Managed XDR Investigation of Ducktail in Trend Micro Vision One

trendmicro.com/en_us/research/23/e/managed-xdr-investigation-of-ducktail-in-trend-micro-vision-one.html

May 9, 2023

Malware

Managed XDR Investigation of Ducktail in Trend Vision One™

The Trend Micro Managed XDR team investigated several Ducktail-related web browser credential dumping incidents involving different customers.

By: Khristian Joseph Morales, Gilbert Sison May 09, 2023 Read time: (words)

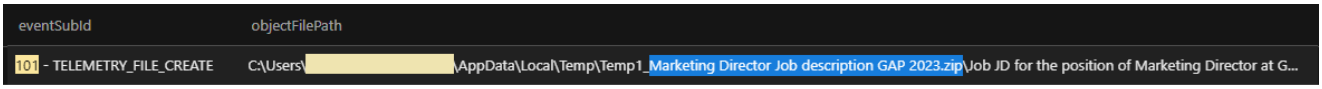
In July 2022, security researchers discovered an operation called Ducktail, in which threat actors used information-stealing malware to target, individuals and employees who might have access to Facebook business accounts. The perpetrators launched a spear-phishing campaign via LinkedIn direct messages that are aimed at marketing and HR professionals. This scheme would allow the threat actor behind Ducktail to take over Facebook business accounts and abuse the ad function for malicious advertising deployments. Given its growth and popularity, LinkedIn has increasingly become a preferred option for social engineering schemes and cybercriminal operations.

In March 2023, the Trend Micro Managed XDR team investigated several Ducktail-related web browser credential dumping incidents involving different customers. As a result, we discovered the involvement of a file that gathers user data, such as browser information, IP address, and geolocation, while also connecting to Facebook and Telegram domains. In this blog entry, we present our findings and technical analysis based on these incidents.

Technical Analysis

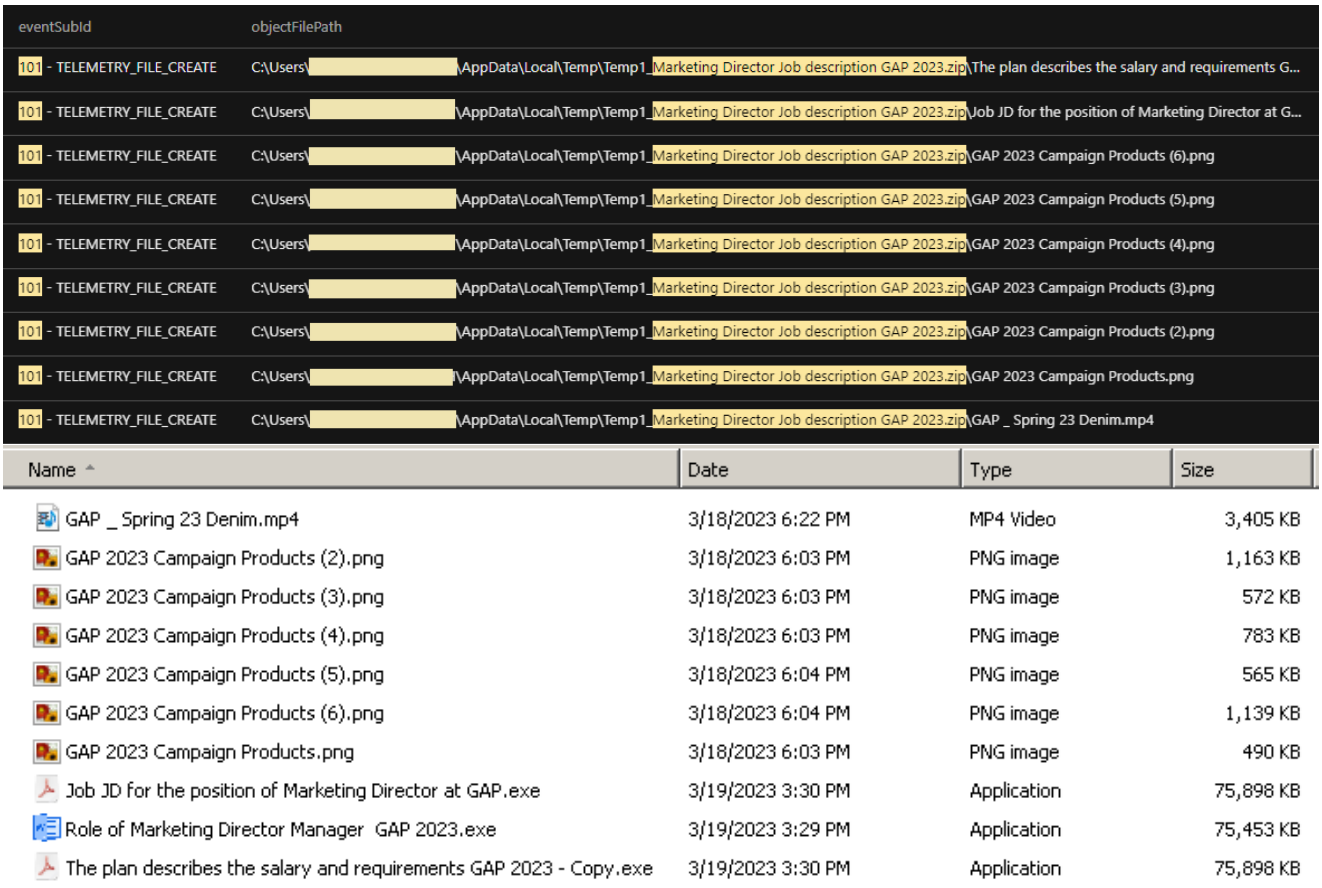
The file name of the sample file, which includes a reference to a job opening for a marketing director (Figure 1), is clearly aimed at marketing professionals. It is also likely that it mentions a higher leadership position to lure them into accessing the archive. Note that we only had access to the download link, so we can't definitively say how these links were delivered to the target; however, it's possible that LinkedIn messages were used given Ducktail's historical use of the platform.

Through the file name, we were able to gather the contents (Figure 2) as well as the source (Figure 3) of the archive. Upon checking the domain, we found that the malicious file was hosted on iCloud, Apple's cloud file-hosting service. Note that the URL is already inactive at the time of writing.



eventSubId	objectFilePath
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\Job JD for the position of Marketing Director at G...

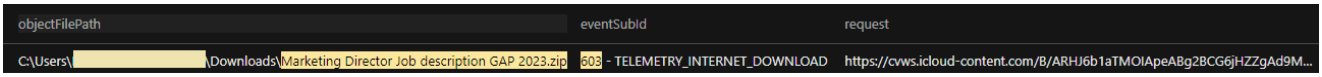
Figure 1. The archive name with a reference to a marketing director job position



eventSubId	objectFilePath
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\The plan describes the salary and requirements G...
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\Job JD for the position of Marketing Director at G...
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\GAP 2023 Campaign Products (6).png
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\GAP 2023 Campaign Products (5).png
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\GAP 2023 Campaign Products (4).png
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\GAP 2023 Campaign Products (3).png
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\GAP 2023 Campaign Products (2).png
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\GAP 2023 Campaign Products.png
101 - TELEMETRY_FILE_CREATE	C:\Users\ \AppData\Local\Temp\Temp1_Marketing Director Job description GAP 2023.zip\GAP _ Spring 23 Denim.mp4

Name	Date	Type	Size
GAP _ Spring 23 Denim.mp4	3/18/2023 6:22 PM	MP4 Video	3,405 KB
GAP 2023 Campaign Products (2).png	3/18/2023 6:03 PM	PNG image	1,163 KB
GAP 2023 Campaign Products (3).png	3/18/2023 6:03 PM	PNG image	572 KB
GAP 2023 Campaign Products (4).png	3/18/2023 6:03 PM	PNG image	783 KB
GAP 2023 Campaign Products (5).png	3/18/2023 6:04 PM	PNG image	565 KB
GAP 2023 Campaign Products (6).png	3/18/2023 6:04 PM	PNG image	1,139 KB
GAP 2023 Campaign Products.png	3/18/2023 6:03 PM	PNG image	490 KB
Job JD for the position of Marketing Director at GAP.exe	3/19/2023 3:30 PM	Application	75,898 KB
Role of Marketing Director Manager GAP 2023.exe	3/19/2023 3:29 PM	Application	75,453 KB
The plan describes the salary and requirements GAP 2023 - Copy.exe	3/19/2023 3:30 PM	Application	75,898 KB

Figure 2. The content of the archive



objectFilePath	eventSubId	request
C:\Users\ \Downloads\Marketing Director Job description GAP 2023.zip	603 - TELEMETRY_INTERNET_DOWNLOAD	https://cvws.icloud-content.com/B/ARHJ6b1aTMOIApeABg2BCG6jHZZgAd9M...

Figure 3. The file download link

We looked into the created processes and observed three processes total. Two of these — one was for Microsoft Edge (Figure 5) and one was for Google Chrome (Figure 6) — are used to gather the IP addresses and geolocation of the victims.

The following argument is used for these processes:

> *--headless --disable-gpu --disable-logging --dump-dom hxxps://getip[.]pro*

The last process (Figure 7) is used to open a PDF file containing the description for the fake job position.

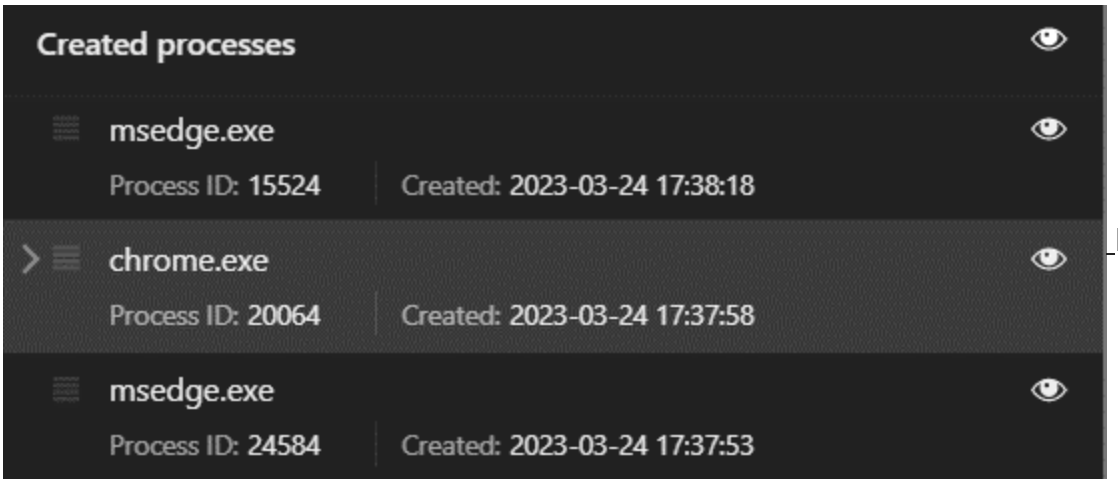


Figure 4. Browser processes spawned by Ducktail to gather information and mask its activities

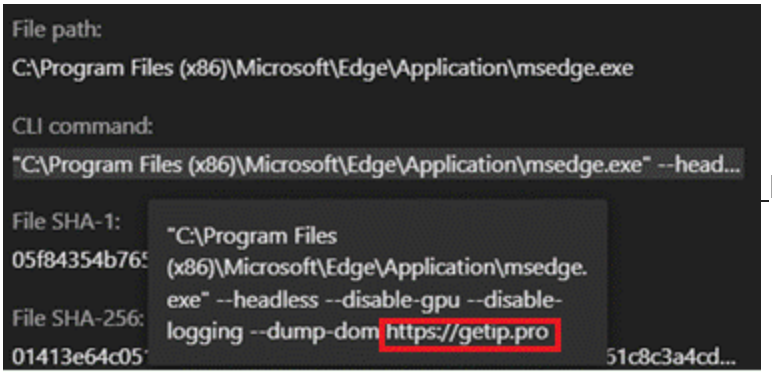


Figure 5. The spawned “Msedge.exe” file used to gather user IP addresses and geolocation

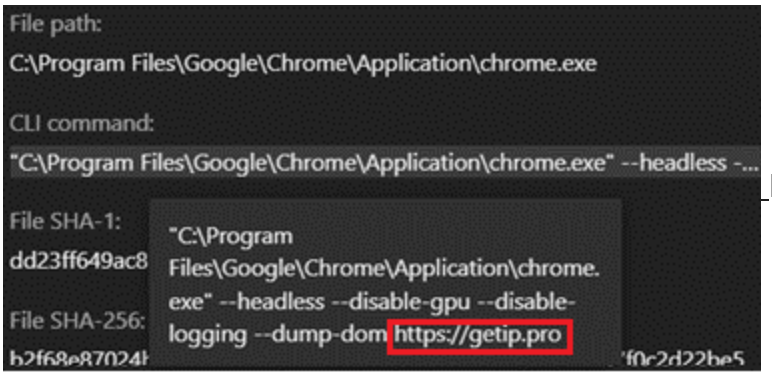


Figure 6. The spawned “Chrome.exe” file used to gather user IP addresses and geolocation

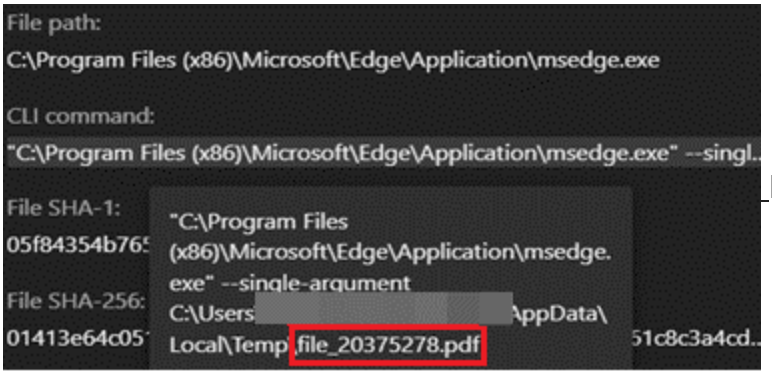


Figure 7. Ducktail opens a PDF file to masquerade itself.

While victims are busy reading the spawned PDF file, the malware is already gathering browser credentials and connecting to their Facebook domain to gather Facebook-related information. Once the data is gathered, the malware stores it in a text file as *%User.*

Temp%\temp_update_data_8.txt. It is then exfiltrated using Telegram. Our observation is that the malware updates and sends the data every 10 minutes.

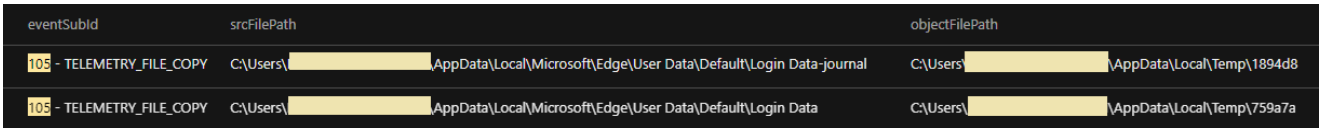


Figure 8. Login data being copied to a temp file

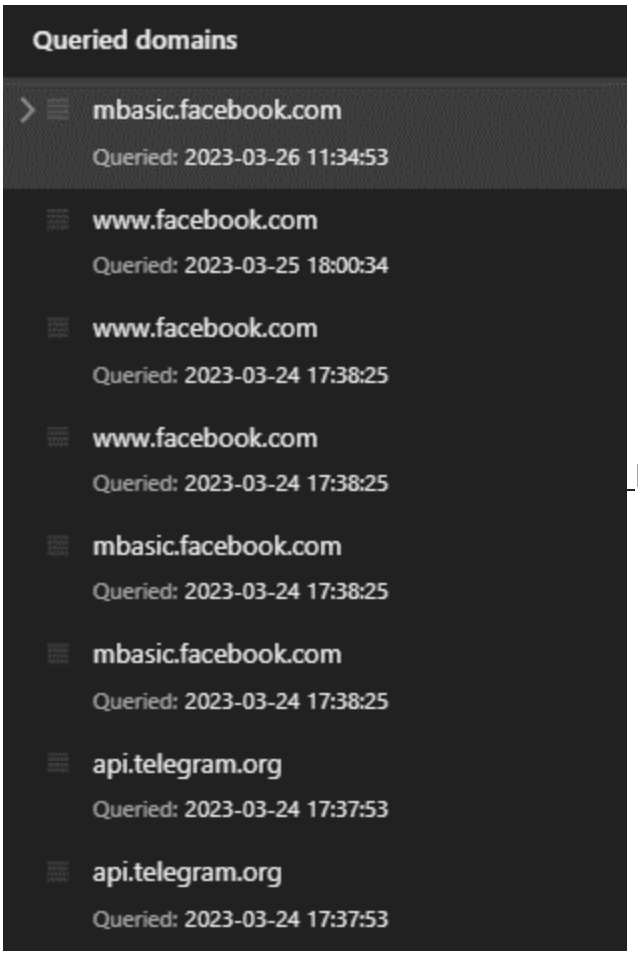


Figure 9. Connection to the “facebook.com” and “telegram.org” domains

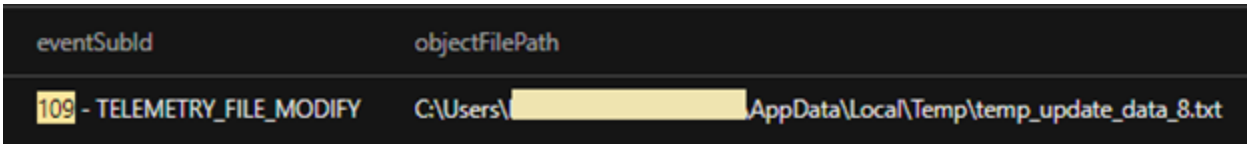
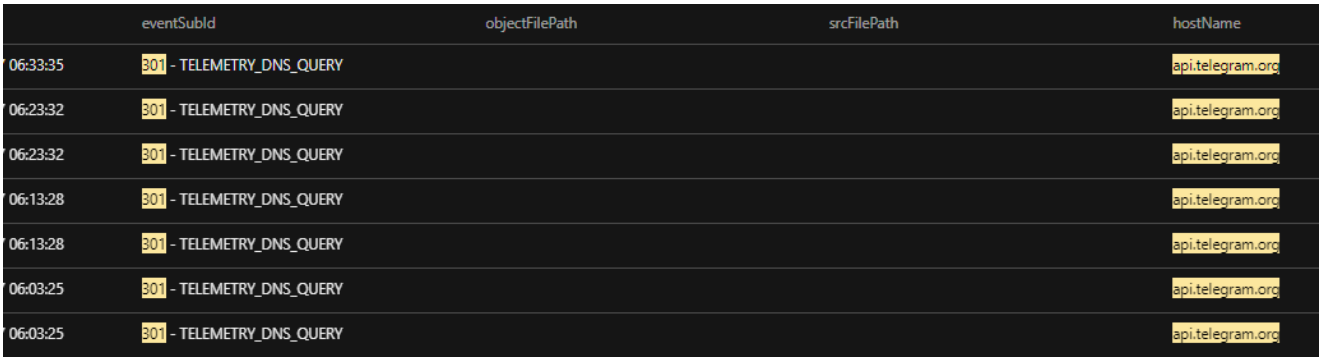


Figure 10. The malware stored as a text file



	eventSubId	objectFilePath	srcFilePath	hostName
06:33:35	301 - TELEMETRY_DNS_QUERY			api.telegram.org
06:23:32	301 - TELEMETRY_DNS_QUERY			api.telegram.org
06:23:32	301 - TELEMETRY_DNS_QUERY			api.telegram.org
06:13:28	301 - TELEMETRY_DNS_QUERY			api.telegram.org
06:13:28	301 - TELEMETRY_DNS_QUERY			api.telegram.org
06:03:25	301 - TELEMETRY_DNS_QUERY			api.telegram.org
06:03:25	301 - TELEMETRY_DNS_QUERY			api.telegram.org

Figure 11. Connecting to Telegram every 10 minutes to exfiltrate data

Hunting for other affected machines

Once the threat connected to Telegram, we decided to search for other affected machines. Using the Telegram IP address, we searched for other possible infections in the environment using the Search app function of Trend Vision One™. The search yielded the following processes on a couple of machines:

- *C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MS Excel.exe*
- *C:\Users\<user>\AppData\Local\Temp\onefile<random>\MicrosofOffice.exe*

We verified that all files were similar to the first detected file. Notably, the name of the binaries in this case made it seem like they were office applications.

Security recommendations and Trend solutions

Given the heavy use of social engineering lures by today's threat actors, individual users and organizations should take great care to avoid selecting links or downloading files from unknown sources, whether they are sent via social media websites such as LinkedIn and Facebook, or through emails. The following best practices can help users avoid being victimized by spear-phishing attacks:

1. Users should be cautious of unexpected or unsolicited emails. Before responding to or opening any attachments or links, users should first verify the sender's identity.
2. Users should avoid selecting suspicious links, especially if they are from unknown or suspicious sources. Hovering over the link to see the URL can help recipients check if a link leads to a legitimate website.
3. Organizations should ensure that their employees are educated on spear phishing and how to recognize and avoid it. Conducting regular training sessions can help keep everyone informed and up to date.

Managed XDR uses expert analytics to analyze vast amounts of data collected from various Trend technologies. XDR employs advanced AI and expert security analytics to correlate data from both customer environments and global threat intelligence, resulting in fewer but

more accurate alerts and leading to quicker detection. Additionally, Vision One provides a single console that has prioritized alerts and is supported with guided investigation, making it easier for organizations to understand the full scope of an attack and its impact.

With Trend One™, businesses can enhance their resilience with round-the-clock premium support, managed XDR, and incident response services. This service includes automated updates and upgrades for solutions, on-demand training, access to best practice guides, and the ability to consult with cybersecurity experts.

Trend Micro Apex One™ combines threat detection, response, and investigation in one solution. It automatically detects and responds to many types of threats, such as ransomware and fileless attacks. Apex One has advanced tools to detect and respond to attacks and can integrate with security information and event management (SIEM) systems.

Trend Cloud One™ – Endpoint Security and Workload Security protect endpoints, servers, and cloud workloads through unified visibility, management, and role-based access control. These services provide specialized security optimized for your diverse endpoint and cloud environments, which eliminate the cost and complexity of multiple point solutions. Meanwhile, the Trend Cloud One™ – Network Security solution goes beyond traditional intrusion prevention system (IPS) capabilities, and includes virtual patching and post-compromise detection and disruption as part of a powerful hybrid cloud security platform.

Indicators of Compromise (IOCs)

The indicators of compromise for this entry can be found here.