Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors

Background

Over the last year Mandiant has been tracking UNC3890, a cluster of activity targeting Israeli shipping, government, energy and healthcare organizations via social engineering lures and a potential watering hole. Mandiant assesses with moderate confidence this actor is linked to Iran, which is notable given the strong focus on shipping and the ongoing naval conflict between Iran and Israel. While we believe this actor is focused on intelligence collection, the collected data may be leveraged to support various activities, from hack-and-leak, to enabling kinetic warfare attacks like those that have plagued the shipping industry in recent years.

Mandiant assesses with moderate confidence that UNC3890 conducts espionage and intelligence collection activity to support multiple Iranian interests and operations. Targeting patterns indicate a strong interest in Israeli entities and organizations of various sectors, including government, shipping, energy and healthcare. We observed several limited technical connections to Iran, such as PDB strings and Farsi language artifacts.

This campaign has been active since at least late 2020, and is still ongoing as of mid-2022, and though it is regional in nature, targeted entities include global companies.

UNC3890 uses at least two unique tools: a backdoor which we named SUGARUSH, and a browser credential stealer, which exfiltrates stolen data via Gmail, Yahoo and Yandex email services that we've named SUGARDUMP. UNC3890 also uses multiple publicly available tools, such as the METASPLOIT framework and NorthStar C2.

In addition, Mandiant discovered UNC3890 operates an inter-connected network of Command-and-Control (C2) servers. The C2 servers host domains and fake login pages spoofing legitimate services such as Office 365, social networks such as LinkedIn and Facebook, as well as fake job offers and fake commercials for AI-based robotic dolls. We observed the C2 servers communicating with multiple targets, as well as with a watering hole that we believe was targeting the Israeli shipping sector, in particular entities that handle and ship sensitive components.

This blog post details the activity of UNC3890, including their proprietary malware, TTPs we have not previously seen deployed by Iran, and the publicly available tools we identified in our investigation. Mandiant continues to track UNC3890 as well as other potentially related clusters of activity by the same threat actor.

Attribution

Mandiant uses the label “UNC” groups – or “uncategorized” groups – to refer to a cluster of intrusion activity that includes observable artifacts, such as adversary infrastructure , tools, and tradecraft that we are not yet ready to give a classification such as TEMP, APT, or FIN (learn more about how Mandiant tracks uncategorized threat actors). Mandiant found no significant connections between UNC3890 and other clusters of activities we currently track, and therefore sees it as a standalone group. However, we identified several connections suggesting the activity is conducted by an Iran-nexus group:

- Usage of Farsi words, as observed in strings left by the developers in the newest version of SUGARDUMP, for example “KHODA” (the Farsi word for “God”) and “yaal” (the Farsi word for a horse’s mane).
- Focused targeting of Israeli entities and organizations, or organizations operating in Israel, consistent with other clusters of activity operated by Iranian threat actors, specifically UNC757.
- Usage of the same PDB path as another Iranian cluster of activity Mandiant tracks as UNC2448 (operated by the Iranian IRGC, according to public sources), publicly referred to in a U.S. government statement from November 17, 2021. Several publications suggested that UNC2448 is linked to APT35/Charming Kitten cluster of activities, which according to several public sources is operated by the Iranian Islamic Revolutionary Guard Corps (IRGC). UNC2448 has been targeting Israeli entities as well, among other countries of interest to Iran.
- Utilization of NorthStar C2 Framework, a C2 framework preferred by other Iranian actors . However, since it is a publicly available framework used by multiple threat actors, we consider this link circumstantial.

Targeting

In late 2021, Mandiant identified UNC3890 targeting Israeli entities and showing interest in various sectors, including government, shipping, energy, aviation and healthcare. Even though the targeting we observed is focused to Israel, some of the entities targeted by UNC3890, especially in the shipping sector, are global companies. Therefore, the potential impact of UNC3890 activity described in this blog may extend beyond Israel. The activity is consistent with historical Iranian interest in these targets. Targeting patterns and lures used by UNC3890 indicate an attempt to disguise their activity as legitimate login activity, legitimate services and social network applications, and technology-related visual content.

Malware Observed

Mandiant observed UNC3890 deploy the following malware families.

Malware Family	Description
SUGARUSH	SUGARUSH is a backdoor written to establish a connection with an embedded C2 and to execute CMD commands.
SUGARDUMP	SUGARDUMP is a credential harvesting utility, capable of password collection from Chromium-based browsers.
SUGARDUMP SMTP-based	A more advanced version of SUGARDUMP, exfiltrating the stolen credentials via Gmail, Yahoo and Yandex email addresses. Uses a commercial for robotic dolls as a lure.
SUGARDUMP HTTP-based	The newest version of SUGARDUMP, exfiltrating the stolen credentials to a dedicated server over HTTP. Uses a fake job offer as a lure.

METASPLOIT	METASPLOIT is a penetration testing software, often abused by malicious threat actors.
UNICORN	UNICORN is a publicly available tool for conducting a PowerShell downgrade attack and to inject a shellcode into memory.
NORTHSTAR C2	NORTHSTAR C2 is an open-source C2 framework developed for penetration testing and red teaming.

Outlook and Implications

UNC3890 has been operating since at least late 2020. Their focused targeting poses a threat to Israel-based organizations and entities, particularly those affiliated with the government, shipping, energy, aviation and healthcare sectors. While we are not aware of targeting outside Israel, it is possible such targeting has occurred, or will occur. UNC3890 utilization of legitimate or publicly available tools, in addition to their unique exfiltration method using Gmail, Yahoo and Yandex email addresses, may reflect their efforts to evade detection and to bypass heuristics or network-based security measures.

UNC3890 Attack Lifecycle

Establish Foothold

While Mandiant primarily identified post-exploitation implants utilized by UNC3890, there are some findings that shed light about their initial access methodologies. Mandiant identified UNC3890 potentially used the following initial access vectors:

- **Watering holes** – Mandiant identified a potential watering hole hosted on a login page of a legitimate Israeli shipping company, which was likely compromised by UNC3890. The watering hole was active at least until November 2021, and upon entering the legitimate login page, the user would be sending a POST request with preliminary data about the logged user to an attacker controlled non-ASCII Punycode domain (lirıkedin[.]com, interpreted as xn--lirkedin-vkb[.]com).

The URL structure of the POST request:

hxxps[:]//xn--lirkedin-vkb[.]com/object[.]php?browser=<user_browser>&ip=<user_ip>

When we inspected the watering hole, it was already inactive, but it was most likely used to target clients and users of that Israeli shipping company, in particular, one's shipping or handling heat-sensitive cargo (based on the nature of the compromised website). We have an additional indication of an attempted targeting of another major Israeli shipping company by UNC3890, which is consistent with the watering hole.

- **Credentials harvesting by masquerading as legitimate services** – we uncovered several domains resolving to UNC3890's C2 servers. Some of the domains were masquerading as legitimate services and entities, as can be observed in the table below. UNC3890 may have used these domains to harvest credentials to legitimate services, to send phishing lures, or to overall mask their activity and blend in with expected network traffic.

It should be noted that many of these domains were hosted on the same infrastructure used by UNC3890, but date back to late 2020, which is before we can corroborate UNC3890 has been active.

UNC3890 Domain	Legitimate entity/service	Comment
lirıkedin[.]com (xn--lirkedin-vkb[.]com)	LinkedIn	C2 domain of watering hole
pfizerpoll[.]com	Pfizer	Hosted a fake Citrix login page
rnfacebook[.]com	Facebook	
office365update[.]live	Office 365	
fileupload[.]shop	n/a	
celebritylife[.]news	n/a	
naturaldolls[.]store xxx-doll[.]com	Part of a robotic dolls commercial which was used to harvest credentials and as a lure to install SUGARDUMP	Hosts a fake Outlook login page

In addition, we identified an UNC3890 server that hosted several ZIP files containing scraped contents of Facebook and Instagram accounts of legitimate individuals. It is possible they were targeted by UNC3890, or used as lures in a social engineering effort.

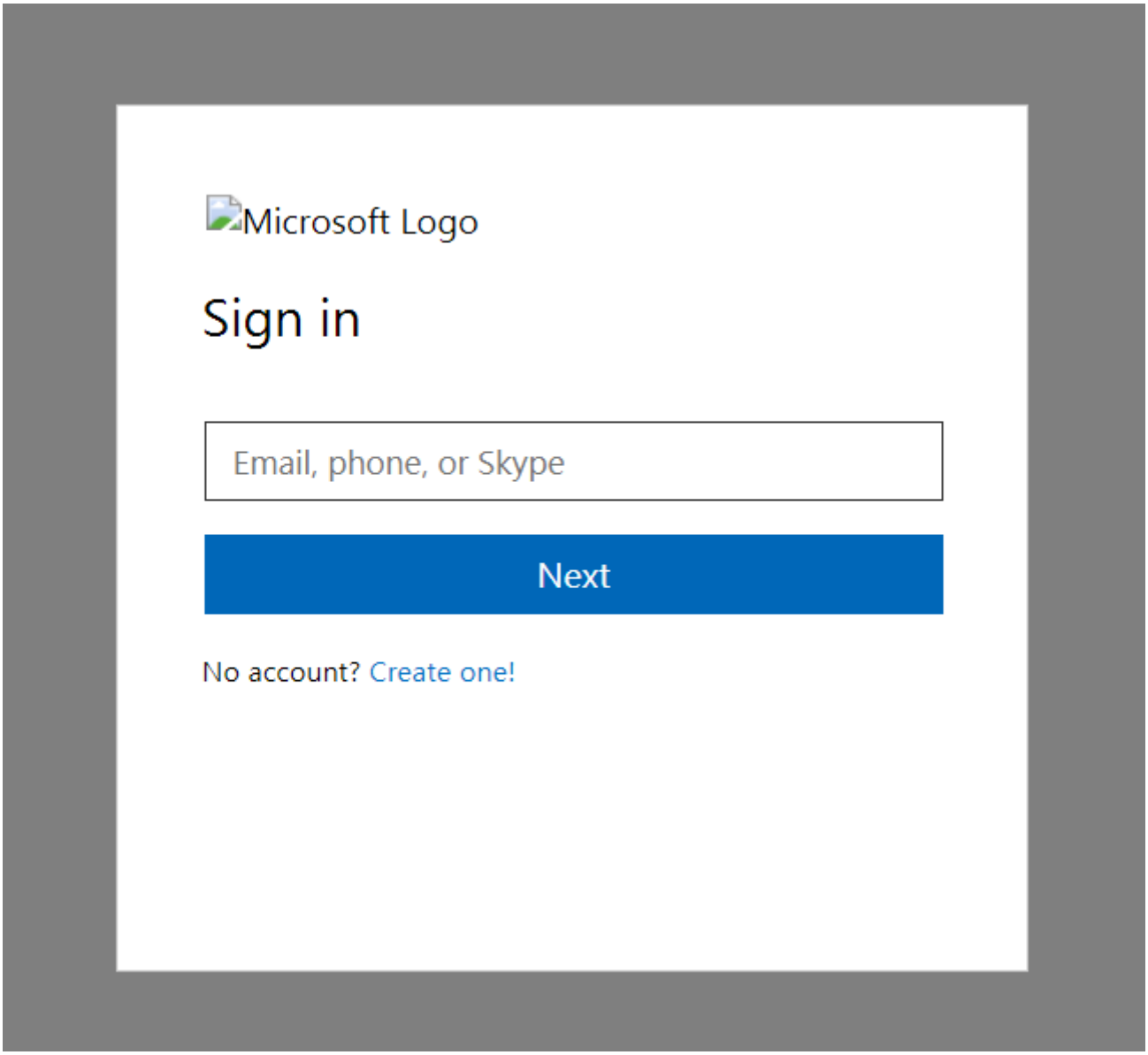

Figure 1: A fake Outlook Web Access login page hosted on UNC3890's domain naturaldolls[.]store

Fake job offers, potentially as part of a phishing or watering hole campaign – we observed UNC3890 utilize a .xls lure file designed as a fake job offer (MD5: 639f83fa4265ddbb43e85b763fe3dbac) which installs SUGARDUMP, a credential harvesting tool. The job offer was for a software developer position in LexisNexis, a company offering a data analytics solution.

Title

Java Architect
Full Stack Development

Description

LexisNexis has a Converged Identity and Access Management (IAM) Product – Compact Identity (CI) which provides SSO, Password Management, Provisioning/de-provisioning and Access Governance feature to its customers. Current SSO module support SAML protocol, with which customer can integrate SAML-supported applications with CI for Authentication and SSO. CI supports multi-tenant cloud deployment (on Ilantus/Partner AWS Cloud) as well as on-prem deployment (on customer premise)

We are looking for a Java Architect who understand the product in detail and guide/assist the engineering team to deliver fixes, enhancements and new features

Your Recommendations

Detailed Requirements

Review & understand the current architecture of Compact Identity (CI)
- Platform components
- CI modules and integration between these modules
- Data Repositories
- Provide recommendation on addressing design flaws (if any) and improving scalability and security on CI application
- Guide & assist team in developing these recommendations

Your Requirements

Figure 2: A fake LexisNexis job offer which drops SUGARDUMP

- **Fake commercials for AI-based robotic dolls** – one of UNC3890's most recent endeavor to target victims includes the usage of a video commercial for AI-based robotic dolls, used as a lure to deliver SUGARDUMP. In addition, we observed UNC3890 usage of domains with similar themes such as naturaldolls[.]store (hosting a fake Outlook login page) and xxx-doll[.]com. In addition, UNC3890 infrastructure hosted a fake page for the alleged purchasing of robotic dolls, redirecting victims to an attacker controlled infrastructure.

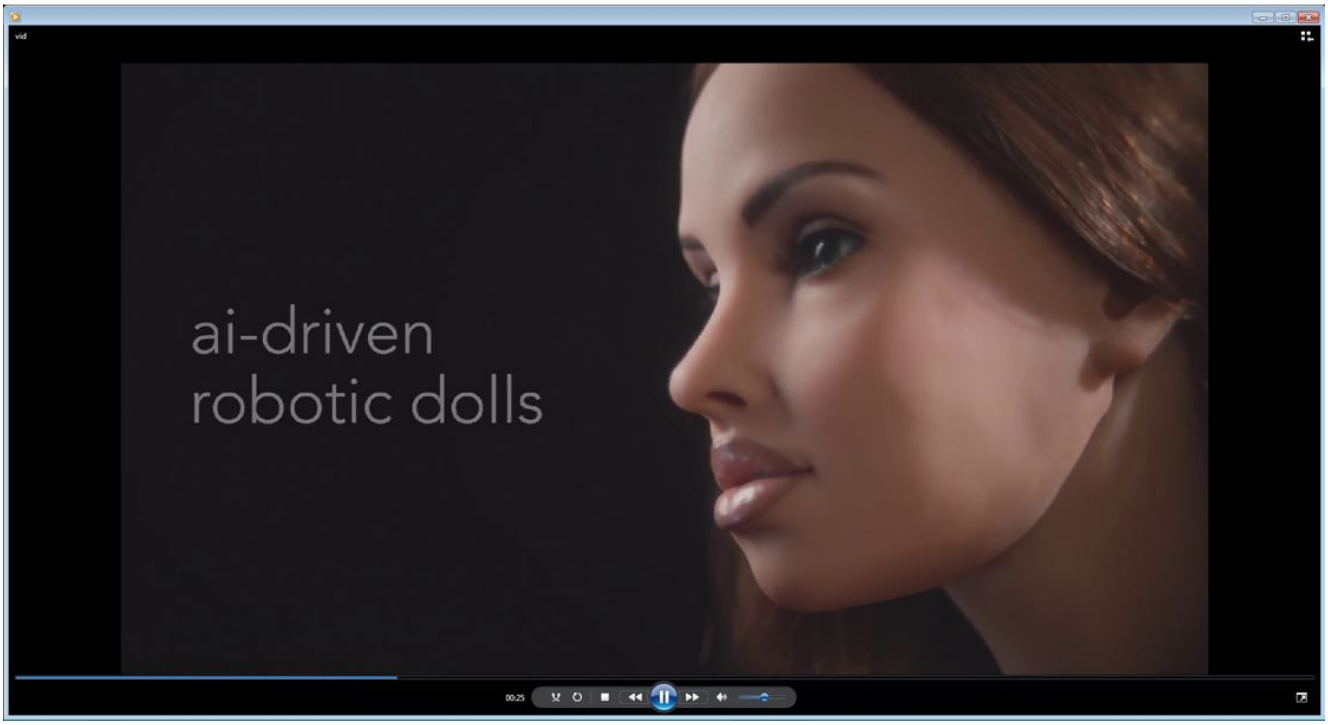

Figure 3: a screenshot taken from the social engineering video played when SUGARDUMP executes


```
  <!-- starapps_scripts_start -->
<!-- This code is automatically managed by StarApps Studio -->
<!-- Please contact support@starapps.studio for any help -->
<script type="text/javascript" src="https://cdn.starapps.studio/apps/vdk/[redacted]dollscom/script-1599202993.js?shop=[redacted]dollscom.myshopify.com"
<!-- starapps_scripts_end -->
```

Figure 4: HTML page hosted on UNC3890 infrastructure, with references to purchasing of robotic dolls

Post-Exploitation: From Credentials Harvesting to Full Access and Control

After gaining initial access, UNC3890 utilizes a broad toolset to access and control the victim's environment. In this sector we will focus on the analysis of two of UNC3890's proprietary tools we identified in our investigation: the SUGARUSH backdoor, and the SUGARDUMP credential harvesting tool. We will also provide a brief analysis of the public tools utilized by UNC3890.

Most of the tools were available for download directly from UNC3890 controlled infrastructure, indicating they may have been served as 1st stage implants. Alternatively, they may have been used as 2nd stages (or later), but UNC3890 may have misconfigured their infrastructure, making it publicly accessible.

SUGARUSH Analysis: A Small But Efficient Backdoor

SUGARUSH is a small custom backdoor that establishes a reverse shell over TCP to a hardcoded C&C address.

Upon first execution, SUGARUSH will create a new service called “Service1”. Subsequently, SUGARUSH creates a logging folder called “Logs”, and stores it under its current execution path. A new folder named “ServiceLog” is created in the “Logs” folder, and a new log file is written with the message “Service is started at <current_date>”. The name of the log files is the current date of the infected machine.

SUGARUSH will then check for internet connectivity of the host and will create a log file indicating the result with message “You are online at <current_date>” or “You are offline at <current_date>”. If the attempt for internet connection is successful, SUGARUSH will establish a new TCP connection to an embedded C&C address via port 4585.

SUGARUSH then waits to receive an answer from the C2 which will be interpreted as a CMD command for execution.

SUGARUSH Samples:

- 37bdb9ea33b2fe621587c887f6fb2989
- 3f045ebb014d859a4e7d15a4cf827957
- a7a2d6a533b913bc50d14e91bcf6c716
- d528e96271e791fab5818c01d4bc139f

SUGARDUMP Analysis: A Browser Credential Harvesting Tool

SUGARDUMP is a small custom utility used for harvesting credentials from Chrome, Opera and Edge Chromium browsers.

When executed SUGARDUMP will access the following paths:

- %AppData%\\Google\\Chrome\\User Data
- %AppData&\\Opera Software\\Opera Stable
- %AppData%\\Microsoft\\Edge\\User Data

Out of each path SUGARDUMP will attempt collect specific folders:

- \\Default\\Login Data
- \\Login Data
- Any other folder that has the string “Profile” in its name.

Afterwards, SUGARDUMP will extract all of the available usernames and passwords from these folders.

The collected information is subsequently stored in the following format:

```
URL: <login_URL>
Username: <user_name>
Password: <password>
Application: <app_name>
==========
```

Figure 5: SUGARDUMP exfiltrated data format

We observed several versions of SUGARDUMP:

- SUGARDUMP first known version, dated to early 2021. This early version stores the credentials without exfiltrating them. It is possible it was an unfinished version, or that UNC3890 used other tools and/or manually connect to the victim to exfiltrate the stolen credentials.
- SUGARDUMP using SMTP-based communication, dated to late 2021-early 2022. This version utilizes Yahoo, Yandex and Gmail addresses for exfiltration, and uses a commercial AI-driven robotic dolls as a lure.
- SUGARDUMP using HTTPs-based communication, dated to April 2022. This version uses a fake NexisLexis job offer as a lure.

SUGARDUMP first known version – dated to early 2021, we observed two variants of this version: the first one saves the stolen credentials under in a .txt file under the path: "C:\\Users\\User\\Desktop\\test2.txt". The second variant prints the stolen credentials as a CMD output.

We observed two PDB paths contained in SUGARDUMP samples:

- **C:\Users\User\source\repos**\passrecover\passrecover\obj\Release\passrecover.pdb – we observed a similar PDB path (the part in **bold**) used in a toolset (for example, MD5: 69b2ab3369823032991d4b306a170425) by UNC2448, an actor affiliated with Iran, which was mentioned in a U.S. government statement in November 17, 2021. Since this is a rather generic PDB path, this similarity may be circumstantial, and we consider it a weak link.
- C:\Users\User\Desktop\sourc\Chrome-Password-Recovery-master\Chrome-Password-Recovery-master\obj\Debug\ChromeRecovery.pdb

SUGARDUMP using SMTP for C2 communication – dated to late 2021-early 2022. This variant was downloaded from a known UNC3890 C2 (URL: hxxp://128.199.6[.]246/3-Video-VLC.exe), and is a slightly more advanced version with similar credential harvesting functionality.

The downloaded file "3-Video-VLC.exe" (MD5: ae0a16b6feddd53d1d52ff50d85a42d5) is a Windows installer which, upon execution, drops and executes two files under the path %AppData%\\Roaming\\:

1. CrashReporter.exe (MD5: 084ad50044d6650f9ed314e99351a608) – a browser credential harvesting tool (SUGARDUMP).
2. RealDo1080.mp4 (MD5: d8fb3b6f5681cf5eec2b89be9b632b05) – a social engineering video, played using Windows Media Player while CrashReporter.exe is executed. The video contains a commercial for AI-driven robotic dolls.

Upon first execution, CrashReporter.exe (SUGARDUMP) attempts to locate the folder: *%AppData%**Microsoft**Edge**User Data**CrashPad*\\

If it wasn't found it will search for folder: *%AppData%**Microsoft**Internet Explorer**TabRoaming*\\

If the latter folder is not found as well, the malware proceeds to create it. The malware will then copy itself into "TabRoaming" folder again under the name "CrashReporter.exe". Subsequently, a scheduled task is created, which ensures the persistence of this version of SUGARDUMP:

- In Windows 7 the scheduled task is called: "MicrosoftInternetExplorerCrashRepoeterTaskMachineUA", and contains the description *"Keep your Microsoft software without any bugs. If this task is disabled or stopped, your Microsoft software may not work properly, meaning bugs that may arise cannot be fixed and features may not work."*
- In other Windows OS versions the scheduled task is called: "MicrosoftEdgeCrashRepoeterTaskMachineUA", and contains the description *"Keep your Microsoft software without any bugs. If this task is disabled or stopped, your Edge browser may not work properly, meaning bugs that may arise cannot be fixed and features may not work."*

The scheduled task is configured to execute CrashReporter.exe during user logon.

The malware then attempts to connect to "smtp.yandex.com" and "smtp.mail.yahoo.com" via port 587. If the attempt is successful, the malware starts to harvest bowser related information on the host.

This version of SUGARDUMP harvest credentials from the following browsers:

- Firefox (added functionality with relation to the previous version)
- Chrome
- Opera
- Edge

For each browser the malware attempts to extract login credentials from the following paths:

- %Appdata%\\Mozilla\\Firefox\\Profiles
- %Appdata%\\Google\\Chrome\\User Data
- %Appdata%\\Opera Software\\Opera Stable
- %Appdata%\\Microsoft\\Edge\\User Data

This version of SUGARDUMP also extracts the browser's version, browsing history, bookmarks, and cookies.

The extracted data structure looks as follows:

```
<browser_name> Informations - Version = <browser_version>

<<<<<<<< ------ Passwords Total: <number_of_extracted_passwords> --------- >>>>>>>>

For each extracted password:
Username = <user_name>, Password = <password>, Url = <login_url>

<<<<<<<< ------ Historys Total: <number_of_browsing_history_entries_collectd> ---------
>>>>>>>>

For each entry:
Url = <url>, Count = <number_of_visits>

<<<<<<<< ------ Bookmarks Total: <number_of_collected_bookmarks> --------- >>>>>>>>

For each bookmark:
Url = <bookmark_url>, Title = <name_of_bookmark>, DateCreated = <bookmark_creation_date>

<<<<<<<< ------ Cookies Total: <number_of_colleted_cookies> --------- >>>>>>>>

For each cookie:
Host = <cookie_hostname>, CookieName = <cookie_name>, CookieValue = <cookie_value>,
ExpireTime = <cookie_expire_date>, CreateTime = <cookie_creation_date>, LastAccess =
<last_access_time>, Path = <path>, IsSecure = <is_secure>
```

Figure 6: Exfiltrated data format of SUGARDUMP

The collected data is subsequently encoded using base64 and stored under: *%<malware_execution_folder>%\\CrashLog.txt*

The malware will then send the file “CrashLog.txt” via email, by connecting and sending it from one of the two following email addresses:

- john.macperson2021@yandex[.]com
- john.macperson2021@yahoo[.]com

The email is sent to one of these four email addresses:

- john.macperson2021@yandex[.]com
- john.macperson2021@yahoo[.]com
- john.macperson2021@gmail[.]com
- john.macperson@protonmail[.]com

The subject for each message would be “VLC Player”, with “CrashLog.txt” attached.

If SUGARDUMP fails to send the message, it creates a new file under: *%<malware_current_execution_path>%\\CrashLogName.txt*, and writes to the file the error details. "CrashLogName.txt" is also sent via email, using the same method mentioned above. Afterwards, the malware terminates its execution.

SUGARDUMP using HTTP for C2 communication – dated to April 2022, this version sends the stolen credentials to an UNC3890 C2 server (144.202.123[.]248:80). We observed this version dropped by a .xls file which contains a fake job offer to a software developer position in NexisLexis, a data analytics platform (MD5: 639f83fa4265ddbb43e85b763fe3dbac).

The .xls file contains a Macro, which upon enablement attempts to execute an embedded PE file using RunDLL (MD5: e125ed072fc4529687d98cf4c62e283e). The PE file is the newest version of SUGARDUMP we observed so far.

Like previous versions, this version of SUGARDUMP harvests credentials from Chromium-based browsers Chrome, Opera and Edge. The data is saved in a new file under *%TEMP%\\DebugLogWindowsDefender.txt*.

The collected data is subsequently encrypted using AES encryption using Cipher Block Chaining (CBC) mode. The encryption key is the Sha256 of an embedded password: “1qazXSW@3edc123456be name KHODA 110 !!)1qazXSW@3edc”. The word “KHODA” means god in Farsi.

After the encryption process, the data is also encoded using Base64, and subsequently sent over HTTP to an UNC3890 C2 server: 144.202.123[.]248:80.

The .NET project for this version of SUGARDUMP was named "yaal", which is the Farsi word for a horse’s mane. This, along with the use of the word “KHODA” in SUGARDUMP’s encryption key, may strengthen the possibility that the developers of SUGARDUMP are Farsi speakers.

SUGARDUMP Samples:

- f362a2d9194a09eaca7d2fa04d89e1e5 – early version
- 08dc5c2af21ecee6f2b25ebdd02a9079 – early version
- ae0a16b6feddd53d1d52ff50d85a42d5 – SMTP-based version
- e125ed072fc4529687d98cf4c62e283e – HTTP-based version

MITRE ATT&CK Techniques

Resource Development
Obtain Capabilities (T1588)

- **Tool** (T1588.002)

Develop Capabilities (T1587)

- **Malware** (T1587.001)

Initial Access
Phishing (T1566)

- **Phishing: Spearphishing Link** (T1566.002)

Trusted Relationship (T1199)
Valid Accounts (T1078)

Execution
Scheduled Task/Job (T1053)

- **Scheduled Task** (T1053.005)

Command and Scripting Interpreter (T1059)

System Services (T1569)

- **Service Execution** (T1569.002)

User Execution (T1204)

- **Malicious File** (T1204.002)

Persistence
Scheduled Task/Job (T1053)

- **Scheduled Task** (T1053.005)

Create or Modify System Process (T1543)

- **Windows Service** (T1543.003)

Privilege Escalation
Scheduled Task/Job (T1053)

- **Scheduled Task** (T1053.005)

Credential Access
Credentials from Password Stores (T1555)

- **Credentials from Web Browsers** (T1555.003)

Input Capture (T1056)

Command and Control
Ingress Tool Transfer (T1105)

Remote Access Software (T1219)

Application Layer Protocol (T1071)

- **Web Protocols** (T1071.001)

Protocol Tunneling (T1572)

Web Service (T1102)

- **Bidirectional Communication** (T1102.002)

Exfiltration

Exfiltration Over C2 Channel (T1041)

Exfiltration Over Web Service (T1567)

Indicators of Compromise

Type	Value	Description
MD5	f362a2d9194a09eaca7d2fa04d89e1e5	SUGARDUMP early ver.
MD5	08dc5c2af21ecee6f2b25ebdd02a9079	SUGARDUMP early ver.
MD5	ae0a16b6feddd53d1d52ff50d85a42d5	SUGARDUMP SMTP dropper
MD5	084ad50044d6650f9ed314e99351a608	SUGARDUMP SMTP
MD5	d8fb3b6f5681cf5eec2b89be9b632b05	SUGARDUMP SMTP lure video
MD5	639f83fa4265ddbb43e85b763fe3dbac	SUGARDUMP HTTP lure file
MD5	e125ed072fc4529687d98cf4c62e283e	SUGARDUMP HTTP
MD5	37bdb9ea33b2fe621587c887f6fb2989	SUGARUSH
MD5	3f045ebb014d859a4e7d15a4cf827957	SUGARUSH
MD5	a7a2d6a533b913bc50d14e91bcf6c716	SUGARUSH
MD5	d528e96271e791fab5818c01d4bc139f	SUGARUSH
MD5	d5671df2af6478ac108e92ba596d5557	PowerShell downloader
MD5	fcc09a4262b9ca899ba08150e287caa9	METASPLOIT payload
MD5	d47bbec805c00a549ab364d20a884519	METASPLOIT payload
MD5	6dbd612bbc7986cf8beb9984b473330a	METASPLOIT payload
MD5	3b2a719ffb12a291acbfe9056daf52a7	METASPLOIT payload
MD5	f97c0f19e84c79e9423b4420531f5a25	METASPLOIT payload
MD5	f538cb2e584116a586a50d607d517cfd	UNICORN
MD5	532f5c8a85b706ccc317b9d4158014bf	PowerSherll TCP ReverseShell
MD5	9c8788e7ae87ae4f46bfe5ba7b7aa938	.NET executable that dropps and executes ReverseShell
MD5	2fe42c52826787e24ea81c17303484f9	NORTHSTAR C2 Stager
MD5	2a09c5d85667334d9accbd0e06ae9418	PowerShell downloader
MD5	c5116a9818dcd48b8e9fb1ddf022df29	PowerShell downloader
IP	143.110.155[.]195	NorthStar C2 server
IP	128.199.6[.]246	Malware/Tools Hosting, Watering Hole C2, Fake Login Pages Hosting
IP	161.35.123[.]176	SUGARUSH C2, Reverse Shell C2, Malicious Domains Hosting
IP	104.237.155[.]129	C2 server
IP	146.185.219[.]88	C2 server
IP	159.223.164[.]185	C2 server
IP	144.202.123[.]248	C2 server
IP	185.170.215[.]170	Malicious Domain Hosting
Domain	lirıkedin[.]com (xn--lirkedin-vkb[.]com)	Fake domain
Domain	pfizerpoll[.]com	Fake domain
Domain	office365update[.]live	Fake domain
Domain	celebritylife[.]news	Fake domain
Domain	rnfacebook[.]com	Fake domain
Domain	fileupload[.]shop	Fake domain

Domain naturaldolls[.]store	Domain
Domain xxx-doll[.]com	Domain
Domain aspiremovecentraldays[.]net (suspect)	Domain