Jun 22 2023

NETMANAGEIT

Intelligence Report

Analysis: Aurora Stealer

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Aurora Stealer malware infections have been observed in the manufacturing industry. It's distributed via fake Google Ads for Notepad++ installer. Aurora Stealer gathers sensitive data, including cookies, autofill information, and encrypted passwords from browsers such as Opera, Brave, Mozilla Firefox, Chrome, etc. However, it is worth noting that the stealer does not collect credentials from Mozilla Firefox.

Confidence

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

15 / 100

Attack-Pattern

Name
Credentials from Password Stores
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 that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.
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)). 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) 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)

Name

Gather Victim Host Information

ID

T1592

Description

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts 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)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Name

Drive-by Compromise

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising] (https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

Automated Exfiltration

ID

T1020

Description

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

Name

Screen Capture

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)

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)

Sector

Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.

Indicator

Name

195.123.218.52

Description

ISP: ITL LLC **OS:** None ---------- Hostnames: - vds1152184.hosted-by-itldc.com ---------- Domains: - hosted-by-itldc.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA9TRVaODpQ+B896UB/0XvvM xHZ2Zf/978VdNhUAmvuGLw+6nqja3zOof9D8kfuJNlCP+dT+FqOis4uPxUM6CZg= Fingerprint: 3a:87:53:a1:7b:20:1a:cc:1c:74:51:17:8b:c7:34:f9 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com 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 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 ``` ---------- **2053:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Sec-Websocket-Version: 13 X-Content-Type-Options: nosniff Date: Tue, 20 Jun 2023 08:03:27 GMT Content-Length: 12 ``` ---------- **2087:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Connection: close 400 Bad Request ``` ---------- **8880:** ``` HTTP/1.1 204 No Content date: Thu, 22 Jun 2023 05:03:35 GMT server: uvicorn content-type: application/json ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.123.218.52']

Name

https://www.passcape.com/index.php?section=docsys&cmd=details&id=28#14

Pattern Type

stix

Pattern

[url:value = 'https://www.passcape.com/index.php?section=docsys&cmd=details&id=28#14']

Name

185.106.93.135

Description

CC=RU ASN=AS211409 Shelter LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.106.93.135']

Name

aa349ad45bb48e85b5cd1b55308ae835353859219f28ece9685c8ae552e8e63a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa349ad45bb48e85b5cd1b55308ae835353859219f28ece9685c8ae552e8e63a']

Name

www.passcape.com

Pattern Type

stix

Pattern

[hostname:value = 'www.passcape.com']

Name

185.106.93.245

Description

CC=RU ASN=AS211409 Shelter LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.106.93.245']

Name

5b26c93f2e3d524fc3192082220b2f45d187f86c

Description

Detects the Build/Group IDs if present / detects an unobfuscated AuroraStealer binary; tested on version 22.12.2022 and March 2023 update

Pattern Type

yara

Pattern

rule AuroraStealer { meta: author = "eSentire Threat Intelligence" description = "Detects the Build/Group IDs if present / detects an unobfuscated AuroraStealer binary; tested on version 22.12.2022 and March 2023 update" date = "3/24/2023" strings: $b1 = { 48 8D 0D ?? ?? 04 00 E8 ?? ?? EF FF } $b2 = { 48 8D 0D ?? ?? 05 00 E8 ?? ?? EF FF } $ftp = "FOUND FTP" $go = "Go build ID" $machineid = "MachineGuid" condition: 3 of them }

Name

212.87.204.93

Description

Aurora Stealer CC=US ASN=AS211252 Delis LLC

Pattern Type

stix
Pattern
[ipv4-addr:value = '212.87.204.93']

Malware

Name
Hydraq

Description
[Hydraq](https://attack.mitre.org/software/S0203) is a data-theft trojan first used by [Elderwood](https://attack.mitre.org/groups/G0066) in the 2009 Google intrusion known as Operation Aurora, though variations of this trojan have been used in more recent campaigns by other Chinese actors, possibly including [APT17](https://attack.mitre.org/groups/G0025).(Citation: MicroFocus 9002 Aug 2016)(Citation: Symantec Elderwood Sept 2012)(Citation: Symantec Trojan.Hydraq Jan 2010)(Citation: ASERT Seven Pointed Dagger Aug 2015)(Citation: FireEye DeputyDog 9002 November 2013)(Citation: ProofPoint GoT 9002 Aug 2017)(Citation: FireEye Sunshop Campaign May 2013)(Citation: PaloAlto 3102 Sept 2015)

Name
Vidar

Vulnerability

Name
CVE-2023-27997

StixFile

Value
aa349ad45bb48e85b5cd1b55308ae835353859219f28ece9685c8ae552e8e63a

Hostname

Value
www.passcape.com

IPv4-Addr

Value
185.106.93.245
195.123.218.52
185.106.93.135
212.87.204.93

Url

Value
https://www.passcape.com/index.php?section=docsys&cmd=details&id=28#14

External References

- https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-aurora-stealer
- https://otx.alienvault.com/pulse/64944b41915f5405ef355ef4