Managed XDR Investigation of Ducktail in Trend Micro Vision One

Published: 2023-05-09 · Archived: 2026-04-02 11:38:25 UTC

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.

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.

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 XDRservices 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™services, 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™products 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 productsand Workload Security productsprotect 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 productssolution 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.
