Oct 28 2023

NETMANAGEIT

Intelligence Report

Understanding DNS Tunneling Traffic in the Wild

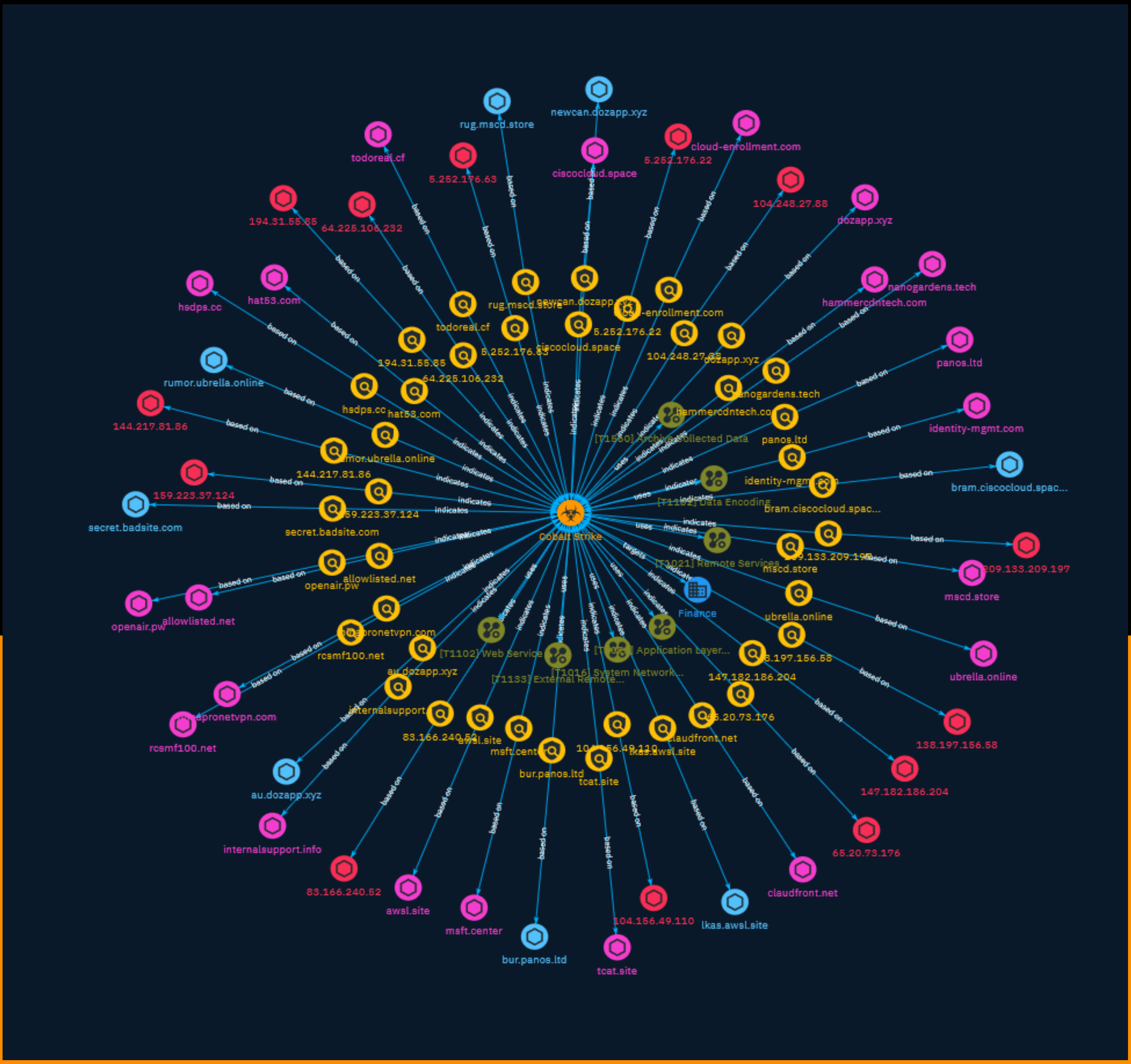

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A study by Palo Alto Networks on how DNS tunneling techniques are used in the wild shows that attackers are using the protocol to bypass security policies in enterprise networks and bypass circumvention and censorship circumventions.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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

System Network Configuration Discovery

ID

T1016

Description

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. `show ip route`, `show ip interface`).(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion) Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

Name

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

External Remote Services

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

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)

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.

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Indicator

Name

104.156.49.110

Description

ISP: HIVELOCITY, Inc. **OS:** None ------------------------- Hostnames: - 104-156-49-110.static.hvvc.us ------------------------- Domains: - hvvc.us ------------------------- Services: **53:** ``` ``` ------------------ **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Oct 2023 01:17:54 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Tue, 11 Apr 2023 17:22:46 GMT Connection: keep-alive ETag: "64359766-267" Accept-Ranges: bytes ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.156.49.110']

Name

209.133.209.197

Description

ISP: HIVELOCITY, Inc. **OS:** None ------------------------- Hostnames: - 209-133-209-197.static.hvvc.us ------------------------- Domains: - hvvc.us

-------------------------- Services: **53:** ``` ``` ------------------ **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Oct 2023 08:47:21 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Wed, 19 Oct 2022 10:48:51 GMT Connection: keep-alive ETag: "634fd613-267" Accept-Ranges: bytes ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.133.209.197']

Name

bur.panos.ltd

Pattern Type

stix

Pattern

[hostname:value = 'bur.panos.ltd']

Name

138.197.156.58

Description

CC=CA ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '138.197.156.58']

Name

awsl.site

Pattern Type

stix

Pattern

[domain-name:value = 'awsl.site']

Name

5.252.176.22

Description

CC=RU ASN=AS39798 MivoCloud SRL

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.176.22']

Name

newcan.dozapp.xyz

Pattern Type

stix

Pattern

[hostname:value = 'newcan.dozapp.xyz']

Name

internalsupport.info

Pattern Type

stix

Pattern

[domain-name:value = 'internalsupport.info']

Name

mscd.store

Pattern Type

stix

Pattern

[domain-name:value = 'mscd.store']

Name

cloud-enrollment.com

Pattern Type
stix
Pattern
[domain-name:value = 'cloud-enrollment.com']
Name
tcat.site
Pattern Type
stix
Pattern
[domain-name:value = 'tcat.site']
Name
todoreal.cf
Pattern Type
stix
Pattern
[domain-name:value = 'todoreal.cf']
Name
au.dozapp.xyz

Pattern Type

stix

Pattern

[hostname:value = 'au.dozapp.xyz']

Name

hammercdntech.com

Pattern Type

stix

Pattern

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

Name

claudfront.net

Pattern Type

stix

Pattern

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

Name

rumor.ubrella.online

Pattern Type

stix

Pattern

[hostname:value = 'rumor.ubrella.online']

Name

bram.ciscocloud.space

Pattern Type

stix

Pattern

[hostname:value = 'bram.ciscocloud.space']

Name

64.225.106.232

Description

CC=DE ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.225.106.232']

Name

rcsmf100.net

Pattern Type

stix

Pattern

[domain-name:value = 'rcsmf100.net']

Name

65.20.73.176

Description

CC=IN ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '65.20.73.176']

Name

83.166.240.52

Description

CC=RU ASN=AS24936 Plusinfo OOO

Pattern Type

stix

Pattern

[ipv4-addr:value = '83.166.240.52']

Name

hsdps.cc

Pattern Type

stix

Pattern

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

Name

5.252.176.63

Description

CC=RU ASN=AS39798 MivoCloud SRL

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.176.63']

Name
rug.mscd.store
Pattern Type
stix
Pattern
[hostname:value = 'rug.mscd.store']

Name
144.217.81.86
Description
ISP: OVH SAS **OS:** None ------------------------- Hostnames: - vps-cb876b65.vps.ovh.ca ------------------------- Domains: - ovh.ca ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDxhpFPHn7t1/U0cfVUQmCyLoLtYmNqDzMAhdOzCB8Qx1lB pVo8IUHP6Wj20DQO1nSvsxxW3gHA57iyOtSv2rsDYl9lcXAgI1Lt0yEBQloqAN5xE+c2s/yOkUrn mnODpk6sHL03usI0BwBy1QJKekbm9FZfechp1LbNqVXhJuBgu2S7+8saNiQ9Nc6xS+RkWztJtHtQ FtWx4yhCcvqPaeI1tl8l/C4I6bTj8cpOlt34HCqLVQXNv2A4L3lD1j5/2LI1BRQhagyr74RRrjOw o9TAzVaRSWpVI3wqurzTdFvb68Kf6iQ4/5GszXhOJiQqvyJz+3AdhuiU6X0wyXnyg9tlMRQmTCsL I1IFBjDKN4g09ggUu2bJmYYw9S9AQpXMqmOH0bLB9HYVmjSjmiVJWfzpZUImFwgTnFCnSAh6HJ mm zJgSn/yNTaQhevnQVNVUQVBqD3dEw+iAyXjl7XuTBuG43TvaJu9Loyux0tCw0abV6ZgeTsr50Hkg sIAz4rMuDLE= Fingerprint: 5f:a3:7b:e8:bb:f6:4d:4d:cb:12:62:fa:f1:c8:69:95 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com

umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression
Algorithms: none zlib@openssh.com ``` ------------------ **110:** ``` SSH-2.0-
dropbear_2019.78 Key type: ssh-rsa Key:
AAAAB3NzaC1yc2EAAAADAQABAAABAQCFwHDRHzq1zvBZwbI5R5xWo021wunnSRYvILLymnyM40
Gu KQgb8nJbm0wI4T8DjH7hxCKcrdzbZ5kA6GLH8pipgP7568IIo/
1HqloyBt1dQptQDoqjwGjowVTn RN5ukV/
L18r1L+wRW6JqbRoE2oFkVeKDFwS4lsjcZQUiTejOB0axD87Bbz9hkYkstBK2vciC/MJ9
0CA0iuOmMDLx24pJhpHfxBZFgoZAiBCoPBaJV1YjoAk5lc8/ZWZngEinX3ySs3VZaroJDLJ5TmeU
SajGlCmTO/mbe63wtrsGcYKNJ31AF2fkuITnB5FREOGORQDuGg8We3JKhkxnSDSipeeD
Fingerprint: 58:0b:28:47:d3:7c:11:c7:c3:c0:4e:88:10:fb:81:fa Kex Algorithms: curve25519-sha256
curve25519-sha256@libssh.org ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256
diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 kexguess2@matt.ucc.asn.au
Server Host Key Algorithms: ecdsa-sha2-nistp256 ssh-rsa ssh-dss Encryption Algorithms:
aes128-ctr aes256-ctr aes128-cbc aes256-cbc 3des-ctr 3des-cbc MAC Algorithms: hmac-sha1-96 hmac-sha1 hmac-sha2-256 Compression Algorithms: zlib@openssh.com none ```
------------------ **443:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '144.217.81.86']

Name

identity-mgmt.com

Pattern Type

stix

Pattern

[domain-name:value = 'identity-mgmt.com']

Name

secret.badsite.com

Pattern Type

stix

Pattern

[hostname:value = 'secret.badsite.com']

Name

104.248.27.88

Description

CC=DE ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.248.27.88']

Name

lkas.awsl.site

Pattern Type

stix

Pattern

[hostname:value = 'lkas.awsl.site']

Name

dozapp.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'dozapp.xyz']

Name

ciscocloud.space

Pattern Type

stix

Pattern

[domain-name:value = 'ciscocloud.space']

Name

194.31.55.85

Description

CC=LT ASN=AS47583 Hostinger International Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.31.55.85']

Name

nanogardens.tech

Pattern Type

stix

Pattern

[domain-name:value = 'nanogardens.tech']

Name

msft.center

Pattern Type

stix

Pattern

[domain-name:value = 'msft.center']

Name

allowlisted.net

Pattern Type

stix

Pattern

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

Name

ubrella.online

Pattern Type

stix

Pattern

[domain-name:value = 'ubrella.online']

Name

159.223.37.124

Description

CC=SG ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.223.37.124']

Name

panos.ltd

Pattern Type

stix

Pattern

[domain-name:value = 'panos.ltd']

Name

hat53.com

Pattern Type

stix

Pattern

[domain-name:value = 'hat53.com']

Name

openair.pw

Pattern Type

stix

Pattern

[domain-name:value = 'openair.pw']

Name

147.182.186.204

Description

CC=US ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '147.182.186.204']

Name

minapronetvpn.com

Pattern Type

stix

Pattern

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

Malware

Name
Cobalt Strike

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Domain-Name

Value
cloud-enrollment.com
hammercdntech.com
rcsmf100.net
dozapp.xyz
openair.pw
msft.center
ubrella.online
awsl.site
hat53.com
tcat.site
todoreal.cf
identity-mgmt.com
claudfront.net

ciscocloud.space
mscd.store
internalsupport.info
nanogardens.tech
allowlisted.net
minapronetvpn.com
panos.ltd
hsdps.cc

Hostname

Value
rumor.ubrella.online
lkas.awsl.site
au.dozapp.xyz
rug.mscd.store
bur.panos.ltd
newcan.dozapp.xyz
bram.ciscocloud.space
secret.badsite.com

IPv4-Addr

Value
104.156.49.110
5.252.176.63
159.223.37.124
147.182.186.204
64.225.106.232
138.197.156.58
83.166.240.52
5.252.176.22
65.20.73.176
104.248.27.88
209.133.209.197
144.217.81.86
194.31.55.85

External References

- https://otx.alienvault.com/pulse/652d66ac8e5d67bf88fd27a3
- https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild/