Nov 26 2023

NETMANAGEIT

Intelligence Report

Tracking Vidar Infrastructure with Censys

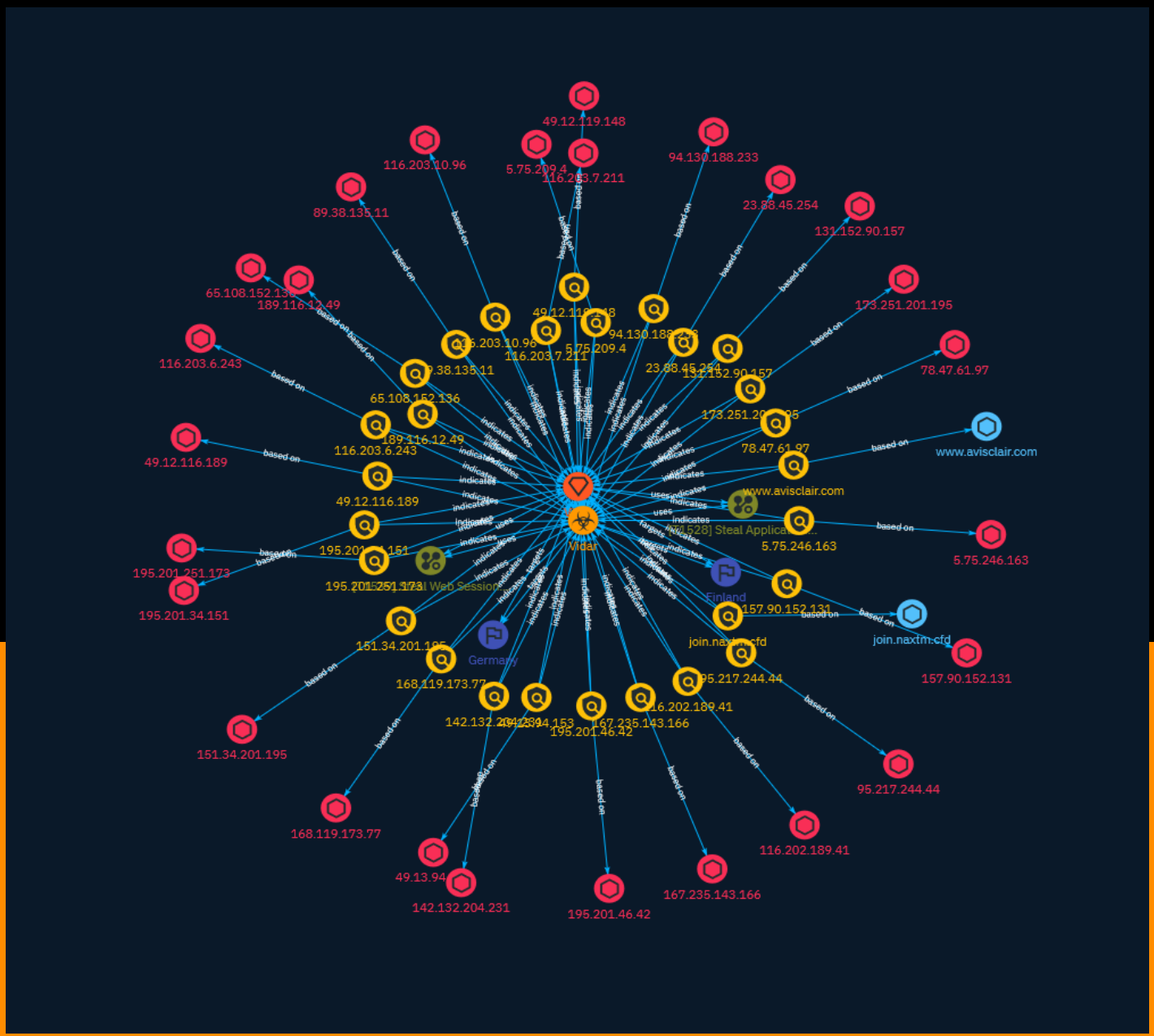

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Following Censys' research, we look at some of the more advanced malware trojans that are used to steal data from infected computers and other systems, including 2FA Software and the Tor Browser.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Steal Application Access Token

ID

T1528

Description

Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources. Application access tokens are used to make authorized API requests on behalf of a user or service and are commonly used as a way to access resources in cloud and container-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019) OAuth is one commonly implemented framework that issues tokens to users for access to systems. Adversaries who steal account API tokens in cloud and containerized environments may be able to access data and perform actions with the permissions of these accounts, which can lead to privilege escalation and further compromise of the environment. In Kubernetes environments, processes running inside a container communicate with the Kubernetes API server using service account tokens. If a container is compromised, an attacker may be able to steal the container’s token and thereby gain access to Kubernetes API commands.(Citation: Kubernetes Service Accounts) Token theft can also occur through social engineering, in which case user action may be required to grant access. An application desiring access to cloud-based services or protected APIs can gain entry using OAuth 2.0 through a variety of authorization protocols. An example commonly-used sequence is Microsoft's Authorization Code Grant flow.(Citation: Microsoft Identity Platform Protocols May 2019)(Citation: Microsoft - OAuth Code Authorization flow - June 2019) An OAuth access token enables a third-party application to interact with resources containing user data in the ways requested by the application without obtaining user credentials. Adversaries can leverage OAuth authorization by constructing a malicious

application designed to be granted access to resources with the target user's OAuth token. (Citation: Amnesty OAuth Phishing Attacks, August 2019)(Citation: Trend Micro Pawn Storm OAuth 2017) The adversary will need to complete registration of their application with the authorization server, for example Microsoft Identity Platform using Azure Portal, the Visual Studio IDE, the command-line interface, PowerShell, or REST API calls.(Citation: Microsoft - Azure AD App Registration - May 2019) Then, they can send a [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) to the target user to entice them to grant access to the application. Once the OAuth access token is granted, the application can gain potentially long-term access to features of the user account through [Application Access Token](https://attack.mitre.org/techniques/T1550/001).(Citation: Microsoft - Azure AD Identity Tokens - Aug 2019) Application access tokens may function within a limited lifetime, limiting how long an adversary can utilize the stolen token. However, in some cases, adversaries can also steal application refresh tokens(Citation: Auth0 Understanding Refresh Tokens), allowing them to obtain new access tokens without prompting the user.

Name

Steal Web Session Cookie

ID

T1539

Description

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

(https://attack.mitre.org/techniques/T1550/004) technique to login to the corresponding web application.

Indicator

Name
89.38.135.11
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '89.38.135.11']
Name
116.202.189.41
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix

Pattern

[ipv4-addr:value = '116.202.189.41']

Name

173.251.201.195

Description

CC=US

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.251.201.195']

Name

23.88.45.254

Description

Vidar botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.88.45.254']

Name
5.75.246.163
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.75.246.163']
Name
195.201.34.151
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '195.201.34.151']
Name
www.avisclair.com

Pattern Type
stix
Pattern
[hostname:value = 'www.avisclair.com']
Name
49.12.116.189
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '49.12.116.189']
Name
5.75.209.4
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix

Pattern

[ipv4-addr:value = '5.75.209.4']

Name

157.90.152.131

Description

Vidar botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '157.90.152.131']

Name

189.116.12.49

Description

CC=BR ASN=AS26615 TIM SA

Pattern Type

stix

Pattern

[ipv4-addr:value = '189.116.12.49']

Name
78.47.61.97
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '78.47.61.97']
Name
142.132.204.231
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '142.132.204.231']
Name
65.108.152.136

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.136.152.108.65.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC5IK0gUZ5D7e/yOJkbH0EAHKKiejFRFgypGda+bkffgtqI 2mQC2EFxaT6vCgXKUnIm8E5WiLLBs7fpYKM++Xjvl0K/8NvVm7YijrGe6nyx+UvRWWlTAXs+0J/cFP5st+EBCwu83ND+rZYIFQbhoJqVGH5jzKTvnB4LzOOA93sCTVvy+b2ZI9gf8/o7qedsXEmCgFg1nPdcvzBoDgnFY0Lfd9K9sn1UuR/DJfwtFXpx50kRhaIqsXRNLqXWWLaAk9yGa6/BN3+0JfPm0ntAPcTwTwZF81/GWnnzGKoTfShH4HVrh//DKGpxNmmUpYLNcVunt+sdjy0nzgv0Jd63d+wEz5WN9pUyL0fNH3GD0XYbpxDAKfpPScl91+Hot3lLR7Bb2ufrbtM8jqcmNO2uoVrnI03o/gD0izHU3GUspfYylCSDQ3wvtI1JrCWaETKO2VIE8kIAmjDk6h5YMehPHzOzYSfhXNQzmFkCddz5jgqA23qSdsi66CCqNchhJM2wN+k= Fingerprint: b9:e7:99:00:9f:da:52:21:c2:e6:6c:0a:86:6f:e6:40 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 ``` ---------- **80:** ``` HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 21 Nov 2023 07:07:51 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive ``` ---------- **443:** ``` ``` HEARTBLEED: 2023/11/07 10:28:34 65.108.152.136:443 - ERROR: write tcp 65.108.152.136:443: connection reset by peer ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '65.108.152.136']

Name

95.217.244.44

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.44.244.217.95.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 21 Nov 2023 04:21:54 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive ``` ---------- **8080:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Sec-Websocket-Version: 13 X-Content-Type-Options: nosniff Date: Sat, 11 Nov 2023 01:32:13 GMT Content-Length: 12 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.217.244.44']

Name

168.119.173.77

Description

Vidar botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '168.119.173.77']

Name
94.130.188.233
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '94.130.188.233']
Name
151.34.201.195
Description
CC=IT ASN=AS1267 Wind Tre S.p.A.
Pattern Type
stix
Pattern
[ipv4-addr:value = '151.34.201.195']
Name
116.203.10.96

Description

Vidar botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '116.203.10.96']

Name

join.naxtm.cfd

Pattern Type

stix

Pattern

[hostname:value = 'join.naxtm.cfd']

Name

195.201.251.173

Description

Vidar botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.201.251.173']

Name

49.12.119.148

Description

Vidar botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '49.12.119.148']

Name

195.201.46.42

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.42.46.201.195.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 21 Nov 2023 06:07:52 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.201.46.42']

Name

116.203.6.243

Description

Vidar botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '116.203.6.243']

Name

131.152.90.157

Description

CC=CH ASN=AS559 SWITCH

Pattern Type

stix

Pattern

[ipv4-addr:value = '131.152.90.157']

Name
49.13.94.153
Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '49.13.94.153']
Name
116.203.7.211
Description
Vidar botnet C2 server (confidence level: 80%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '116.203.7.211']
Name
167.235.143.166

Description
Vidar botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '167.235.143.166']

Intrusion-Set

Name
Vidar

Country

Name
Germany

Name
Finland

Malware

Name
Vidar

Hostname

Value
join.naxtm.cfd
www.avisclair.com

IPv4-Addr

Value
49.12.119.148
116.203.10.96
167.235.143.166
23.88.45.254
116.203.7.211
89.38.135.11
116.203.6.243
49.13.94.153
131.152.90.157
157.90.152.131
195.201.34.151
195.201.251.173
95.217.244.44

5.75.209.4
5.75.246.163
195.201.46.42
94.130.188.233
168.119.173.77
65.108.152.136
189.116.12.49
116.202.189.41
49.12.116.189
173.251.201.195
151.34.201.195
78.47.61.97
142.132.204.231

External References

- https://otx.alienvault.com/pulse/6560829a84f4d4c9903e5443
- https://censys.com/tracking-vidar-infrastructure/