Jun 22 2023

NETMANAGEIT

Intelligence Report

Threat Group Assessment: Muddled Libra

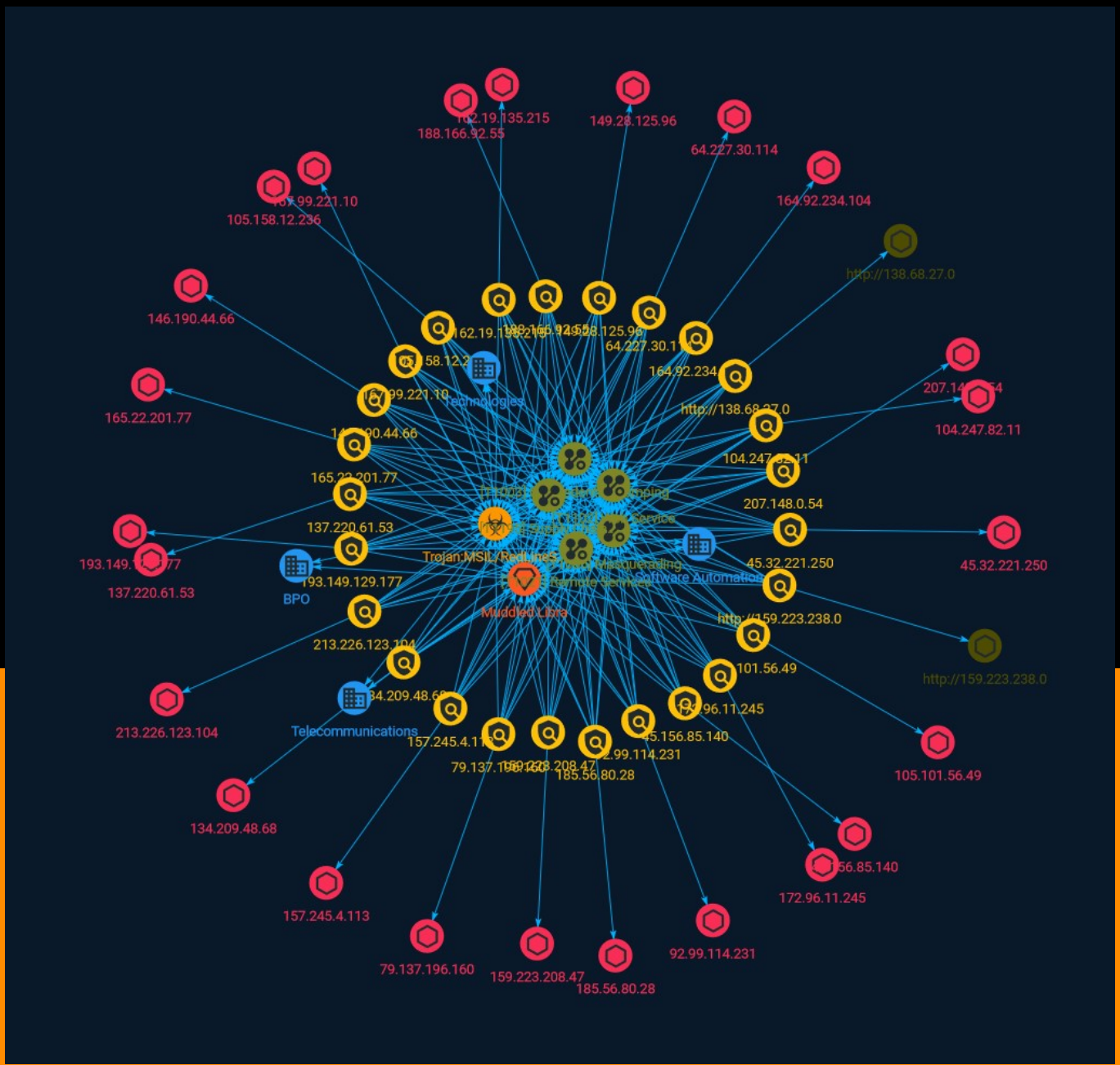

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Muddled Libra is a sophisticated and persistent cyber-attack group that targets high-value cryptocurrency institutions and individuals.

Confidence

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

15 / 100

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name

or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Supply Chain Compromise

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to

access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Sector

Name
BPO
Name
Software Automation
Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name
162.19.135.215
Description
ISP: OVH SAS **OS:** None ---------- Hostnames: - ip215.ip-162-19-135.eu ---------- u7oWc6eJF19EhSblzHIZ6cL5KXOZAin8sD+gEaD7PbT+OcF6U6B0vuE5jwC5fimcIIeOkycMHz7Z /Y4t4tCH91INJluEUl ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-
Pattern Type
stix
Pattern
[ipv4-addr:value = '162.19.135.215']
Name
45.32.221.250
Description
CC=US ASN=AS20473 AS-CHOOPA
Pattern Type

stix

Pattern

[ipv4-addr:value = '45.32.221.250']

Name

193.149.129.177

Description

ISP: BL Networks **OS:** None ---------- Hostnames: ---------- Domains: --
\<\xe7l\xaag\x88\xb5\x12\'S\xb3E\x8cM\x16\xd2B\xf9UU\x00\x00\x00\x00\x10\x00\x00\x00ZZZZZZZZZZZ
``` ---------- **8443:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Mi

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.149.129.177']

Name

164.92.234.104

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domai
group18-sha512 Server Host Key Algorithms: ecdsa-sha2-nistp256 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 En

Pattern Type
```

stix

Pattern

[ipv4-addr:value = '164.92.234.104']

Name

92.99.114.231

Description

CC=AE ASN=AS5384 Emirates Telecommunications Group Company (etisalat Group) Pjsc

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.99.114.231']

Name

146.190.44.66

Description

CC=US ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.190.44.66']

Name

207.148.0.54

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 207.148.0.54.vultruse
kzexMKEahCTXnmQVPT6dxWA8ocQ4GdnVPuhgyOUeyw6jkqqzvhdomxYI+BvHwl5MKccV Fingerprint: c5:be:71:49
aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cas

Pattern Type

stix

Pattern

[ipv4-addr:value = '207.148.0.54']

Name

79.137.196.160

Description

ISP: AEZA GROUP Ltd **OS:** Ubuntu ---------- Hostnames: - ponisha.pro - moonlit-NL.ae
sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman
Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Sun, 18 Jun 2023 1
Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Xss-Protection: 1; mode=block X-Frame-Opti

Pattern Type

stix

Pattern
[ipv4-addr:value = '79.137.196.160']
Name
188.166.92.55
Description
CC=NL ASN=AS14061 DIGITALOCEAN-ASN
Pattern Type
stix
Pattern
[ipv4-addr:value = '188.166.92.55']
Name
105.101.56.49
Description
CC=DZ ASN=AS36947 Telecom Algeria
Pattern Type
stix
Pattern
[ipv4-addr:value = '105.101.56.49']

Name

137.220.61.53

Description

ISP: The Constant Company, LLC **OS:** Debian ---------- Hostnames: - 137.220.61.53.vultr
t9Vx0lWo3kphwWfew4d9vhv/4sbU9VDXfgeJyH95iYfFOtls2mupvgVTzdpc yZm9hc1Knd1ppaZK2k2iSqinvOMw3W
ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.220.61.53']

Name

104.247.82.11

Description

ISP: Team Internet AG **OS:** None ---------- Hostnames: - parkingcrew.net ----------
Lifetime: 30 Content-Type: text/html; charset=UTF-8 Date: Wed, 21 Jun 2023 20:34:27 GMT Server: nginx Vary:

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.247.82.11']

Name
159.223.208.47
Description
ISP: DigitalOcean, LLC **OS:** Ubuntu ---------- Hostnames: ---------- Dom
Pattern Type
stix
Pattern
[ipv4-addr:value = '159.223.208.47']
Name
167.99.221.10
Description
CC=NL ASN=AS14061 DIGITALOCEAN-ASN
Pattern Type
stix
Pattern
[ipv4-addr:value = '167.99.221.10']
Name
http://159.223.238.0

Pattern Type
stix
Pattern
[url:value = 'http://159.223.238.0']
Name
134.209.48.68
Description
CC=US ASN=AS14061 DIGITALOCEAN-ASN
Pattern Type
stix
Pattern
[ipv4-addr:value = '134.209.48.68']
Name
149.28.125.96
Description
CC=US ASN=AS20473 AS-CHOOPA
Pattern Type
stix

Pattern

[ipv4-addr:value = '149.28.125.96']

Name

45.156.85.140

Description

CC=NL ASN=AS30823 combahton GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.156.85.140']

Name

165.22.201.77

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: - stage.bidirco.pt - sso.bidirco.p includeSubDomains X-Robots-Tag: none Cache-Control: no-cache, must-revalidate, no-transform, no-store

Pattern Type

stix

Pattern

[ipv4-addr:value = '165.22.201.77']

Name

http://138.68.27.0

Pattern Type

stix

Pattern

[url:value = 'http://138.68.27.0']

Name

157.245.4.113

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domai
Algorithms: ecdsa-sha2-nistp256 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 Encryption Algorithms: aes256-gcm

Pattern Type

stix

Pattern

[ipv4-addr:value = '157.245.4.113']

Name

105.158.12.236

Description
CC=MA ASN=AS36903 MT-MPLS
Pattern Type
stix
Pattern
[ipv4-addr:value = '105.158.12.236']
Name
172.96.11.245
Description
CC=US ASN=AS64236 UNREAL-SERVERS
Pattern Type
stix
Pattern
[ipv4-addr:value = '172.96.11.245']
Name
213.226.123.104
Description

ISP: IT Resheniya LLC **OS:** None ---------- Hostnames: - plesk.strgsevrers.com ---------
12:21:18 GMT ETag: "1b0-5ea70d8cb6b80" Accept-Ranges: bytes Vary: Accept-Encoding ``` ---------- **1
+OK Dovecot ready. <272e7e.2.6493d07b.lHn0sSCjieX2osPBf7rYuA==@stoic-brattain.213-226-123-104.plesk.pag
CP="NON COR CURa ADMa OUR NOR UNI COM NAV STA" X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; r

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.226.123.104']

Name

64.227.30.114

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domai
IozkBMytAkw/EsT4sU91oFUqp25BgYHTIwWsNgrxwW6go15VlKmgHMeMI90EoMF97coHAvv+uyS9 Ge9mQ1evE55
aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm
MISS from proxy X-Cache-Lookup: NONE from proxy:8800 Connection: close ``` ---------- **8815:** ```
Content-Language: en X-Cache: MISS from proxy X-Cache-Lookup: NONE from proxy:8800 Connection: close
ERR_INVALID_URL 0 Vary: Accept-Language Content-Language: en X-Cache: MISS from proxy X-Cache-Lookup
Content-Length: 3497 X-Squid-Error: ERR_INVALID_URL 0 Vary: Accept-Language Content-Language: en X-Cac
Type: text/html;charset=utf-8 Content-Length: 3497 X-Squid-Error: ERR_INVALID_URL 0 Vary: Accept-Languag
Jun 2023 09:12:39 GMT Content-Type: text/html;charset=utf-8 Content-Length: 3497 X-Squid-Error: ERR_INVAL
Mime-Version: 1.0 Date: Tue, 20 Jun 2023 05:54:24 GMT Content-Type: text/html;charset=utf-8 Content-Length

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.227.30.114']

Name

185.56.80.28

Description

ISP: NForce Entertainment B.V. **OS:** None ---------- Hostnames: - topkek.com ----------
Build: 10.0.17763 Target Name: WIN-FFFRP53NR01 NetBIOS Domain Name: WIN-FFFRP53NR01 NetBIOS Compu
_SILENCE_CXX17_OLD_ALLOCATOR_MEMBERS_DEPRECATION_WARNING _SILENCE_CXX17_CODECVT_HEADER_DI
ABSL_FORCE_ALIGNED_ACCESS", "cxxflags": "/TP", "linkflags": "/nologo /DEBUG /INCREMENTAL:NO /LARGEADI
"sysInfo": "deprecated", "modules": [], "openssl": { "running": "Windows SChannel" }, "javascriptEngine": "moz

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.56.80.28']

Intrusion-Set

Name
Muddled Libra

Malware

Name
Trojan:MSIL/RedLineStealer

IPv4-Addr

Value
79.137.196.160
157.245.4.113
146.190.44.66
92.99.114.231
207.148.0.54
137.220.61.53
105.158.12.236
105.101.56.49
165.22.201.77
149.28.125.96
159.223.208.47
172.96.11.245
193.149.129.177

164.92.234.104
64.227.30.114
45.32.221.250
185.56.80.28
213.226.123.104
162.19.135.215
188.166.92.55
167.99.221.10
104.247.82.11
134.209.48.68
45.156.85.140

External References

- https://unit42.paloaltonetworks.com/muddled-libra/
- https://otx.alienvault.com/pulse/649448a842367084d6039b52