Author: Jack Fitzgerald

LetsDefend

Official Incident Report

Date: Dec, 27, 2023, 11:22 PM

Event ID: 212

Rule Name: SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected

Table of Contents

Alert Details

Severity: Medium

Type: Data Leakage

Hostname: Arthur

Ip Address: 172.16.17.72

Process Name: EmailDownloader.exe

Process Path: C:\Users\LetsDefend\Downloads\EmailDownloader.exe

Parent Process: C:\Windows\Explorer.EXE

Command Line: C:\Users\LetsDefend\Downloads\EmailDownloader.exe

File Hash: cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa

Trigger Reason: Unusual or suspicious patterns of behavior linked to the hash have been identified, indicating potential malicious intent.

Device Action: Allowed

Based on the information provided in the alert, it appears that a suspicious hash has been identified on host **172.16.17.72**. The alert is triggered by rule SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

As of August 2022, APT35 aka Charming Kitten was observed using a new tool called Hyperscrape to extract emails from their victims' mailboxes.

We need to investigate the activity associated with the **EmailDownloader.exe** process on the host named **Arthur** with IP address **172.16.17.72**. Pay close attention to the command line and file hash provided, as they indicate unusual behavior that may suggest data exfiltration activities. Monitor network traffic and review system logs for any additional signs of malicious intent or unauthorized data transfers originating from this host.

Check for related hashes from previous attacks by the APT Group.

Analysis

We can begin the analysis by analyzing the file hash **cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa** using **VirusTotal**.

https://www.virustotal.com/gui/file/cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa

51/71 security vendors flagged this file as malicious

We discovered that the file contacts URL **http://136.243.108.14/index.php?Ck=OK**.

Next, we can analyse the attacker's IP address **173.209.51.54**.

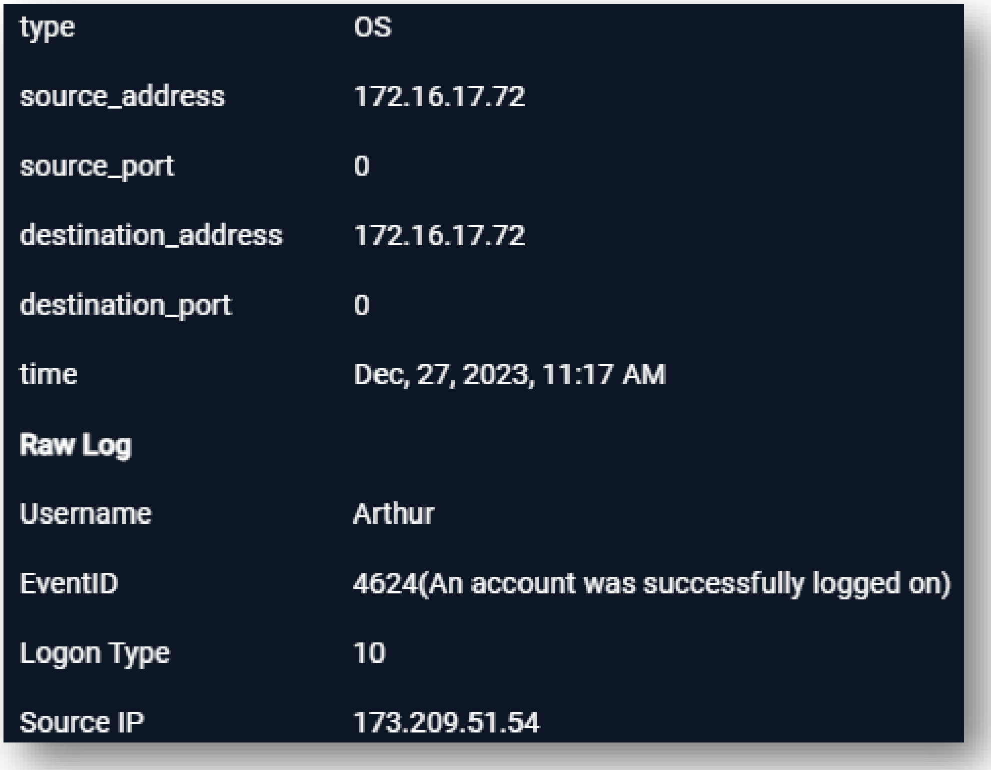
https://www.virustotal.com/gui/ip-address/173.209.51.54

2/95 security vendors flagged this IP address as malicious

The attacker's IP is malicious, also mentioned in a google blog threat analysis report of a new Iranian apt data extraction tool (HYPERSCRAPE).

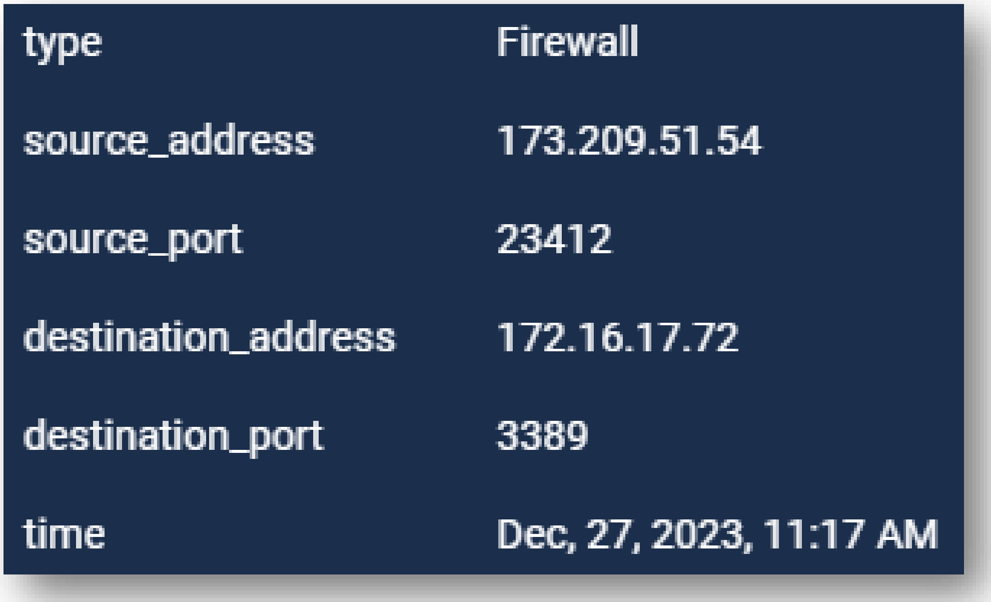
Next, we can analyse the logs found for this incident, where we identify 3 logs.

The first log, we see an actor from **173.209.51.5**4 (malicious IP) successfully logged on to Arthur's machine **172.16.17.72** using RDP (logon type 10 indicates remote logon).



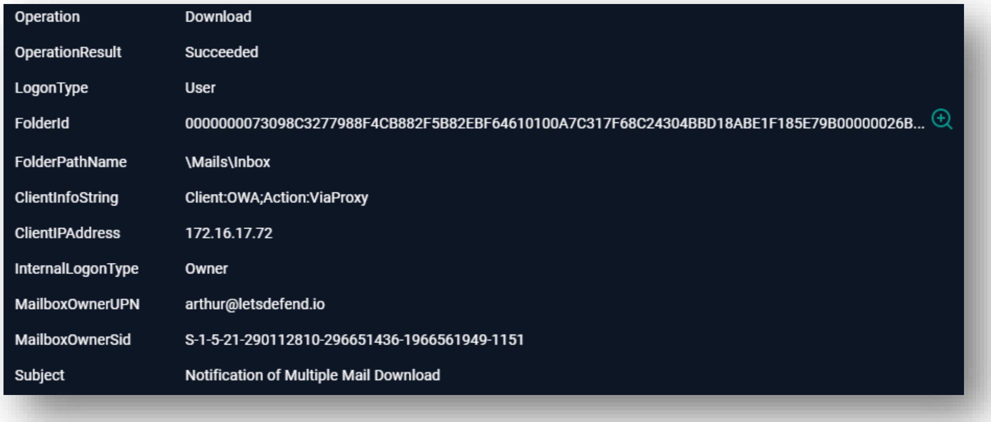
type	OS
source_address	172.16.17.72
source_port	0
destination_address	172.16.17.72
destination_port	0
time	Dec, 27, 2023, 11:17 AM
Raw Log	
Username	Arthur
EventID	4624(An account was successfully logged on)
Logon Type	10
Source IP	173.209.51.54

The second log, we see the firewall detecting that the malicious IP has remotely logged on to Arthur's machine through port 3389, using RDP protocol.



type	Firewall
source_address	173.209.51.54
source_port	23412
destination_address	172.16.17.72
destination_port	3389
time	Dec, 27, 2023, 11:17 AM

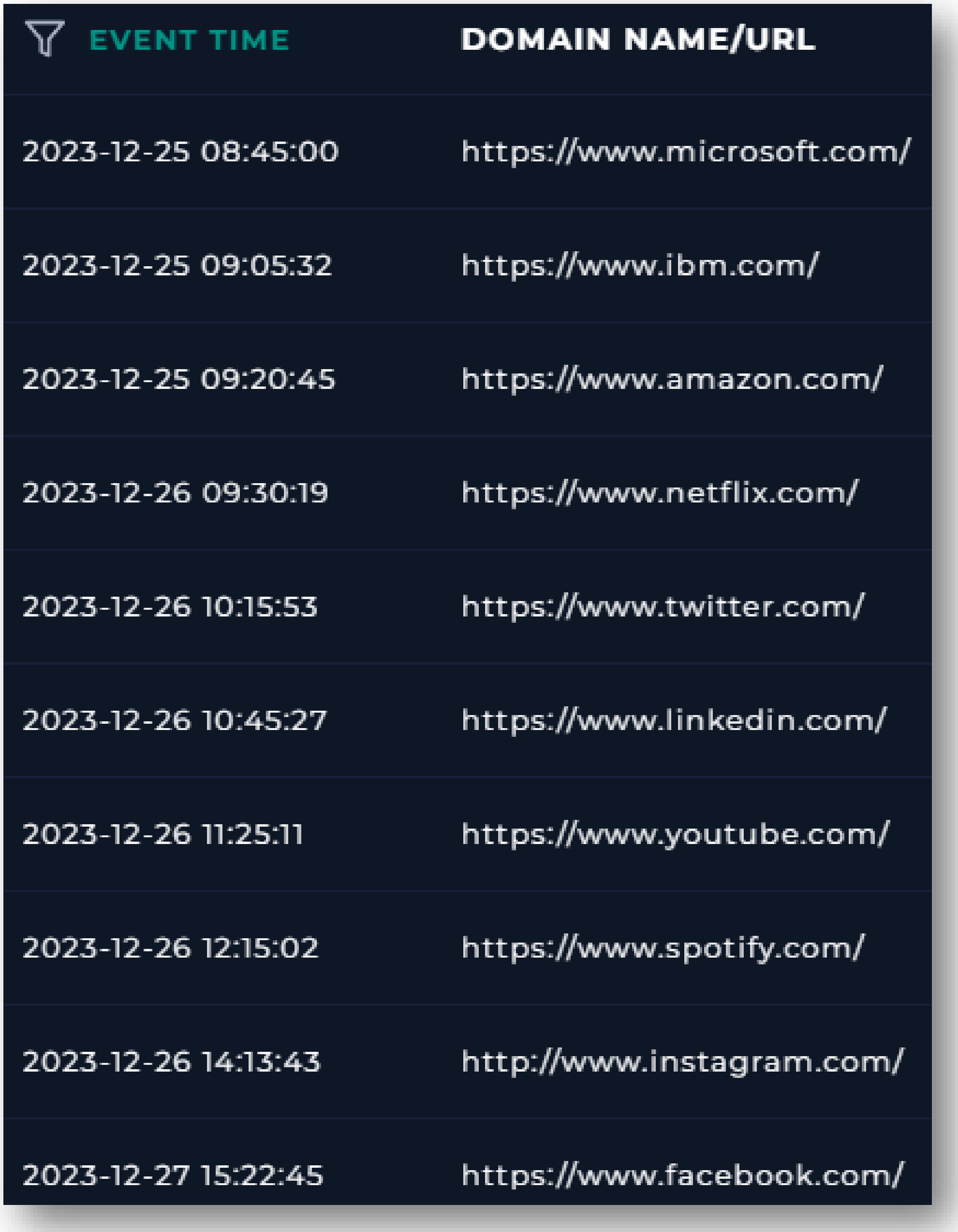
The third log, we see an **email** was sent to Arthur's machine notifying him of the fact that multiple emails of his have been downloaded. This is an indication that HYPERSCRAPE malware has downloaded the user's emails, confirming **data exfiltration** activities.



Operation	Download
OperationResult	Succeeded
LogonType	User
FolderId	0000000073098C3277988F4CB882F5B82EBF64610100A7C317F68C24304BBD18ABE1F185E79B00000026B...
FolderPathName	\Mails\Inbox
ClientInfoString	Client:OWA;Action:ViaProxy
ClientIPAddress	172.16.17.72
InternalLogonType	Owner
MailboxOwnerUPN	arthur@letsdefend.io
MailboxOwnerSid	S-1-5-21-290112810-296651436-1966561949-1151
Subject	Notification of Multiple Mail Download

HYPERSCRAPE is run on the attacker's own machine, where the attacker will remotely logon to the victim's machine using a remote logon protocol (such as RDP in this case), using previously acquired credentials.

Given the user activity prior to the attack, all the URLs Arthur is accessing are HTTPS, which are secure. However, the last URL that Arthur accesses prior to the attack is HTTP, which is NOT secure. This indicates that Arthur's login credentials that he entered when logging into **instagram.com** were leaked from this source.



EVENT TIME	DOMAIN NAME/URL
2023-12-25 08:45:00	https://www.microsoft.com/
2023-12-25 09:05:32	https://www.ibm.com/
2023-12-25 09:20:45	https://www.amazon.com/
2023-12-26 09:30:19	https://www.netflix.com/
2023-12-26 10:15:53	https://www.twitter.com/
2023-12-26 10:45:27	https://www.linkedin.com/
2023-12-26 11:25:11	https://www.youtube.com/
2023-12-26 12:15:02	https://www.spotify.com/
2023-12-26 14:13:43	http://www.instagram.com/
2023-12-27 15:22:45	https://www.facebook.com/

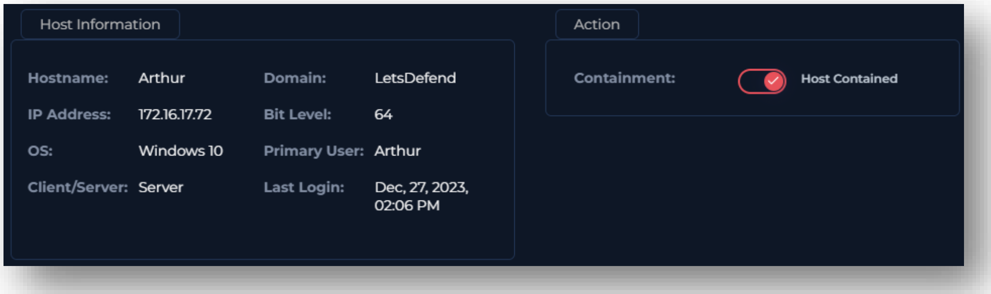
This allows the attacker to use Arthur's Instagram logon credentials on his Windows 10 machine, via RDP on port 3389, where the attacker was successful in logging in, allowing the use of HYPERSCRAPE to download Arthur's emails.

These are the following HYPERSCRAPE Indicators:

- C2
- 136.243.108.14
- 173.209.51.54
- HYPERSCRAPE binaries
- 03d0e7ad4c12273a42e4c95d854408b98b0cf5ecf5f8c5ce05b24729b6f4e369
- 35a485972282b7e0e8e3a7a9cbf86ad93856378fd96cc8e230be5099c4b89208
- 5afc59cd2b39f988733eba427c8cf6e48bd2e9dc3d48a4db550655efe0dca798
- 6dc0600de00ba6574488472d5c48aa2a7b23a74ff1378d8aee6a93ea0ee7364f
- 767bd025c8e7d36f64dbd636ce0f29e873d1e3ca415d5ad49053a68918fe89f4
- 977f0053690684eb509da27d5eec2a560311c084a4a133191ef387e110e8b85f
- ac8e59e8abeacf0885b451833726be3e8e2d9c88d21f27b16ebe00f00c1409e6
- cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa
- Microsoft Live DLL
- 1a831a79a932edd0398f46336712eff90ebb5164a189ef38c4dacc64ba84fe23
- PDB
- E:\Working\Projects\EmailDownloader\EmailDownloaderCookieMode\EmailDownloader\obj\Debug\EmailDownloader.pdb
- E:\Working\Projects\EmailDownloader\EmailDownloaderCookieMode\Mahdi\LiveLib\obj\Release\LiveLib.pdb

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



Host Information

Hostname:	Arthur	Domain:	LetsDefend
IP Address:	172.16.17.72	Bit Level:	64
OS:	Windows 10	Primary User:	Arthur
Client/Server:	Server	Last Login:	Dec, 27, 2023, 02:06 PM

Action

Containment: Host Contained

Summary

The incident involves a compromised system named **Arthur** with an IP address of **172.16.17.72**. The alert was triggered by the identification of a suspicious hash on the host, based on the rule SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected.

Upon further analysis, it was discovered that **cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa** was an indicator of Hyperscrape, which extracts emails from their victims' mailboxes.

The attacker runs HYPERSCRAPE on their own machine to download victims' inboxes using previously acquired credentials; the attacker's mail download was successful in ViaProxy. Users should be more careful with what sites they visit, ensuring the websites they access use HTTPS Protocol.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- HyperScrape relies on valid credentials or session tokens to download victim mailbox data; account credentials may have been compromised earlier (phishing, MFA fatigue, social engineering)

- HyperScrape accesses mailbox contents in bulk, missing or weak detection for abnormal mailbox exports, mass API reads, or message download spikes

- External content loading is a major blind spot

- Patch cycles must include emergent 0-days, not only scheduled updates

Remediation Actions

- Force password resets for affected accounts, revoke all active sessions and refresh tokens, rotate privileged credentials

- Educate users about MFA fatigue attacks, highly targeted spear-phishing used by APT35, social engineering from fake interview/credential-harvesting sites

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Defense Evasion	T1070.004 - Indicator Removal: File Deletion
Collection	T1114.002 - Email Collection: Remote Email Collection
Command and Control	T1041 - Exfiltration Over C2 Channel

Artifacts

Value	Comment	Type
http://www.instagram.com/	Leaked credentials (HTTP - Not Secure)	URL Address
http://136.243.108.14/index.php?Ck=OK	MD5 Hash contacted this URL	URL Address
173.209.51.54	Attacker's IP Address - Logon through RDP	IP Address
136.243.108.14	HYPERSCRAPE Indicator	IP Address
cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa	EmailDownloader.exe	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 212