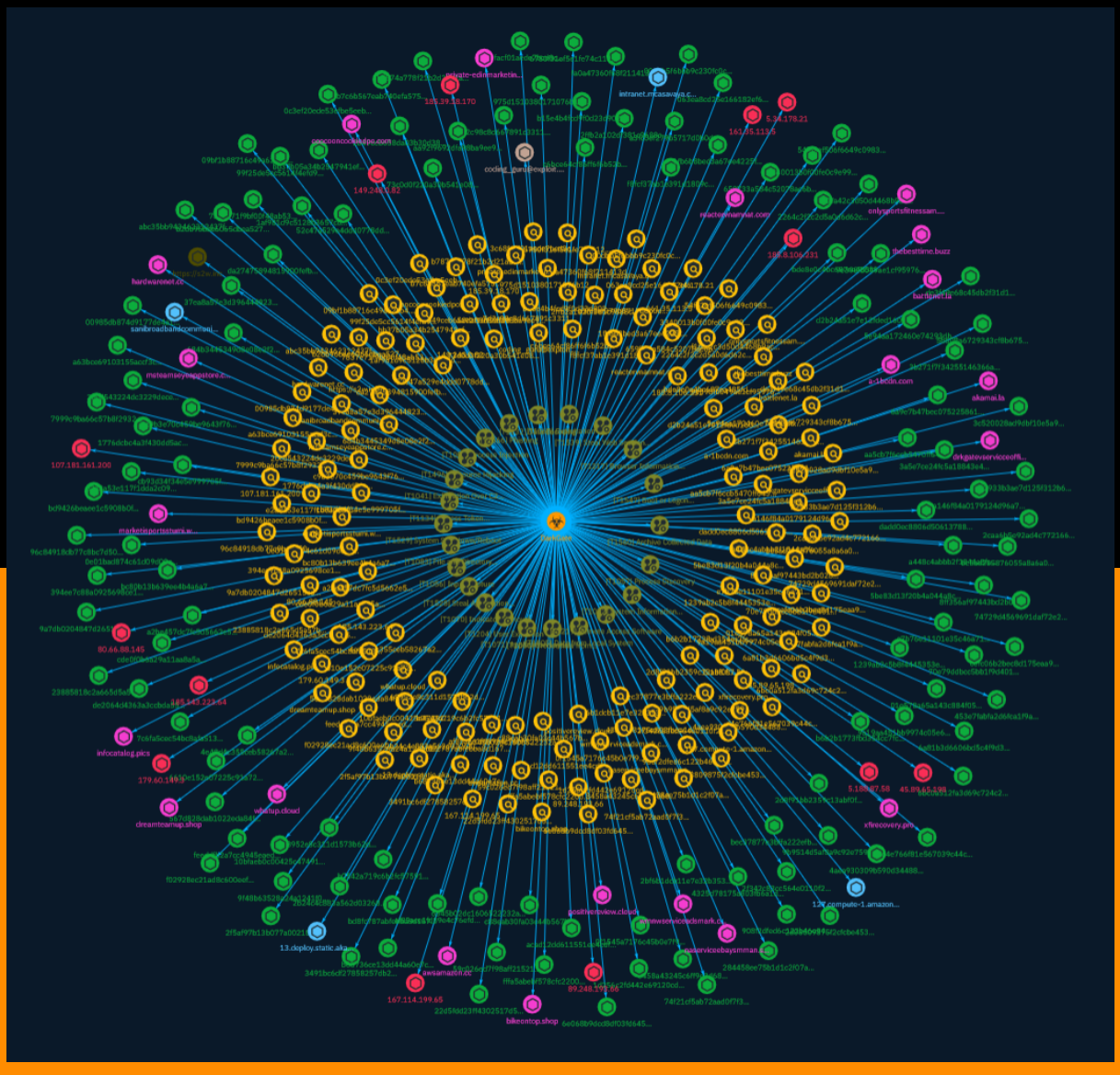

Table of contents

Overview

Entities

Observables

External References

Overview

Description

DarkGate is a malware that has been developed since 2017 and sold as Malware-as-a-Service. The blog looks into the malware, analysing its capabilities and how it has regained popularity due to its loader and botnet capabilities.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Process Discovery

ID

T1057

Description

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

Name

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

Steal Application Access Token

ID

T1528

Description

Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources. Application access tokens are used to make authorized API requests on behalf of a user or service and are commonly used as a way to access resources in cloud and container-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019) OAuth is one commonly implemented framework that issues tokens to users for access to systems. Adversaries who steal account API tokens in cloud and containerized environments may be able to access data and perform actions with the permissions of these accounts, which can lead to privilege escalation and further compromise of the environment. In Kubernetes environments, processes running inside a container communicate with the Kubernetes API server using service account tokens. If a container is compromised, an attacker may be able to steal the container’s token and thereby gain access to Kubernetes API commands.(Citation: Kubernetes Service Accounts) Token theft can also occur through social engineering, in which case user action may be required to grant access. An application desiring access to cloud-based services or protected APIs can gain entry using OAuth 2.0 through a variety of authorization protocols. An example commonly-used sequence is Microsoft's Authorization Code Grant flow.(Citation: Microsoft Identity Platform Protocols May 2019)(Citation: Microsoft - OAuth Code Authorization flow - June 2019) An OAuth access token enables a third-party application to interact with resources containing user data in the ways requested by the application without obtaining user credentials. Adversaries can leverage OAuth authorization by constructing a malicious application designed to be granted access to resources with the target user's OAuth token. (Citation: Amnesty OAuth Phishing Attacks, August 2019)(Citation: Trend Micro Pawn Storm OAuth 2017) The adversary will need to complete registration of their application with the authorization server, for example Microsoft Identity Platform using Azure Portal, the Visual Studio IDE, the command-line interface, PowerShell, or REST API calls.(Citation: Microsoft - Azure AD App Registration - May 2019) Then, they can send a [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) to the target user to entice them to grant access to the application. Once the OAuth access token is granted, the application can gain potentially long-term access to features of the user account through [Application Access Token](https://attack.mitre.org/techniques/T1550/001).(Citation: Microsoft - Azure AD Identity Tokens - Aug 2019) Application access tokens may function within a limited lifetime, limiting how long an adversary can utilize the stolen token. However, in some

cases, adversaries can also steal application refresh tokens(Citation: Auth0 Understanding Refresh Tokens), allowing them to obtain new access tokens without prompting the user.

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

Browser Information Discovery

ID

T1217

Description

Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking

sites, relationships/interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.(Citation: Kaspersky Autofill) Browser information may also highlight additional targets after an adversary has access to valid credentials, especially [Credentials In Files](https://attack.mitre.org/techniques/T1552/001) associated with logins cached by a browser. Specific storage locations vary based on platform and/or application, but browser information is typically stored in local files and databases (e.g., `%APPDATA%/Google/Chrome`).(Citation: Chrome Roaming Profiles)

Name

Indicator Removal

ID

T1070

Description

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

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Credentials from Password Stores

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are

obtained, they can be used to perform lateral movement and access restricted information.

Name

Exploitation for Privilege Escalation

ID

T1068

Description

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

Name

Data Encoding

ID

T1132

Description

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

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

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR) Alternatively, they may engage in proxyjacking by selling use of the victims' network bandwidth and IP address to proxyware services.(Citation: Sysdig Proxyjacking)

Name

Archive Collected Data

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Name

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

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 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

System Shutdown/Reboot

ID

T1529

Description

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device via [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) (e.g. `reload`).(Citation: Microsoft Shutdown Oct 2017)(Citation: alert_TA18_106A) Shutting down or rebooting systems may disrupt access to computer resources for legitimate users while also impeding incident response/recovery. Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) or [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490), to hasten the intended effects on system availability.(Citation: Talos Nyetya June 2017)(Citation: Talos Olympic Destroyer 2018)

Name

Steal Web Session Cookie

ID

T1539

Description

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website. Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.(Citation: Pass The Cookie) There are several examples of malware targeting cookies from web browsers on the local system.(Citation: Kaspersky TajMahal April 2019)(Citation: Unit 42 Mac Crypto Cookies January 2019) There are also open source frameworks such as `Evilginx2` and `Muraena` that can gather session cookies through a malicious proxy (ex: [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)) that can be set up by an adversary and used in phishing campaigns.(Citation: Github evilginx2)(Citation: GitHub Mauraena) After an adversary acquires a valid cookie, they can then perform a [Web Session Cookie] (https://attack.mitre.org/techniques/T1550/004) technique to login to the corresponding web application.

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

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

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

3b271f7f34255146366ab7c7d916fa5ab3b1accfc4b0f3d727e16690cfb7ad3a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3b271f7f34255146366ab7c7d916fa5ab3b1accfc4b0f3d727e16690cfb7ad3a']

Name

bd8fc787abfebba8d167e9979c2ec692f861ab21ea138c3381daa852a58677be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd8fc787abfebba8d167e9979c2ec692f861ab21ea138c3381daa852a58677be']

Name

hardwarenet.cc

Pattern Type

stix

Pattern

[domain-name:value = 'hardwarenet.cc']

Name

whatup.cloud

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'whatup.cloud']

Name

1af981d9c5128b3657cdb5506d61563e0d1908b957e5dd6842059d6d3cfdc622

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1af981d9c5128b3657cdb5506d61563e0d1908b957e5dd6842059d6d3cfdc622']

Name

74729d4569691daf72e23849e91461471411f551639663e11e1091a48790611e

Description

#LowFiCheckAVFolders

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '74729d4569691daf72e23849e91461471411f551639663e11e1091a48790611e']

Name

bec37877e3bffa222efb5c5680c7defd2d917317293d7fa70e0882ad45290a40

Description

VirTool:Win32/DelfInject.gen!CP

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bec37877e3bffa222efb5c5680c7defd2d917317293d7fa70e0882ad45290a40']

Name

37ea8a57e3d3964448238aff31125381c7063b98e1fe0d83a20b315b70546c94

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '37ea8a57e3d3964448238aff31125381c7063b98e1fe0d83a20b315b70546c94']

Name

drkgatevservicceoffice.net

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'drkgatevservicceoffice.net']

Name
107.181.161.200
Description
DarkGate botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '107.181.161.200']
Name
bde8e0c4bc687ea485fd4a00c86bd25ab14a04edf9b2bbc03808e9b86074717b
Description
Cabinet_Archive
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'bde8e0c4bc687ea485fd4a00c86bd25ab14a04edf9b2bbc03808e9b86074717b']
Name

89.248.193.66

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.248.193.66']

Name

6750f31ef5e1fe74c1121b0ab1308f93e09505a63322b6ce16fe04099ce8993e

Description

#LowFiCheckAVFolders

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6750f31ef5e1fe74c1121b0ab1308f93e09505a63322b6ce16fe04099ce8993e']

Name

bc5ad215876055a8a6a097579e16d24e233a323a6157afbb6db49705ac12a1f1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bc5ad215876055a8a6a097579e16d24e233a323a6157afbb6db49705ac12a1f1']

Name

4e48d4c355ceb58267a29fd3337b101722c805a7e53662816b73ce9b756ae321

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4e48d4c355ceb58267a29fd3337b101722c805a7e53662816b73ce9b756ae321']

Name

3340013b0f00fe0c9e99411f722f8f3f0baf9ae4f40ac78796a6d4d694b46d7b

Description

Trojan:Win32/Casdet!rfn

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3340013b0f00fe0c9e99411f722f8f3f0baf9ae4f40ac78796a6d4d694b46d7b']

Name

3491bc6df27858257db26b913da8c35c83a0e48cf80de701a45a30a30544706d

Description

Trojan:VBS/Donvibs

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3491bc6df27858257db26b913da8c35c83a0e48cf80de701a45a30a30544706d']

Name

20cd543224dc3229dece35f018678a52fc98e533596e4995a5534bde0e7e161f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '20cd543224dc3229dece35f018678a52fc98e533596e4995a5534bde0e7e161f']

Name

659733a584c52078ac6b568dfb34a089bef2b3835a5ea737d32c1623a468b743

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '659733a584c52078ac6b568dfb34a089bef2b3835a5ea737d32c1623a468b743']

Name

awsamazon.cc

Pattern Type

stix

Pattern

[domain-name:value = 'awsamazon.cc']

Name

aa92f9692dfa98ba9ee991156612f2015c10a5ecf02b605b0b6d528827430601

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa92f9692dfa98ba9ee991156612f2015c10a5ecf02b605b0b6d528827430601']

Name

6a9e7b47bec075225861d61cf20555c38a17b7b9ff46ff85de7f6791c548cc2e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a9e7b47bec075225861d61cf20555c38a17b7b9ff46ff85de7f6791c548cc2e']

Name

coocooncookiedpo.com

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

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

Name

a-1bcdn.com

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'a-1bcdn.com']

Name

9a19aa451bb9974c05e616bf02762ee001cc02669aca15150199415e5e190f01

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a19aa451bb9974c05e616bf02762ee001cc02669aca15150199415e5e190f01']

Name

00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df

Description

#LowFiCheckAVFolders

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df']

Name

3c520028ad9dbf10e5a94023fbbd5ca7134802a6def3fae427f70620c12f8988

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c520028ad9dbf10e5a94023fbbd5ca7134802a6def3fae427f70620c12f8988']

Name

b0542a719c6b2fc575915e9e4c58920cf999ba5c3f5345617818a9dc14a378b4

Description

Trojan:VBS/Donvibs

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b0542a719c6b2fc575915e9e4c58920cf999ba5c3f5345617818a9dc14a378b4']

Name

0e01bad874c61d09d09ce06f76f5e46f6648a1fc943644874c8e1a53a93af9a7

Description

W32/Injector

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e01bad874c61d09d09ce06f76f5e46f6648a1fc943644874c8e1a53a93af9a7']

Name

5be83d13f20b4a044a8c8281d13723a808555cdd73a7ddcec37422a4e44fbd4e

Description

DarkGate

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5be83d13f20b4a044a8c8281d13723a808555cdd73a7ddcec37422a4e44fbd4e']

Name

marketisportsstumi.win

Description

Remcos botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'marketisportsstumi.win']

Name

a146f84a0179124d96a707f192f4c06c07690e745cffaef521fcda9633766a44

Description

Trojan:VBS/Donvibs

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a146f84a0179124d96a707f192f4c06c07690e745cffaef521fcda9633766a44']

Name

908f2dfed6c122b46e946fe8839feb9218cb095f180f86c43659448e2f709fc7

Description

Trojan:VBS/Donvibs

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '908f2dfed6c122b46e946fe8839feb9218cb095f180f86c43659448e2f709fc7']

Name

99f25de5cc5614f4efd967db0dae50f20e2acbae9e98920aff3d98638b9ca1f1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99f25de5cc5614f4efd967db0dae50f20e2acbae9e98920aff3d98638b9ca1f1']

Name

5.188.87.58

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.188.87.58']

Name

feeddfb2a7cc4945eaedd8f75907c42ff097252c3e38d7ef2006bd7a191f09ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'feeddfb2a7cc4945eaedd8f75907c42ff097252c3e38d7ef2006bd7a191f09ae']

Name

onlysportsfitnessam.com

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

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

Name

bikeontop.shop

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'bikeontop.shop']

Name

b2db96bae6065dbea52711c6f732a29bd39cbb4e81dde9e7d854d52cfb1970f0

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b2db96bae6065dbea52711c6f732a29bd39cbb4e81dde9e7d854d52cfb1970f0']

Name

msteamseyeappstore.com

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

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

Name

acad12dd611551ee4cdfd9fba7dd06c1f6a7c4d8cd8619cbbafa3d8f88bde910

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'acad12dd611551ee4cdfd9fba7dd06c1f6a7c4d8cd8619cbbafa3d8f88bde910']

Name

intranet.mcasavaya.com

Pattern Type

stix

Pattern

[hostname:value = 'intranet.mcasavaya.com']

Name

d4e766f81e567039c44ccca90ef192a7f063c1783224ee4be3e3d7786980e236

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd4e766f81e567039c44ccca90ef192a7f063c1783224ee4be3e3d7786980e236']

Name

cde0f0b6a29a11aa8a5a4ee543fd632cb460bc11927c7153c1f5f8664e474d23

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cde0f0b6a29a11aa8a5a4ee543fd632cb460bc11927c7153c1f5f8664e474d23']

Name

c6bce64cf86ff6f6b52b9ffa8b8dc2283645b9f0cea7391117d5dd80c2092ce6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c6bce64cf86ff6f6b52b9ffa8b8dc2283645b9f0cea7391117d5dd80c2092ce6']

Name

0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2

Description

#LowFiCheckAVFolders

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2']

Name

1776dcbc4a3f430dd5ace833aac80b0954a050e5a7dec164b53b62fbe72feab3

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1776dcbc4a3f430dd5ace833aac80b0954a050e5a7dec164b53b62fbe72feab3']

Name

3a5e7ce24fc5a18843e4f877f5c704bf95eb90c039bc8d791273c191e4ca3242

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3a5e7ce24fc5a18843e4f877f5c704bf95eb90c039bc8d791273c191e4ca3242']

Name

f02928ec21ad8c600eef3e3a006581a3af858975cbc2ad29ba3dfdd1a78d3cb9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f02928ec21ad8c600eef3e3a006581a3af858975cbc2ad29ba3dfdd1a78d3cb9']

Name

b7874a778f21b2d21a2a2ab2c2ec4a7ae5042443e1d3f20a070424d628079056

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b7874a778f21b2d21a2a2ab2c2ec4a7ae5042443e1d3f20a070424d628079056']

Name

battlenet.la

Pattern Type

stix

Pattern

[domain-name:value = 'battlenet.la']

Name

de2064d4363a3ccbda5518c619f1c803393b0876e349530583a72b1d1643c16a

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de2064d4363a3ccbda5518c619f1c803393b0876e349530583a72b1d1643c16a']

Name

coding_guru@exploit.im

Pattern Type

stix

Pattern

[email-addr:value = 'coding_guru@exploit.im']

Name

8458a43245c6ff9e3d688a8393f692d3088bf5338ae810ff78b8b3a1d751a87e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8458a43245c6ff9e3d688a8393f692d3088bf5338ae810ff78b8b3a1d751a87e']

Name

09bf1b88716c49a62cb4ff708f7ff4f09cb7c3ff42e58661802cd66f1a2a0311

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '09bf1b88716c49a62cb4ff708f7ff4f09cb7c3ff42e58661802cd66f1a2a0311']

Name

1239ab2c5b8f4445353eacba276938c9cce9711a643851db8979728defc5a3ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1239ab2c5b8f4445353eacba276938c9cce9711a643851db8979728defc5a3ee']

Name

2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084']

Name

f8fcf37ab1e391d1809c4b5baf00d669c4263682d99230432c5199bde5914a60

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f8fcf37ab1e391d1809c4b5baf00d669c4263682d99230432c5199bde5914a60']

Name

453e7fabfa2d6fca1f9a5b9edc456e46417d8fb76332d397a39fcc8e76ccf54f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '453e7fabfa2d6fca1f9a5b9edc456e46417d8fb76332d397a39fcc8e76ccf54f']

Name

a2be457dc7fc5d5662e5db1b51b77094898449fedab7b1a9f837c093c249c5ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a2be457dc7fc5d5662e5db1b51b77094898449fedab7b1a9f837c093c249c5ba']

Name

9e398fb049ae1cf95976ba1c80280cb3f78833569fe7fc5c1ba93c7e57c00fac

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9e398fb049ae1cf95976ba1c80280cb3f78833569fe7fc5c1ba93c7e57c00fac']

Name

567d828dab1022eda84f90592d6d95e331e0f2696e79ed7d86ddc095bb2efdc8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '567d828dab1022eda84f90592d6d95e331e0f2696e79ed7d86ddc095bb2efdc8']

Name

b7c6b567eab740efa575826c94f4c9c552ed5894b8b3ef57e77959b740d8bec8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b7c6b567eab740efa575826c94f4c9c552ed5894b8b3ef57e77959b740d8bec8']

Name

2caa6b5e92ad4c772166860d428d388a4fa376c5adc439b10ee2f045e0a1b003

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2caa6b5e92ad4c772166860d428d388a4fa376c5adc439b10ee2f045e0a1b003']

Name

bd9426beaee1c5908b0f71b31539ae4fe3ffed155ab00041b543d48fda3f1654

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd9426beaee1c5908b0f71b31539ae4fe3ffed155ab00041b543d48fda3f1654']

Name

54f52ef506f6649c09838b9935aed223f0f320798e13fdb9541ffd1db3e08816

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '54f52ef506f6649c09838b9935aed223f0f320798e13fdb9541ffd1db3e08816']

Name

2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4

Description

#LowFiCheckAVFolders

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4']

Name

684b3445349d8e08e2f2d33f3b30d509a3fde82cb798ccbad2726105301a9470

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '684b3445349d8e08e2f2d33f3b30d509a3fde82cb798ccbad2726105301a9470']

Name

dadd0ec8806d506137889d7f1595b3b5447c1ea30159432b1952fa9551ecfba5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dadd0ec8806d506137889d7f1595b3b5447c1ea30159432b1952fa9551ecfba5']

Name

45.89.65.198

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.89.65.198']

Name

2b49ceb658da03b30d38ee2dc46bcf2bb85af728cece29f8c30d7c1a92c1ad09

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b49ceb658da03b30d38ee2dc46bcf2bb85af728cece29f8c30d7c1a92c1ad09']

Name

6345b02dc1606522232ac853a0e2599d166aef91ae1d7f4d4104d184273dc1e8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6345b02dc1606522232ac853a0e2599d166aef91ae1d7f4d4104d184273dc1e8']

Name

80.66.88.145

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.88.145']

Name

de3f49e68c45db2f31d1cc1d10ff09f8cfce302b92a1f5361c8f34c3d78544e5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de3f49e68c45db2f31d1cc1d10ff09f8cfce302b92a1f5361c8f34c3d78544e5']

Name

1d256c2fd442e69120cdf8d12d7bd865f058ec667e2119a66259fc9052dbaa36

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1d256c2fd442e69120cdf8d12d7bd865f058ec667e2119a66259fc9052dbaa36']

Name

3c68facf01aede7bcd8c2aea853324a2e6a0ec8b026d95c7f50a46d77334c2d2

Description

Other:Malware-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c68facf01aede7bcd8c2aea853324a2e6a0ec8b026d95c7f50a46d77334c2d2']

Name

aa5cb7f6ccb5470ff643cfcba9254263c9db9e7a84984d30166cc14945e219f2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa5cb7f6ccb5470ff643cfcba9254263c9db9e7a84984d30166cc14945e219f2']

Name

9f48b63528a24a1241f0bc793e960d420314d595c9927e2294f4475c4be143cd

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f48b63528a24a1241f0bc793e960d420314d595c9927e2294f4475c4be143cd']

Name

c9b3e70c459be9643f764afd535976f9d308d098e1476013de431e7aea22b3e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c9b3e70c459be9643f764afd535976f9d308d098e1476013de431e7aea22b3e9']

Name

b6b2b1773fbd354cc7fcf409f4b4208e570be077658c2a92ea59319c250d9f8c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b6b2b1773fbd354cc7fcf409f4b4208e570be077658c2a92ea59319c250d9f8c']

Name

infocatalog.pics

Pattern Type

stix

Pattern

[domain-name:value = 'infocatalog.pics']

Name

01e578a65a143c884f054c96574f2f9e203b49f47ebf74a0749ff484866b2eb7

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01e578a65a143c884f054c96574f2f9e203b49f47ebf74a0749ff484866b2eb7']

Name

185.143.223.64

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.143.223.64']

Name

2ffb2a102df381c9688cc78c2cba4faa6a561d5aa78a9163888ebf7c73bdc8d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ffb2a102df381c9688cc78c2cba4faa6a561d5aa78a9163888ebf7c73bdc8d0']

Name

4aea930309b590d34488187a8c9cb31b83ff1faa2ff4d27606e50fac3a0db742

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4aea930309b590d34488187a8c9cb31b83ff1faa2ff4d27606e50fac3a0db742']

Name

cb93d34f34e5e999705fd5d17d6725b452c57bc799fc835899e4af9330f4169f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cb93d34f34e5e999705fd5d17d6725b452c57bc799fc835899e4af9330f4169f']

Name

1fb6b8bed3a67ee4225f852c3d90fd2b629f2541ab431b4bd4d9d9f5bbd2c4b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1fb6b8bed3a67ee4225f852c3d90fd2b629f2541ab431b4bd4d9d9f5bbd2c4b7']

Name

4325d78175a803fb6a1d235e8255816a07283501087e1b115f28c38b6b542856

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4325d78175a803fb6a1d235e8255816a07283501087e1b115f28c38b6b542856']

Name

abc35bb943462312437f0c4275b012e8ec03899ab86d353143d92cbefedd7f9d

Description

Trojan:VBS/Donvibs

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'abc35bb943462312437f0c4275b012e8ec03899ab86d353143d92cbefedd7f9d']

Name

cefc06b2bec8d175eaa9bf3f91c8246731811a8ad7b52af336478655dbc70039

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cefc06b2bec8d175eaa9bf3f91c8246731811a8ad7b52af336478655dbc70039']

Name

13.deploy.static.akamaitechnologies.pw

Pattern Type

stix

Pattern

[hostname:value = '13.deploy.static.akamaitechnologies.pw']

Name

fa0a47360f68f211413d582d2c73035594a9191c2399c52612c940b45402065f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa0a47360f68f211413d582d2c73035594a9191c2399c52612c940b45402065f']

Name

59c026ed7f98aff21521b7a76845821aa5f1ce1a978d1c90404c073bd6310a1d

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '59c026ed7f98aff21521b7a76845821aa5f1ce1a978d1c90404c073bd6310a1d']

Name

23885818c2a665d5a57ba16acfe46db68258da619a8db3df8f069c0205ac648e

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23885818c2a665d5a57ba16acfe46db68258da619a8db3df8f069c0205ac648e']

Name

5.34.178.21

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.34.178.21']

Name

c88eab30fa03c44b567bcb4e659a60ee0fe5d98664816c70e3b6e8d79169cbea

Description

Trojan:Win32/Casdet!rfn

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c88eab30fa03c44b567bcb4e659a60ee0fe5d98664816c70e3b6e8d79169cbea']

Name

7837e71f9bf00f48ab5336ed8647b116471561181069b79d29dbaee0e951ded7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7837e71f9bf00f48ab5336ed8647b116471561181069b79d29dbaee0e951ded7']

Name

6a81b3d6606bd5c4f9d3484719ec35fc6d2dedb902a85553705a71a6e1273104

Description
Cabinet_Archive
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6a81b3d6606bd5c4f9d3484719ec35fc6d2dedb902a85553705a71a6e1273104']
Name
96c84918db77c8bc7d5080aca1b618f7ea7c824d27f67b2346364756f04b3226
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '96c84918db77c8bc7d5080aca1b618f7ea7c824d27f67b2346364756f04b3226']
Name
akamai.la
Pattern Type
stix
Pattern

[domain-name:value = 'akamai.la']

Name

2bf6b1dcb11e7e32b353e0c135aca9c979177d14aa9834119cd8e4c1a5b08562

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2bf6b1dcb11e7e32b353e0c135aca9c979177d14aa9834119cd8e4c1a5b08562']

Name

149.248.0.82

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '149.248.0.82']

Name

reactervnamnat.com

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

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

Name

wmnwserviceadsmark.com

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

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

Name

b15e4b4fcd9f0d23d902d91af9cc4e01417c426e55f6e0b4ad7256f72ac0231a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b15e4b4fcd9f0d23d902d91af9cc4e01417c426e55f6e0b4ad7256f72ac0231a']

Name

2d08809875f2cfcbe4538d11ee5537768beba0b7740e1785ac35fd90d32e5c25

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2d08809875f2cfcbe4538d11ee5537768beba0b7740e1785ac35fd90d32e5c25']

Name

e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243']

Name

a448c4abbb2f1844a8fa0c929cd84c2f6f57a4af0442a6a4b5307af89c35cef6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a448c4abbb2f1844a8fa0c929cd84c2f6f57a4af0442a6a4b5307af89c35cef6']

Name

af85ace1fd89e4c76efdda065cc2fc44de987bfd75f9f6850610327526c97d4b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af85ace1fd89e4c76efdda065cc2fc44de987bfd75f9f6850610327526c97d4b']

Name

9a7db0204847d26515ed249f9ed577220326f63a724a2e0fb6bb1d8cd33508a3

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a7db0204847d26515ed249f9ed577220326f63a724a2e0fb6bb1d8cd33508a3']

Name

xfirecovery.pro

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'xfirecovery.pro']

Name

167.114.199.65

Description

CC=CA ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '167.114.199.65']

Name

00dbb5f6bbb9c230fc0c7f7526b46d697850587b30d0b4f4d54106eb3a3d5410

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '00dbb5f6bbb9c230fc0c7f7526b46d697850587b30d0b4f4d54106eb3a3d5410']

Name

127.compute-1.amazonaws.cdnprivate.tel

Pattern Type

stix

Pattern

[hostname:value = '127.compute-1.amazonaws.cdnprivate.tel']

Name

https://s2w.inc

Pattern Type

stix

Pattern

[url:value = 'https://s2w.inc']

Name

22933b3ae7d125f312b6d1fe6356092cdcd1def6dca3ad128de65ba7986266ae

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22933b3ae7d125f312b6d1fe6356092cdcd1def6dca3ad128de65ba7986266ae']

Name

22d5fdd23ff4302517d5652375ee5ec3bfb28cb964015b3e9902d2398c908fd9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22d5fdd23ff4302517d5652375ee5ec3bfb28cb964015b3e9902d2398c908fd9']

Name

73c0d0f220a30b541e0855e8039b8050d1332ff03c3e0c8a35671bd5eb9d30be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '73c0d0f220a30b541e0855e8039b8050d1332ff03c3e0c8a35671bd5eb9d30be']

Name

6bc0a512fa3d69c724c2a0aaea8f915795f9c0ef68617dbd32d3b78ee5cddc06

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6bc0a512fa3d69c724c2a0aaea8f915795f9c0ef68617dbd32d3b78ee5cddc06']

Name

185.8.106.231

Description

ISP: UAB Cherry Servers **OS:** Windows Server 2022 (build 10.0.20348) ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **80:** ``` HTTP/1.1 404 Not Found Server: Microsoft-IIS/10.0 Date: Tue, 21 Nov 2023 18:49:20 GMT Content-Length: 0 ``` ----------------- **135:** ``` Microsoft RPC Endpoint Mapper 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 185.8.106.231:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\402361\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 185.8.106.231:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\402361\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 185.8.106.231:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\402361\pipe\lsass 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 185.8.106.231:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\402361\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 185.8.106.231:49665 ncalrpc: WindowsShutdown ncacn_np: \\402361\PIPE\InitShutdown ncalrpc: WMsgKRpc0DD660 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\402361\PIPE\InitShutdown ncalrpc: WMsgKRpc0DD660 ncalrpc: WMsgKRpc0DFF01 ncalrpc: WMsgKRpc05ED022 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-2d8e3c9a6e05b96825 ncalrpc: LRPC-cfa43cbde63d37c8e0 ncalrpc: LRPC-

a73a92a59b6f4b9c26 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-2d8e3c9a6e05b96825 ncalrpc: LRPC-cfa43cbde63d37c8e0 ncalrpc: LRPC-a73a92a59b6f4b9c26 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-cfa43cbde63d37c8e0 ncalrpc: LRPC-a73a92a59b6f4b9c26 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-a73a92a59b6f4b9c26 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-32b96ae0f59d4f474a ncalrpc: LRPC-6e576ac62d71f2fb56 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-2d8e3c9a6e05b96825 ncalrpc: LRPC-cfa43cbde63d37c8e0 ncalrpc: LRPC-a73a92a59b6f4b9c26 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-cfa43cbde63d37c8e0 ncalrpc: LRPC-a73a92a59b6f4b9c26 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 0d47017b-b33b-46ad-9e18-fe96456c5078 version: v1.0 ncalrpc: umpo 95406f0b-b239-4318-91bb-cea3a46ff0dc version: v1.0 ncalrpc: umpo 4ed8abcc-f1e2-438b-981f-bb0e8abc010c version: v1.0 ncalrpc: umpo 0ff1f646-13bb-400a-ab50-9a78f2b7a85a version: v1.0 ncalrpc: umpo 6982a06e-5fe2-46b1-b39c-a2c545bfa069 version: v1.0 ncalrpc: umpo 082a3471-31b6-422a-b931-a54401960c62 version: v1.0 ncalrpc: umpo fae436b0-b864-4a87-9eda-298547cd82f2 version: v1.0 ncalrpc: umpo e53d94ca-7464-4839-b044-09a2fb8b3ae5 version: v1.0 ncalrpc: umpo 178d84be-9291-4994-82c6-3f909aca5a03 version: v1.0 ncalrpc: umpo 4dace966-a243-4450-ae3f-9b7bcb5315b8 version: v2.0 ncalrpc: umpo 1832bcf6-cab8-41d4-85d2-c9410764f75a version: v1.0 ncalrpc: umpo c521facf-09a9-42c5-b155-72388595cbf0 version: v0.0 ncalrpc: umpo 2c7fd9ce-e706-4b40-b412-953107ef9bb0 version: v0.0 ncalrpc: umpo 88abcbc3-34ea-76ae-8215-767520655a23 version: v0.0 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-21f4c140d89da09cb9 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel

ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-85155c6c24703e46c6 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo dd59071b-3215-4c59-8481-972edadc0f6a version: v1.0 ncalrpc: OLE98F3E390ED4E7DF270AE7499CDD2 ncalrpc: actkernel ncalrpc: umpo 0361ae94-0316-4c6c-8ad8-c594375800e2 version: v1.0 ncalrpc: umpo 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2 version: v1.0 ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-8bf202166d39e8ccc0 ncalrpc: IUserProfile2 ncalrpc: LRPC-add7f540430a4f45eb ncalrpc: LRPC-1983125202d16c35db ncalrpc: senssvc ncalrpc: LRPC-523e7b293f0210097a f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-cc924a9c9484797c4a ncalrpc: LRPC-8fd3803e2887f9f36a e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-a9236b8f6f6d05af0e 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-62594d1a8f2ef571ca ncalrpc: OLE1D36DEA986ED7637E6CC9D669794 ncalrpc: LRPC-32b96ae0f59d4f474a 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-947c337d7d755d24eb a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-7f3dd550e8efb25779 ncalrpc: LRPC-6e576ac62d71f2fb56 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-18eb14928d13897f4c 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-56990264b5a55cc209 ncalrpc: DNSResolver f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 185.8.106.231:49666 ncacn_np: \\402361\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: dhcpcsvc 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-67ef270bbd68cdffff 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-6ef3d1c82191cfc2f1 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 185.8.106.231:49667 ncalrpc: LRPC-443a2764cf6a7250e7 ncalrpc: ubpmtaskhostchannel ncacn_np: \\402361\PIPE\atsvc ncalrpc: LRPC-f3ead2c15c808e33c3 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 185.8.106.231:49667 ncalrpc:

LRPC-443a2764cf6a7250e7 ncalrpc: ubpmtaskhostchannel ncacn_np: \\402361\PIPE\atsvc ncalrpc: LRPC-f3ead2c15c808e33c3 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-443a2764cf6a7250e7 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \402361\PIPE\atsvc ncalrpc: LRPC-f3ead2c15c808e33c3 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\402361\PIPE\atsvc ncalrpc: LRPC-f3ead2c15c808e33c3 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \ \402361\PIPE\atsvc ncalrpc: LRPC-f3ead2c15c808e33c3 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-f3ead2c15c808e33c3 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-ad00b265bf4be4d7f4 ncalrpc: OLE6C44BDF144DEF31428AB0DB80D1E 3f787932-3452-4363-8651-6ea97bb373bb version: v1.0 annotation: NSP Rpc Interface ncalrpc: LRPC-9684af15085ba2f7f7 ncalrpc: OLEC1BCF10C5D76C15297D61B6F494E 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\402361\PIPE\wkssvc ncalrpc: LRPC-bff0f1d900b646fb02 eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-bff0f1d900b646fb02 f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-bff0f1d900b646fb02 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 185.8.106.231:49668 ncacn_np: \\402361\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-523e7b293f0210097a 13560fa9-8c09-4b56-a1fd-04d083b9b2a1 version: v1.0 ncalrpc: LRPC-7d69fc07dc7921e3d6 ncalrpc: OLE78D11F70AABEA68C2F28366A4C65 c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-7d69fc07dc7921e3d6 ncalrpc: OLE78D11F70AABEA68C2F28366A4C65 f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-7d69fc07dc7921e3d6 ncalrpc: OLE78D11F70AABEA68C2F28366A4C65 b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-7d69fc07dc7921e3d6 ncalrpc: OLE78D11F70AABEA68C2F28366A4C65 abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-7d69fc07dc7921e3d6 ncalrpc: OLE78D11F70AABEA68C2F28366A4C65 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-f94930b93359f47853 ncalrpc: OLED487AA039E625F297F9E7B564637 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-f94930b93359f47853 ncalrpc: OLED487AA039E625F297F9E7B564637 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-93810c2a3c6bb10b51 ncalrpc: LRPC-e86475b6d206ce6c12 ncalrpc: LRPC-8d315c52e91214abf6 ncalrpc: LRPC-191b94b10f2b07235a f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-e86475b6d206ce6c12 ncalrpc: LRPC-8d315c52e91214abf6 ncalrpc: LRPC-191b94b10f2b07235a 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-8d315c52e91214abf6 ncalrpc: LRPC-191b94b10f2b07235a dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-191b94b10f2b07235a 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 185.8.106.231:49669 ncalrpc: LRPC-02fda3141859093314 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp:

185.8.106.231:49669 ncalrpc: LRPC-02fda3141859093314 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 185.8.106.231:49669 ncalrpc: LRPC-02fda3141859093314 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 185.8.106.231:49669 ncalrpc: LRPC-02fda3141859093314 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 185.8.106.231:49669 ncalrpc: LRPC-02fda3141859093314 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-858d0134ad5fc34ab1 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-858d0134ad5fc34ab1 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-858d0134ad5fc34ab1 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-858d0134ad5fc34ab1 b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-722bfcbb61ac6e3469 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-81c472a245592cb856 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-3719deef2998aa5aa9 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-3719deef2998aa5aa9 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: 185.8.106.231:49670 ncalrpc: ipsec 26268c86-e770-433e-86ef-5f3ba6731fba version: v1.0 ncalrpc: LRPC-52dc1aa6ddb4d06228 ncalrpc: OLEA07B88F31B628C435171C61F16DF 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 185.8.106.231:49671 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc05ED022 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-dc279a96837d4afadf ncalrpc: OLED0F6ECC48A2AA11B20118B08E110 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-dc279a96837d4afadf ncalrpc: OLED0F6ECC48A2AA11B20118B08E110 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-dc279a96837d4afadf ncalrpc: OLED0F6ECC48A2AA11B20118B08E110 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-0e3c90a9011ca0e82d 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-1d252c5f97971258d8 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-1d252c5f97971258d8 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-1d252c5f97971258d8 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-1d252c5f97971258d8 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-1d252c5f97971258d8 906b0ce0-c70b-1067-

b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-23271354176030a4ed ncalrpc: LRPC-23271354176030a4ed ncalrpc: LRPC-23271354176030a4ed d249bd56-4cc0-4fd3-8ce6-6fe050d590cb version: v0.0 ncalrpc: LRPC-9ce541f0942280bc2f d8140e00-5c46-4ae6-80ac-2f9a76df224c version: v0.0 ncalrpc: LRPC-9ce541f0942280bc2f a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-f4b48e002cf7adbfc3 ncalrpc: OLE1434030A9955084D57456BC25EC1 0dd94748-2ff1-11ee-be56-0242ac120002 version: v2.0 ncalrpc: LRPC-0e1a2a1ab9c5a5a684 ncalrpc: OLE41A1E5BBBA86978EAC44D39E7FEE 8c7daf44-b6dc-11d1-9a4c-0020af6e7c57 version: v1.0 annotation: Group Policy RPC Interface provider: appmgmts.dll ncalrpc: LRPC-a183b9dc09fd35861b 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-9d6136efbfe93393a7 ncalrpc: OLEB59BBB3ADE453D243265CD726FB4 d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-9d6136efbfe93393a7 ncalrpc: OLEB59BBB3ADE453D243265CD726FB4 e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-9d6136efbfe93393a7 ncalrpc: OLEB59BBB3ADE453D243265CD726FB4 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-9d6136efbfe93393a7 ncalrpc: OLEB59BBB3ADE453D243265CD726FB4 fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-9d6136efbfe93393a7 ncalrpc: OLEB59BBB3ADE453D243265CD726FB4 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-9d6136efbfe93393a7 ncalrpc: OLEB59BBB3ADE453D243265CD726FB4 d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-9d6136efbfe93393a7 ncalrpc: OLEB59BBB3ADE453D243265CD726FB4 7df1ceae-de4e-4e6f-ab14-49636e7c2052 version: v1.0 ncalrpc: LRPC-f65a8a44d986a58fc7 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: 84c5d621-4341-4ffe-b36f-c12e4d60abe7 ncalrpc: LRPC-c2cb0a47a514fde730 a111f1c5-5923-47c0-9a68-d0bafb577901 version: v1.0 annotation: NetSetup API ncalrpc: LRPC-7e7ee53bcf4d8f1a59 ``` ---------- **137:** ``` NetBIOS Response: Server Name: 402361 MAC Address: AC:1F:6B:3A:B9:4E Names: 402361 <0x20> 402361 <0x0> WORKGROUP <0x0> Additional Interfaces: 192.168.137.1 192.168.209.1 32.168.61.7 ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ---------- **902:** ``` 220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , , NFCSSL supported/t, ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: 402361 NetBIOS Domain Name: 402361 NetBIOS Computer Name: 402361 DNS Domain Name: s402361 FQDN: s402361 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 23 Nov 2023 06:32:58 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: 402361 NetBIOS Domain Name: 402361 NetBIOS Computer Name: 402361 DNS Domain Name: s402361 FQDN: s402361 ``` ---------- **5986:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 20 Nov 2023 21:21:04 GMT Connection: close

Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: 402361 NetBIOS Domain Name: 402361 NetBIOS Computer Name: 402361 DNS Domain Name: s402361 FQDN: s402361 ``` HEARTBLEED: 2023/11/20 21:21:11 185.8.106.231:5986 - ERROR: write tcp 185.8.106.231:5986: broken pipe ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.8.106.231']

Name

f1fa42c3d50d4468b9ac3f7e5cdb1160c8f7ed7bbb6e4017859b837dac7e8d93

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f1fa42c3d50d4468b9ac3f7e5cdb1160c8f7ed7bbb6e4017859b837dac7e8d93']

Name

284458ee75b1d1c2f07ad9fe3a811589360c23092852b2b80a67d2e25e06b269

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '284458ee75b1d1c2f07ad9fe3a811589360c23092852b2b80a67d2e25e06b269']

Name

975d1510380171076b122cd556a1a05bd1eca33b98a9fd003fb3662cb8c83571

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '975d1510380171076b122cd556a1a05bd1eca33b98a9fd003fb3662cb8c83571']

Name

8ff356af97443bd2b028eb57f160a92c2a1ecab2d227977a87a221ae6409c4be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8ff356af97443bd2b028eb57f160a92c2a1ecab2d227977a87a221ae6409c4be']

Name

positivereview.cloud

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'positivereview.cloud']

Name

da27475894815900fefb9d383de0d255bfa3b7a22927b2912a2d614742b3109c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da27475894815900fefb9d383de0d255bfa3b7a22927b2912a2d614742b3109c']

Name

9b9514d5af8a9c92e7596dc15aadba0defaedd9f08ec50a588279aa6f6b8ea80

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9b9514d5af8a9c92e7596dc15aadba0defaedd9f08ec50a588279aa6f6b8ea80']

Name

a63bce69103155accf3c836e7bedf155bee789276624def8713a4431d6562883

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a63bce69103155accf3c836e7bedf155bee789276624def8713a4431d6562883']

Name

thebesttime.buzz

Pattern Type

stix

Pattern

[domain-name:value = 'thebesttime.buzz']

Name

b68736ce13dd44a60e7c462b4f451a4132187a0b76adf9cc201a1468379e7601

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b68736ce13dd44a60e7c462b4f451a4132187a0b76adf9cc201a1468379e7601']

Name

52c47a529e4ddd0778dde84b7f54e1aea326d9f8eeb4ba4961a87835a3d29866

Description

Trojan:Win32/Casdet!rfn

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '52c47a529e4ddd0778dde84b7f54e1aea326d9f8eeb4ba4961a87835a3d29866']

Name

70e79ddbcc5bb1f9d40133e4f3dbcea6362794854d47b6a2081f1439ff795dcd

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '70e79ddbcc5bb1f9d40133e4f3dbcea6362794854d47b6a2081f1439ff795dcd']

Name

6610e152e07225c91a723f3b65e33af4b0df0d816dd69fe73f9d25dc0fc975d4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6610e152e07225c91a723f3b65e33af4b0df0d816dd69fe73f9d25dc0fc975d4']

Name

5e94aa172460e74293db106a98327778ae2d32c6ce6592857a1ec0c581543572

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e94aa172460e74293db106a98327778ae2d32c6ce6592857a1ec0c581543572']

Name

2d8f91bb2359c13abf0ff31af101fc6ecb39849350fbfde015b549e97c8877d5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2d8f91bb2359c13abf0ff31af101fc6ecb39849350fbfde015b549e97c8877d5']

Name

7999c9ba66c57b8f2932f54db723feeef411295f8ed6a6d403376278153745c6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7999c9ba66c57b8f2932f54db723feeef411295f8ed6a6d403376278153745c6']

Name

a3fc0ef279b5717d0b0dcbe25f8e543efee252cc116336a744968279ce9d3c29

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a3fc0ef279b5717d0b0dcbe25f8e543efee252cc116336a744968279ce9d3c29']

Name

10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896

Description

VirTool:Win32/DelfInject.gen!CP

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896']

Name

7d2c98c8d667891c33119d314d1945c285e2a28701970532f6272cad91f59028

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7d2c98c8d667891c33119d314d1945c285e2a28701970532f6272cad91f59028']

Name

fffa5abebf578cfc2200b4856889e397e412e56c5bff0032d2d7565d9286685f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fffa5abebf578cfc2200b4856889e397e412e56c5bff0032d2d7565d9286685f']

Name

394ee7c88a0925698ce1a2e0268ca49404591eb5cdd961d657d785993212cd86

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '394ee7c88a0925698ce1a2e0268ca49404591eb5cdd961d657d785993212cd86']

Name

d2b24a51e7e12fded160344bbac9ee1a9082b690d0c6f326170ea8a224038215

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd2b24a51e7e12fded160344bbac9ee1a9082b690d0c6f326170ea8a224038215']

Name

2f342c83cc564e0110f2c0a32a3259f0ef624cd47c50d82000b308411a402c17

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f342c83cc564e0110f2c0a32a3259f0ef624cd47c50d82000b308411a402c17']

Name

0c3ef20ede53efbe5eebca50171a589731a17037147102838bdb4a41c33f94e5

Description

Trojan:Win32/Casdet!rfn

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0c3ef20ede53efbe5eebca50171a589731a17037147102838bdb4a41c33f94e5']

Name

5b608a6729343cf8b6752d5bb201f906920fcb472f5949e04173b907f65ceff1

Description

W32/Injector

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5b608a6729343cf8b6752d5bb201f906920fcb472f5949e04173b907f65ceff1']

Name

dreamteamup.shop

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'dreamteamup.shop']

Name

063ea8cd25e166182ef68ab1b1157e6448caccaa89cf0f0166c08c21501bf273

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '063ea8cd25e166182ef68ab1b1157e6448caccaa89cf0f0166c08c21501bf273']

Name

74f21cf5ab72aad0f7f3cf3274a167c20e787f9513019510561f39d4230f3c4b

Description

VirTool:Win32/DelfInject.gen!CP

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '74f21cf5ab72aad0f7f3cf3274a167c20e787f9513019510561f39d4230f3c4b']

Name

179.60.149.3

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '179.60.149.3']

Name

161.35.113.5

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBB8h1yUbmctr51/DpeOr3RXk Op6ARdaXW3cuUisKTwGeAR3jfNH6mSsoVfs4MIiuLVxWodkca0YZsm28HtDS6ls= Fingerprint: 1c:51:1a:90:92:f0:72:11:ff:9d:b2:d1:0d:5e:2b:73 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 = '161.35.113.5']

Name

68952e8c311d1573b62d02c60a189e8c248530d4584eef1c7f0ff5ee20d730ab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '68952e8c311d1573b62d02c60a189e8c248530d4584eef1c7f0ff5ee20d730ab']

Name

bb37b05a34b2547941efdceee54ec8745e2ce7a7d5d0968c3b5c10274dc81880

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb37b05a34b2547941efdceee54ec8745e2ce7a7d5d0968c3b5c10274dc81880']

Name

e7b76e11101e35c46a7199851f82c69e819a3d856f6f68fa3af0636c3efde0ca

Description

PUA_Crypto_Mining_CommandLine_Indicators_Oct21

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7b76e11101e35c46a7199851f82c69e819a3d856f6f68fa3af0636c3efde0ca']

Name

bc80b13b639ee4b4a6a79555cb4daf3ec360682322ffae68c1272b5aed8b1593

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bc80b13b639ee4b4a6a79555cb4daf3ec360682322ffae68c1272b5aed8b1593']

Name

185.39.18.170

Description

CC=NL ASN=AS62005 BlueVPS OU

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.39.18.170']

Name

naserviceebaysmman.shop

Description

DarkGate botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'naserviceebaysmman.shop']

Name

sanibroadbandcommunicton.duckdns.org

Pattern Type

stix

Pattern

[hostname:value = 'sanibroadbandcommunicton.duckdns.org']

Name

2264c2f2c2d5a0d6d62c33cadb848305a8fff81cdd79c4d7560021cfb304a121

Description

Trojan:Win32/Casdet!rfn

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2264c2f2c2d5a0d6d62c33cadb848305a8fff81cdd79c4d7560021cfb304a121']

Name

7c6fa5cec54bc8afa51376db19c9c83d7c17f6e21ce761bfb1daeb7ad31d898d

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c6fa5cec54bc8afa51376db19c9c83d7c17f6e21ce761bfb1daeb7ad31d898d']

Name

private-edinmarketing.com

Pattern Type
stix
Pattern
[domain-name:value = 'private-edinmarketing.com']
Name
6e068b9dcd8df03fd6456faeb4293c036b91a130a18f86a945c8964a576c1c70
Description
Cabinet_Archive
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6e068b9dcd8df03fd6456faeb4293c036b91a130a18f86a945c8964a576c1c70']

Malware

Name
DarkGate

Domain-Name

Value
reactervnamnat.com
thebesttime.buzz
bikeontop.shop
whatup.cloud
onlysportsfitnessam.com
dreamteamup.shop
coocooncookiedpo.com
a-1bcdn.com
hardwarenet.cc
wmnwserviceadsmark.com
infocatalog.pics
private-edinmarketing.com
akamai.la

msteamseyeappstore.com

drkgatevservicceoffice.net

awsamazon.cc

marketisportsstumi.win

positivereview.cloud

xfirecovery.pro

battlenet.la

naserviceebaysmman.shop

Email-Addr

Value
coding_guru@exploit.im

StixFile

Value
bc80b13b639ee4b4a6a79555cb4daf3ec360682322ffae68c1272b5aed8b1593
2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084
2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4
8458a43245c6ff9e3d688a8393f692d3088bf5338ae810ff78b8b3a1d751a87e
bde8e0c4bc687ea485fd4a00c86bd25ab14a04edf9b2bbc03808e9b86074717b
6a9e7b47bec075225861d61cf20555c38a17b7b9ff46ff85de7f6791c548cc2e
d2b24a51e7e12fded160344bbac9ee1a9082b690d0c6f326170ea8a224038215
659733a584c52078ac6b568dfb34a089bef2b3835a5ea737d32c1623a468b743
2caa6b5e92ad4c772166860d428d388a4fa376c5adc439b10ee2f045e0a1b003
bd8fc787abfebba8d167e9979c2ec692f861ab21ea138c3381daa852a58677be
09bf1b88716c49a62cb4ff708f7ff4f09cb7c3ff42e58661802cd66f1a2a0311
cb93d34f34e5e999705fd5d17d6725b452c57bc799fc835899e4af9330f4169f
feeddfb2a7cc4945eaedd8f75907c42ff097252c3e38d7ef2006bd7a191f09ae

af85ace1fd89e4c76efdda065cc2fc44de987bfd75f9f6850610327526c97d4b

6610e152e07225c91a723f3b65e33af4b0df0d816dd69fe73f9d25dc0fc975d4

2264c2f2c2d5a0d6d62c33cadb848305a8fff81cdd79c4d7560021cfb304a121

284458ee75b1d1c2f07ad9fe3a811589360c23092852b2b80a67d2e25e06b269

1776dcbc4a3f430dd5ace833aac80b0954a050e5a7dec164b53b62fbe72feab3

cde0f0b6a29a11aa8a5a4ee543fd632cb460bc11927c7153c1f5f8664e474d23

908f2dfed6c122b46e946fe8839feb9218cb095f180f86c43659448e2f709fc7

f02928ec21ad8c600eef3e3a006581a3af858975cbc2ad29ba3dfdd1a78d3cb9

bd9426beaee1c5908b0f71b31539ae4fe3ffed155ab00041b543d48fda3f1654

73c0d0f220a30b541e0855e8039b8050d1332ff03c3e0c8a35671bd5eb9d30be

a3fc0ef279b5717d0b0dcbe25f8e543efee252cc116336a744968279ce9d3c29

3c68facf01aede7bcd8c2aea853324a2e6a0ec8b026d95c7f50a46d77334c2d2

dadd0ec8806d506137889d7f1595b3b5447c1ea30159432b1952fa9551ecfba5

7c6fa5cec54bc8afa51376db19c9c83d7c17f6e21ce761bfb1daeb7ad31d898d

2ffb2a102df381c9688cc78c2cba4faa6a561d5aa78a9163888ebf7c73bdc8d0

c6bce64cf86ff6f6b52b9ffa8b8dc2283645b9f0cea7391117d5dd80c2092ce6

00dbb5f6bbb9c230fc0c7f7526b46d697850587b30d0b4f4d54106eb3a3d5410

74f21cf5ab72aad0f7f3cf3274a167c20e787f9513019510561f39d4230f3c4b

9a19aa451bb9974c05e616bf02762ee001cc02669aca15150199415e5e190f01

e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243

59c026ed7f98aff21521b7a76845821aa5f1ce1a978d1c90404c073bd6310a1d

aa5cb7f6ccb5470ff643cfcba9254263c9db9e7a84984d30166cc14945e219f2

7d2c98c8d667891c33119d314d1945c285e2a28701970532f6272cad91f59028

6345b02dc1606522232ac853a0e2599d166aef91ae1d7f4d4104d184273dc1e8

bec37877e3bffa222efb5c5680c7defd2d917317293d7fa70e0882ad45290a40

a2be457dc7fc5d5662e5db1b51b77094898449fedab7b1a9f837c093c249c5ba

9e398fb049ae1cf95976ba1c80280cb3f78833569fe7fc5c1ba93c7e57c00fac

3340013b0f00fe0c9e99411f722f8f3f0baf9ae4f40ac78796a6d4d694b46d7b

7837e71f9bf00f48ab5336ed8647b116471561181069b79d29dbaee0e951ded7

063ea8cd25e166182ef68ab1b1157e6448caccaa89cf0f0166c08c21501bf273

52c47a529e4ddd0778dde84b7f54e1aea326d9f8eeb4ba4961a87835a3d29866

7999c9ba66c57b8f2932f54db723feeef411295f8ed6a6d403376278153745c6

c88eab30fa03c44b567bcb4e659a60ee0fe5d98664816c70e3b6e8d79169cbea

23885818c2a665d5a57ba16acfe46db68258da619a8db3df8f069c0205ac648e

e7b76e11101e35c46a7199851f82c69e819a3d856f6f68fa3af0636c3efde0ca

684b3445349d8e08e2f2d33f3b30d509a3fde82cb798ccbad2726105301a9470

9b9514d5af8a9c92e7596dc15aadba0defaedd9f08ec50a588279aa6f6b8ea80

453e7fabfa2d6fca1f9a5b9edc456e46417d8fb76332d397a39fcc8e76ccf54f

01e578a65a143c884f054c96574f2f9e203b49f47ebf74a0749ff484866b2eb7

5be83d13f20b4a044a8c8281d13723a808555cdd73a7ddcec37422a4e44fbd4e

22d5fdd23ff4302517d5652375ee5ec3bfb28cb964015b3e9902d2398c908fd9

0e01bad874c61d09d09ce06f76f5e46f6648a1fc943644874c8e1a53a93af9a7

fa0a47360f68f211413d582d2c73035594a9191c2399c52612c940b45402065f

2d08809875f2cfcbe4538d11ee5537768beba0b7740e1785ac35fd90d32e5c25

567d828dab1022eda84f90592d6d95e331e0f2696e79ed7d86ddc095bb2efdc8

f1fa42c3d50d4468b9ac3f7e5cdb1160c8f7ed7bbb6e4017859b837dac7e8d93

8ff356af97443bd2b028eb57f160a92c2a1ecab2d227977a87a221ae6409c4be

a63bce69103155accf3c836e7bedf155bee789276624def8713a4431d6562883

aa92f9692dfa98ba9ee991156612f2015c10a5ecf02b605b0b6d528827430601

68952e8c311d1573b62d02c60a189e8c248530d4584eef1c7f0ff5ee20d730ab

2f342c83cc564e0110f2c0a32a3259f0ef624cd47c50d82000b308411a402c17

f8fcf37ab1e391d1809c4b5baf00d669c4263682d99230432c5199bde5914a60

2bf6b1dcb11e7e32b353e0c135aca9c979177d14aa9834119cd8e4c1a5b08562

3c520028ad9dbf10e5a94023fbbd5ca7134802a6def3fae427f70620c12f8988

70e79ddbcc5bb1f9d40133e4f3dbcea6362794854d47b6a2081f1439ff795dcd

4325d78175a803fb6a1d235e8255816a07283501087e1b115f28c38b6b542856

6a81b3d6606bd5c4f9d3484719ec35fc6d2dedb902a85553705a71a6e1273104

4e48d4c355ceb58267a29fd3337b101722c805a7e53662816b73ce9b756ae321

b0542a719c6b2fc575915e9e4c58920cf999ba5c3f5345617818a9dc14a378b4

fffa5abebf578cfc2200b4856889e397e412e56c5bff0032d2d7565d9286685f

2d8f91bb2359c13abf0ff31af101fc6ecb39849350fbfde015b549e97c8877d5

3a5e7ce24fc5a18843e4f877f5c704bf95eb90c039bc8d791273c191e4ca3242

de2064d4363a3ccbda5518c619f1c803393b0876e349530583a72b1d1643c16a

99f25de5cc5614f4efd967db0dae50f20e2acbae9e98920aff3d98638b9ca1f1

a146f84a0179124d96a707f192f4c06c07690e745cffaef521fcda9633766a44

20cd543224dc3229dece35f018678a52fc98e533596e4995a5534bde0e7e161f

1af981d9c5128b3657cdb5506d61563e0d1908b957e5dd6842059d6d3cfdc622

c9b3e70c459be9643f764afd535976f9d308d098e1476013de431e7aea22b3e9

0c3ef20ede53efbe5eebca50171a589731a17037147102838bdb4a41c33f94e5

bc5ad215876055a8a6a097579e16d24e233a323a6157afbb6db49705ac12a1f1

37ea8a57e3d3964448238aff31125381c7063b98e1fe0d83a20b315b70546c94

acad12dd611551ee4cdfd9fba7dd06c1f6a7c4d8cd8619cbbafa3d8f88bde910

4aea930309b590d34488187a8c9cb31b83ff1faa2ff4d27606e50fac3a0db742

abc35bb943462312437f0c4275b012e8ec03899ab86d353143d92cbefedd7f9d

1d256c2fd442e69120cdf8d12d7bd865f058ec667e2119a66259fc9052dbaa36

1239ab2c5b8f4445353eacba276938c9cce9711a643851db8979728defc5a3ee

b2db96bae6065dbea52711c6f732a29bd39cbb4e81dde9e7d854d52cfb1970f0

74729d4569691daf72e23849e91461471411f551639663e11e1091a48790611e

394ee7c88a0925698ce1a2e0268ca49404591eb5cdd961d657d785993212cd86

54f52ef506f6649c09838b9935aed223f0f320798e13fdb9541ffd1db3e08816

da27475894815900fefb9d383de0d255bfa3b7a22927b2912a2d614742b3109c

96c84918db77c8bc7d5080aca1b618f7ea7c824d27f67b2346364756f04b3226

9f48b63528a24a1241f0bc793e960d420314d595c9927e2294f4475c4be143cd

3491bc6df27858257db26b913da8c35c83a0e48cf80de701a45a30a30544706d

3b271f7f34255146366ab7c7d916fa5ab3b1accfc4b0f3d727e16690cfb7ad3a

cefc06b2bec8d175eaa9bf3f91c8246731811a8ad7b52af336478655dbc70039

b7c6b567eab740efa575826c94f4c9c552ed5894b8b3ef57e77959b740d8bec8

de3f49e68c45db2f31d1cc1d10ff09f8cfce302b92a1f5361c8f34c3d78544e5

d4e766f81e567039c44ccca90ef192a7f063c1783224ee4be3e3d7786980e236

b7874a778f21b2d21a2a2ab2c2ec4a7ae5042443e1d3f20a070424d628079056

6bc0a512fa3d69c724c2a0aaea8f915795f9c0ef68617dbd32d3b78ee5cddc06

2b49ceb658da03b30d38ee2dc46bcf2bb85af728cece29f8c30d7c1a92c1ad09

b15e4b4fcd9f0d23d902d91af9cc4e01417c426e55f6e0b4ad7256f72ac0231a

6e068b9dcd8df03fd6456faeb4293c036b91a130a18f86a945c8964a576c1c70

b6b2b1773fbd354cc7fcf409f4b4208e570be077658c2a92ea59319c250d9f8c

22933b3ae7d125f312b6d1fe6356092cdcd1def6dca3ad128de65ba7986266ae

b68736ce13dd44a60e7c462b4f451a4132187a0b76adf9cc201a1468379e7601

5b608a6729343cf8b6752d5bb201f906920fcb472f5949e04173b907f65ceff1

5e94aa172460e74293db106a98327778ae2d32c6ce6592857a1ec0c581543572

bb37b05a34b2547941efdceee54ec8745e2ce7a7d5d0968c3b5c10274dc81880

975d1510380171076b122cd556a1a05bd1eca33b98a9fd003fb3662cb8c83571

9a7db0204847d26515ed249f9ed577220326f63a724a2e0fb6bb1d8cd33508a3

1fb6b8bed3a67ee4225f852c3d90fd2b629f2541ab431b4bd4d9d9f5bbd2c4b7

0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2

10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896

6750f31ef5e1fe74c1121b0ab1308f93e09505a63322b6ce16fe04099ce8993e

a448c4abbb2f1844a8fa0c929cd84c2f6f57a4af0442a6a4b5307af89c35cef6

00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df

Hostname

Value
intranet.mcasavaya.com
13.deploy.static.akamaitechnologies.pw
sanibroadbandcommunicton.duckdns.org
127.compute-1.amazonaws.cdnprivate.tel

IPv4-Addr

Value
80.66.88.145
5.34.178.21
89.248.193.66
185.143.223.64
45.89.65.198
5.188.87.58
161.35.113.5
167.114.199.65
185.39.18.170
149.248.0.82
179.60.149.3
107.181.161.200
185.8.106.231

Url

Value
https://s2w.inc

External References

- https://otx.alienvault.com/pulse/65a90dfc19a9d37bfaeb52fb
- https://medium.com/s2wblog/detailed-analysis-of-darkgate-investigating-new-top-trend-backdoor-malware-0545ecf5f606