Dec 27 2023

NETMANAGEIT

Intelligence Report

Fog of Cyber Warfare: Cloud Atlas Spies Attack Russian Companies Under the guise of Supporting NWO Participants

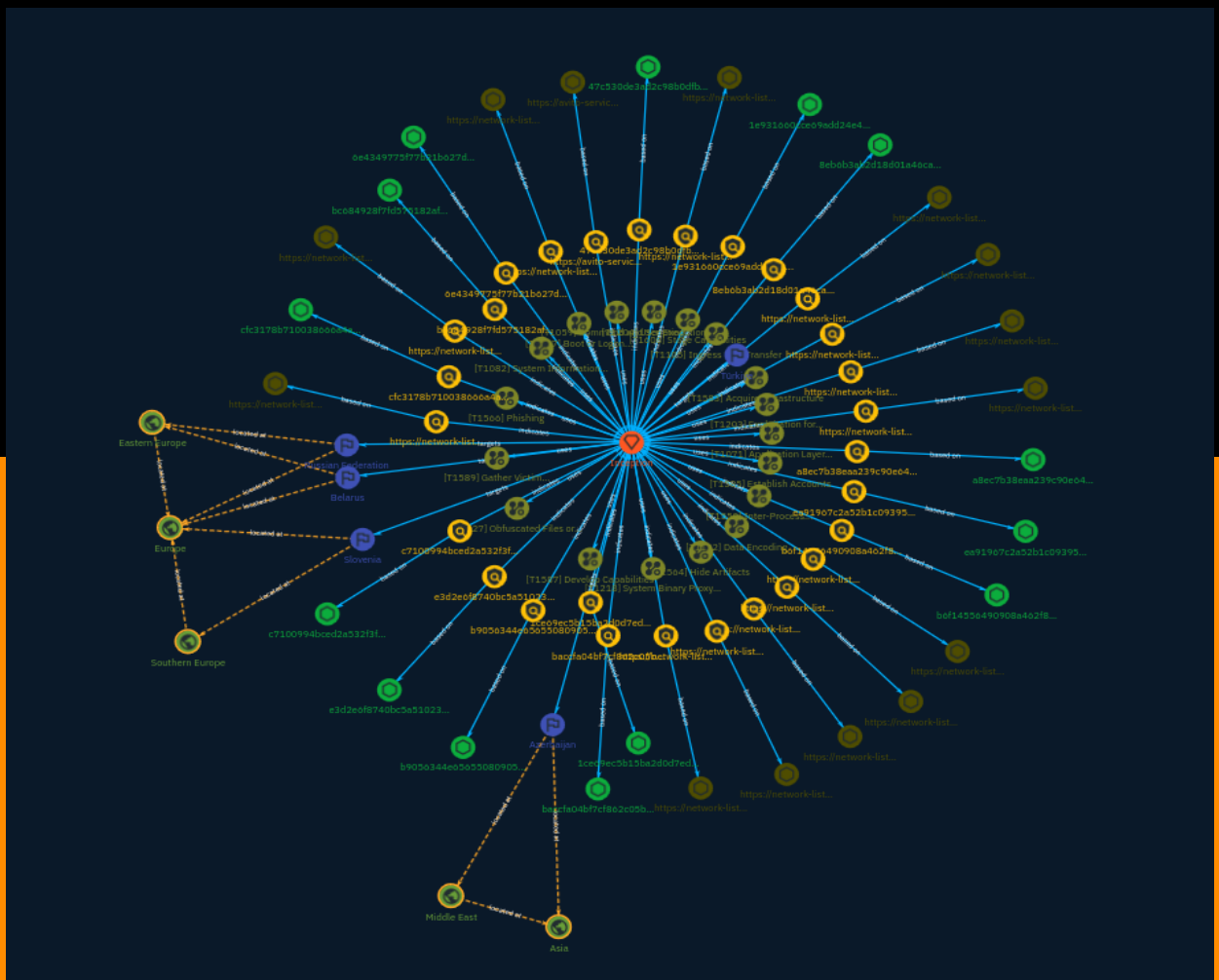

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Cloud Atlas is a pro-government APT group Specializing on cyber espionage and theft of confidential information. According to the researchers, Active at least since 2014. More often than others, Cloud Atlas targets were industrial enterprises and state-owned companies in Russia, Belarus, Azerbaijan, Turkey, and Slovenia. The main attack vector is a targeted email campaign with a malicious attachment.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Establish Accounts

ID

T1585

Description

Adversaries may create and cultivate accounts with services that can be used during targeting. Adversaries can create accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity. (Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) For operations incorporating social engineering, the utilization of an online persona may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, GitHub, Docker Hub, etc.). Establishing a persona may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) Establishing accounts can also include the creation of accounts with email providers, which may be directly leveraged for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1)

Name

Develop Capabilities

ID

T1587

Description

Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: Bitdefender StrongPity June 2020)(Citation: Talos Promethium June 2020) As with legitimate development efforts, different skill sets may be required for developing capabilities. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the capability.

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

Hide Artifacts

ID

T1564

Description

Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Operating systems may have features to hide various artifacts, such as important system files and administrative task execution, to avoid disrupting user work environments and prevent users from changing files or features on the system. Adversaries may abuse these features to hide artifacts such as files, directories, user accounts, or other system activity to evade detection.(Citation: Sofacy Komplex Trojan) (Citation: Cybereason OSX Pirrit)(Citation: MalwareBytes ADS July 2015) Adversaries may also attempt to hide artifacts associated with malicious behavior by creating computing regions that are isolated from common security instrumentation, such as through the use of virtualization technology.(Citation: Sophos Ragnar May 2020)

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

Gather Victim Identity Information

ID

T1589

Description

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about users could also be enumerated via other active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. (Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: OPM Leak)(Citation: Register Deloitte)

(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds) (Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts] (https://attack.mitre.org/techniques/T1078)).

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

Acquire Infrastructure

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090), including from residential proxy services.(Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing) (Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation,

adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

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

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)). 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) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. 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) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

Inter-Process Communication

ID

T1559

Description

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with

each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern. Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) or [Component Object Model](https://attack.mitre.org/techniques/T1559/001). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.(Citation: Linux IPC) Higher level execution mediums, such as those of [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) to facilitate remote IPC execution.(Citation: Fireeye Hunting COM June 2019)

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

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

System 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

Stage Capabilities

ID

T1608

Description

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

Name

Exploitation for Client Execution

ID

T1203

Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

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)

Indicator

Name

e3d2e6f8740bc5a510239af41e77a3e07eaf09f1aa5cda78558035399db3f971

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e3d2e6f8740bc5a510239af41e77a3e07eaf09f1aa5cda78558035399db3f971']

Name

https://network-list.com/?php-wp-content/plugins/contact-form-7/includes/css/styles.css/undesirous

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?php-wp-content/plugins/contact-form-7/includes/css/styles.css/undesirous']

Name

ea91967c2a52b1c09395613f972a319332b678493f4e2ece0e0009e1efd36bec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea91967c2a52b1c09395613f972a319332b678493f4e2ece0e0009e1efd36bec']

Name

b6f14556490908a462f8fb61a46b1b140f40723b5725c93fe4ff87a62f036e80

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b6f14556490908a462f8fb61a46b1b140f40723b5725c93fe4ff87a62f036e80']

Name

https://network-list.com/?php-tag_zabbix/lowlanders

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?php-tag_zabbix/lowlanders']

Name

baccfa04bf7cf862c05bc7180532cf609df43a091febd3d85524d6689df6e405

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'baccfa04bf7cf862c05bc7180532cf609df43a091febd3d85524d6689df6e405']

Name

https://network-list.com/protophloem/p21

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/protophloem/p21']

Name

https://network-list.com/?php-business-and-economy/hematomancy

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?php-business-and-economy/hematomancy']

Name

c7100994bced2a532f3fc350c5db7401775be9658127233c7665e6864c6de2f7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7100994bced2a532f3fc350c5db7401775be9658127233c7665e6864c6de2f7']

Name

cfc3178b710038666a4a4c5676b5c6befea085ad0243663791ae95f65e1468de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cfc3178b710038666a4a4c5676b5c6befea085ad0243663791ae95f65e1468de']

Name

https://network-list.com/outblunder/a63

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/outblunder/a63']

Name

https://network-list.com/?rpgg.html_protophloem

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?rpgg.html_protophloem']

Name

1e931660cce69add24e405c9fbdd3072190c9f716c1675334f00d0bdbf84bf46

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e931660cce69add24e405c9fbdd3072190c9f716c1675334f00d0bdbf84bf46']

Name

a8ec7b38eaa239c90e647a47368159fb2a6a94c0e56df5a4d8f33e5b469e7942

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8ec7b38eaa239c90e647a47368159fb2a6a94c0e56df5a4d8f33e5b469e7942']

Name

47c530de3ad2c98b0dfb0c72a4697240e7a218701c2cce12ae217faf58c32335

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '47c530de3ad2c98b0dfb0c72a4697240e7a218701c2cce12ae217faf58c32335']

Name

https://network-list.com/?php-pvrg.html_outblunder

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?php-pvrg.html_outblunder']

Name

1ce69ec5b15ba2d0d7ed01cd9ae0facecf2b8fbbd32ea3b1f256310c129f5c74

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ce69ec5b15ba2d0d7ed01cd9ae0facecf2b8fbbd32ea3b1f256310c129f5c74']

Name

https://network-list.com/?wkbi.html_handfeed

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?wkbi.html_handfeed']

Name

https://network-list.com/?wp-includes_wlwmanifest.xml/datemark

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?wp-includes_wlwmanifest.xml/datemark']

Name

https://avito-service.net/service/37.html/bersim

Pattern Type

stix

Pattern

[url:value = 'https://avito-service.net/service/37.html/bersim']

Name

https://network-list.com/?wp-content_plugins/photo-gallery/css/bwg-fonts/fonts.css?ver=0.0.1time=1673472550/ballock

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?wp-content_plugins/photo-gallery/css/bwg-fonts/fonts.css?ver=0.0.1time=1673472550/ballock']

Name

https://network-list.com/?area_gifu_?iref=pc_gnavi/semisovereignty

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?area_gifu_?iref=pc_gnavi/semisovereignty']

Name

bc684928f7fd575182af5f797308e9f2286e7bd8d010f6e04913a2600495bbb7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bc684928f7fd575182af5f797308e9f2286e7bd8d010f6e04913a2600495bbb7']

Name

https://network-list.com/?qgcl.html_anapeiratic

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?qgcl.html_anapeiratic']

Name

b9056344e65655080905c4ddb38cfb8a09675fedc4c5244a969918af5b9b39cf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b9056344e65655080905c4ddb38cfb8a09675fedc4c5244a969918af5b9b39cf']

Name

8eb6b3ab2d18d01a46cae3cee0987fe8ecdedce2cb80666057a4880c9f37c529

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8eb6b3ab2d18d01a46cae3cee0987fe8ecdedce2cb80666057a4880c9f37c529']

Name

https://network-list.com/?products_list108.htmlheader-bottom/nemoricole

Pattern Type

stix

Pattern

[url:value = 'https://network-list.com/?products_list108.htmlheader-bottom/nemoricole']

Name

6e4349775f77b21b627d39a125cd60ad9f3df46d2b4f2a7a71df0d459cb7c9ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e4349775f77b21b627d39a125cd60ad9f3df46d2b4f2a7a71df0d459cb7c9ae']

Intrusion-Set

Name
Inception

Description
[Inception](https://attack.mitre.org/groups/G0100) is a cyber espionage group active since at least 2014. The group has targeted multiple industries and governmental entities primarily in Russia, but has also been active in the United States and throughout Europe, Asia, Africa, and the Middle East.(Citation: Unit 42 Inception November 2018)(Citation: Symantec Inception Framework March 2018)(Citation: Kaspersky Cloud Atlas December 2014)

Region

Name
Europe
Name
Asia
Name
Southern Europe
Name
Eastern Europe
Name
Middle East

Country

Name
Azerbaijan
Name
Belarus
Name
Türkiye
Name
Slovenia
Name
Russian Federation

StixFile

Value
1ce69ec5b15ba2d0d7ed01cd9ae0facecf2b8fbbd32ea3b1f256310c129f5c74
cfc3178b710038666a4a4c5676b5c6befea085ad0243663791ae95f65e1468de
1e931660cce69add24e405c9fbdd3072190c9f716c1675334f00d0bdbf84bf46
b6f14556490908a462f8fb61a46b1b140f40723b5725c93fe4ff87a62f036e80
bc684928f7fd575182af5f797308e9f2286e7bd8d010f6e04913a2600495bbb7
6e4349775f77b21b627d39a125cd60ad9f3df46d2b4f2a7a71df0d459cb7c9ae
ea91967c2a52b1c09395613f972a319332b678493f4e2ece0e0009e1efd36bec
baccfa04bf7cf862c05bc7180532cf609df43a091febd3d85524d6689df6e405
a8ec7b38eaa239c90e647a47368159fb2a6a94c0e56df5a4d8f33e5b469e7942
b9056344e65655080905c4ddb38cfb8a09675fedc4c5244a969918af5b9b39cf
c7100994bced2a532f3fc350c5db7401775be9658127233c7665e6864c6de2f7
8eb6b3ab2d18d01a46cae3cee0987fe8ecdedce2cb80666057a4880c9f37c529
e3d2e6f8740bc5a510239af41e77a3e07eaf09f1aa5cda78558035399db3f971

47c530de3ad2c98b0dfb0c72a4697240e7a218701c2cce12ae217faf58c32335

Url

Value
https://network-list.com/?area_gifu_?iref=pc_gnavi/semisovereignty
https://network-list.com/?wkbi.html_handfeed
https://avito-service.net/service/37.html/bersim
https://network-list.com/?wp-includes_wlwmanifest.xml/datemark
https://network-list.com/?qgcl.html_anapeiratic
https://network-list.com/?php-business-and-economy/hematomancy
https://network-list.com/outblunder/a63
https://network-list.com/?rpgg.html_protophloem
https://network-list.com/?wp-content_plugins/photo-gallery/css/bwg-fonts/fonts.css?ver=0.0.1time=1673472550/ballock
https://network-list.com/?php-wp-content/plugins/contact-form-7/includes/css/styles.css/undesirous
https://network-list.com/?php-pvrg.html_outblunder
https://network-list.com/?products_list108.htmlheader-bottom/nemoricole

https://network-list.com/?php-tag_zabbix/lowlanders

https://network-list.com/protophloem/p21

External References

- https://otx.alienvault.com/pulse/658c94713412afcbac226057
- https://www.facct.ru/blog/cloud-atlas/