Mar 27 2024

NETMANAGEIT

Intelligence Report

Breaking Boundaries: Infiltration Beyond LATAM

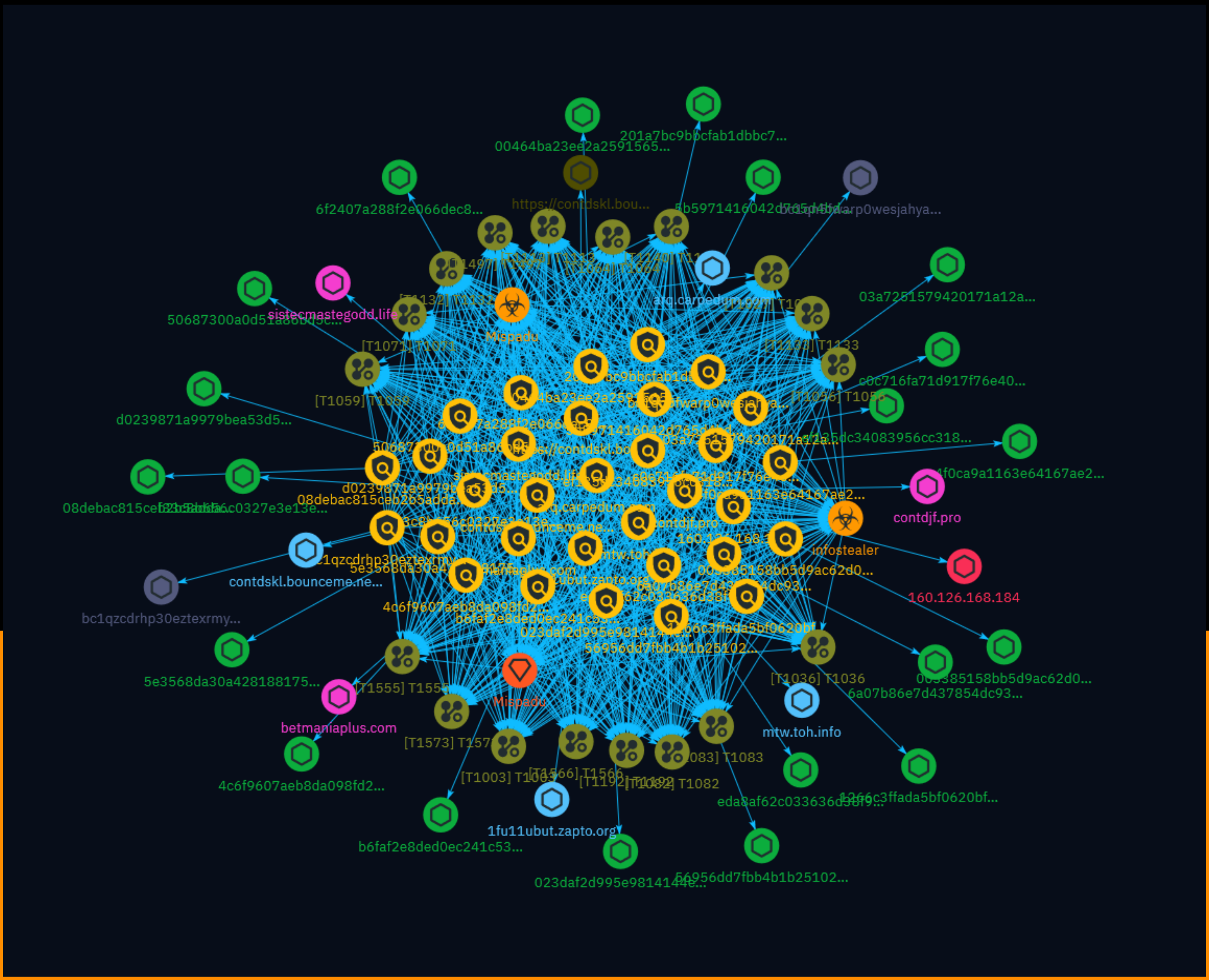

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Recently, Morphisec Labs identified a significant increase in activity linked to Mispadu, a banking trojan first flagged in 2019. Initially concentrated on LATAM countries and Spanish-speaking individuals, Mispadu has broadened its scope in the latest campaign.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

mtw.toh.info

Pattern Type

stix

Pattern

[hostname:value = 'mtw.toh.info']

Name

contdskl.bounceme.net

Pattern Type

stix

Pattern

[hostname:value = 'contdskl.bounceme.net']

Name

arq.carpedum.com

Pattern Type

stix

Pattern

[hostname:value = 'arq.carpedum.com']

Name

1fu11ubut.zapto.org

Pattern Type

stix

Pattern

[hostname:value = '1fu11ubut.zapto.org']

Name

sistecmastegodd.life

Pattern Type

stix

Pattern

[domain-name:value = 'sistecmastegodd.life']

Name

contdjf.pro

Pattern Type

stix

Pattern

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

Name

betmaniaplus.com

Pattern Type

stix

Pattern

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

Name

https://contdskl.bounceme.net/dhyhsh3am1.ahgrher2

Pattern Type

stix

Pattern

[url:value = 'https://contdskl.bounceme.net/dhyhsh3am1.ahgrher2']

Name

160.126.168.184

Pattern Type
stix
Pattern
[ipv4-addr:value = '160.126.168.184']
Name
f33c8b656c0327e3e13e1466e98d3b8e37acec0f28cede0b4d307b52dba63b35
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f33c8b656c0327e3e13e1466e98d3b8e37acec0f28cede0b4d307b52dba63b35']
Name
ef135dc34083956cc31881a526bb6119d24dc93096ee282e0feab8d43d603a03
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ef135dc34083956cc31881a526bb6119d24dc93096ee282e0feab8d43d603a03']
Name

eda8af62c033636d38f9e70e77b011df89c48feb8a393415a7752b7759dcef4c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'eda8af62c033636d38f9e70e77b011df89c48feb8a393415a7752b7759dcef4c']

Name

d0239871a9979bea53d538ca2ef680f433699b749600ab2e93f318fc31a4c33f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd0239871a9979bea53d538ca2ef680f433699b749600ab2e93f318fc31a4c33f']

Name

c0c716fa71d917f76e40c0f50c58e1217bd7bae8ea20d292ad7b4a807774deeb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0c716fa71d917f76e40c0f50c58e1217bd7bae8ea20d292ad7b4a807774deeb']

Name

b6faf2e8ded0ec241c53ed1462032e43d32671877773c7def6f69c9286403fde

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b6faf2e8ded0ec241c53ed1462032e43d32671877773c7def6f69c9286403fde']

Name

6f2407a288f2e066dec8a87f1c8ca4d8b9a0954ef712dfb8c97214781641f150

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f2407a288f2e066dec8a87f1c8ca4d8b9a0954ef712dfb8c97214781641f150']

Name

6a07b86e7d437854dc93fa9efe0a7b20787382589a27885b6f4a4727bfb1e3f2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a07b86e7d437854dc93fa9efe0a7b20787382589a27885b6f4a4727bfb1e3f2']

Name

5e3568da30a42818817529c5c4156555a6b8d01a0f3259349311fbd1f1e892c0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e3568da30a42818817529c5c4156555a6b8d01a0f3259349311fbd1f1e892c0']

Name

5b5971416042d765d4bd57efe4b912ae24475f3f27de40facad91582e446aadc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5b5971416042d765d4bd57efe4b912ae24475f3f27de40facad91582e446aadc']

Name

56956dd7fbb4b1b251022ec5f84dea9a6049ac5e5b6d0ce077c850f8d63b81eb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'56956dd7fbb4b1b251022ec5f84dea9a6049ac5e5b6d0ce077c850f8d63b81eb']

Name

50687300a0d51a86bd5c858b6ee6fa0db171926da7fcbc8ac93f9a336e709443

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'50687300a0d51a86bd5c858b6ee6fa0db171926da7fcbc8ac93f9a336e709443']

Name

4f0ca9a1163e64167ae2406b17f6bb340235a173e12d4e8aa621665c7af3b571

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'4f0ca9a1163e64167ae2406b17f6bb340235a173e12d4e8aa621665c7af3b571']

Name

4c6f9607aeb8da098fd2e802a0722a3f1ee2c1d4cbe5cc4cbd25832367424162

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'4c6f9607aeb8da098fd2e802a0722a3f1ee2c1d4cbe5cc4cbd25832367424162']

Name

201a7bc9bbcfab1dbbc7f51312fa45c779ffb929393c646f636f6e6f44936b10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'201a7bc9bbcfab1dbbc7f51312fa45c779ffb929393c646f636f6e6f44936b10']

Name

1266c3ffada5bf0620bf64a60c24457f14468c26996af6d321d7ca2cb3977f37

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'1266c3ffada5bf0620bf64a60c24457f14468c26996af6d321d7ca2cb3977f37']

Name

08debac815ceb2b5addaa2a93c292fceac6d8d46ec32cdf4e4ffd976f7e99366

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'08debac815ceb2b5addaa2a93c292fceac6d8d46ec32cdf4e4ffd976f7e99366']

Name

03a7251579420171a12a1e416ca91f7231058fe008d008aaede2b5e589c01b25

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'03a7251579420171a12a1e416ca91f7231058fe008d008aaede2b5e589c01b25']

Name

023daf2d995e9814144e3bf0743d6e32b6e50f2279e245df006c3eaae507dab5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '023daf2d995e9814144e3bf0743d6e32b6e50f2279e245df006c3eaae507dab5']

Name

00464ba23ee2a2591565912294f3d3b16f7c67e4cf9335dab39eb202f483f5b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '00464ba23ee2a2591565912294f3d3b16f7c67e4cf9335dab39eb202f483f5b3']

Name

003385158bb5d9ac62d0f3f9fb4a43a2f970a4f36d8e9b5185158b6cfa598896

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '003385158bb5d9ac62d0f3f9fb4a43a2f970a4f36d8e9b5185158b6cfa598896']

Name

bc1qzcdrhp30eztexrmyvz5dwuyzzqyylq5muuyllf

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = 'bc1qzcdrhp30eztexrmyvz5dwuyzzqyylq5muuyllf']

Name

bc1qn5fwarp0wesjahyaavj3zpzawsh3mp0mpuw94n

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = 'bc1qn5fwarp0wesjahyaavj3zpzawsh3mp0mpuw94n']

Intrusion-Set

Name
Mispadu

Malware

Name
Mispadu

Name
infostealer

Attack-Pattern

Name
T1192
ID
T1192
Name
T1132
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

T1056

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

T1573

ID

T1573

Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

Name

T1064

ID

T1064

Description

This technique has been deprecated. Please use [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) where appropriate. Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and [PowerShell](https://attack.mitre.org/techniques/T1086) but could also be in the form of command-line batch scripts. Scripts can be embedded inside Office documents as macros that can be set to execute when files used in [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), where adversaries will rely on macros being allowed or that the user will accept to activate them. Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit (Citation: Metasploit_Ref), Veil (Citation: Veil_Ref), and PowerSploit (Citation: Powersploit) are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell. (Citation: Alperovitch 2014)

Name

T1083

ID

T1083

Description

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

Name

T1059

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

T1027

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

T1566

ID

T1566

Description

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

Name

T1497

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

Name

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1555

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

T1140

ID

T1140

Description

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

Name

T1082

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

T1071

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

T1133

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

T1003

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Name

T1113

ID

T1113

Description

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

Hostname

Value
mtw.toh.info
contdskl.bounceme.net
arq.carpedum.com
1fu11ubut.zapto.org

Domain-Name

Value
sistecmastegodd.life
contdjf.pro
betmaniaplus.com

Url

Value
https://contdskl.bounceme.net/dhyhsh3am1.ahgrher2

IPv4-Addr

Value
160.126.168.184

StixFile

Value
ef135dc34083956cc31881a526bb6119d24dc93096ee282e0feab8d43d603a03
f33c8b656c0327e3e13e1466e98d3b8e37acec0f28cede0b4d307b52dba63b35
eda8af62c033636d38f9e70e77b011df89c48feb8a393415a7752b7759dcef4c
d0239871a9979bea53d538ca2ef680f433699b749600ab2e93f318fc31a4c33f
c0c716fa71d917f76e40c0f50c58e1217bd7bae8ea20d292ad7b4a807774deeb
b6faf2e8ded0ec241c53ed1462032e43d32671877773c7def6f69c9286403fde
6f2407a288f2e066dec8a87f1c8ca4d8b9a0954ef712dfb8c97214781641f150
6a07b86e7d437854dc93fa9efe0a7b20787382589a27885b6f4a4727bfb1e3f2
5e3568da30a42818817529c5c4156555a6b8d01a0f3259349311fbd1f1e892c0
5b5971416042d765d4bd57efe4b912ae24475f3f27de40facad91582e446aadc
56956dd7fbb4b1b251022ec5f84dea9a6049ac5e5b6d0ce077c850f8d63b81eb
50687300a0d51a86bd5c858b6ee6fa0db171926da7fcbc8ac93f9a336e709443
4f0ca9a1163e64167ae2406b17f6bb340235a173e12d4e8aa621665c7af3b571

4c6f9607aeb8da098fd2e802a0722a3f1ee2c1d4cbe5cc4cbd25832367424162
201a7bc9bbcfab1dbbc7f51312fa45c779ffb929393c646f636f6e6f44936b10
1266c3ffada5bf0620bf64a60c24457f14468c26996af6d321d7ca2cb3977f37
08debac815ceb2b5addaa2a93c292fceac6d8d46ec32cdf4e4ffd976f7e99366
03a7251579420171a12a1e416ca91f7231058fe008d008aaede2b5e589c01b25
023daf2d995e9814144e3bf0743d6e32b6e50f2279e245df006c3eaae507dab5
003385158bb5d9ac62d0f3f9fb4a43a2f970a4f36d8e9b5185158b6cfa598896
00464ba23ee2a2591565912294f3d3b16f7c67e4cf9335dab39eb202f483f5b3

Cryptocurrency-Wallet

Value
bc1qzcdrhp30eztexrmyvz5dwuyzzqyylq5muuyllf
bc1qn5fwarp0wesjahyaavj3zpzawsh3mp0mpuw94n

External References

- https://blog.morphisec.com/mispadu-infiltration-beyond-latam
- https://otx.alienvault.com/pulse/6603e57df78a2aaec0f17cfe