650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

Bulletin: 2021- 009

Date: 11/09/2021

Name: IcedID Campaign

Classification: Banking Trojan

Summary

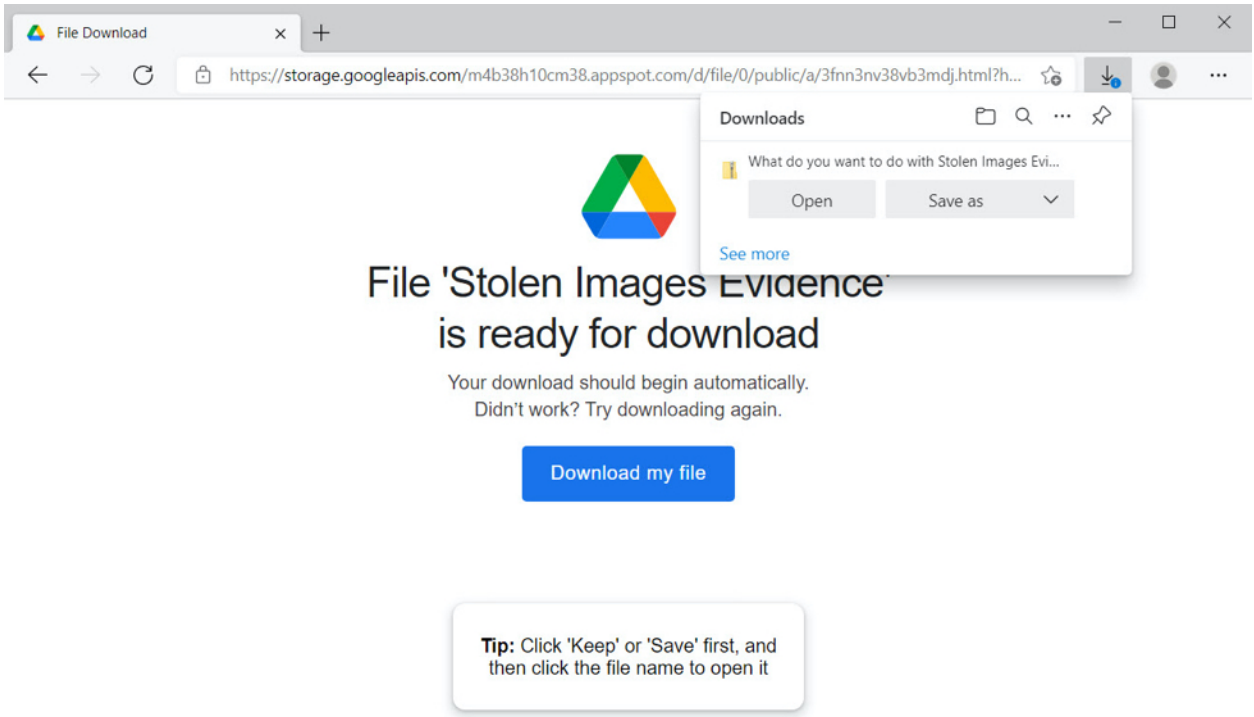
Menlo Labs has been tracking a malware campaign known as the “Stolen Images Evidence” campaign. This campaign sends emails that are generated through contact forms on various websites. These form-submitted emails include a malicious Google Drive link in the message body. The email misleads the user into clicking the link by suggesting they will receive a proof of stolen images that resulted in a copyright violation. However, clicking the link delivers a zipped JavaScript file that downloads a malicious Windows DLL that includes a malware called IcedID.

Infection Vector

1. Attackers are sending a malicious link via email that appears to be a shared google file/drive.
   a. The email subjects are “Stolen Images Evidence”, “Critical Errors Report” and “Alert: Contact Us Form Submission”
2. When users click the link it takes them to a fake google drive landing page. When the user lands on these pages, they are presented with an image of the google drive logo and a link to download the shared file.

650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin



3. Clicking on the Download buttons downloads a malicious .zip file that contains a malicious JavaScript file inside.
4. If the user runs the script it will download a malicious DLL and run it.
5. The DLL is 10MB and will be saved to the “AppData\Local\Temp” directory.
6. While there was no apparent sign of persistence, (rebooting the computer ended this infection), if left running an attacker could use the malware to download more malware and establish or maintain a presence in the victim's environment.

650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

Menlo Policy Recommendations

Based on the characteristics of this campaign, Menlo customers can implement the following policies to prevent both the download and block any CnC communication:

- The Menlo platform allows customers to define policies to files in archives. The customer can specify a custom ‘JS’ file type and then block downloads of archives containing this ‘JS’ filetype.
- Ensure that all non browser traffic categorized as a threat is blocked.

Menlo Protection

Menlo Labs continues monitoring the threat and updating the platform accordingly with IOCs. IOCs in this campaign are currently being added to the product and are now categorized as *malware*. Customers are recommended to set their policy for threat categories across isolated and application web requests to *block*.

The Menlo cloud security platform has multiple content inspection engines that analyze and block such threats from reaching the endpoint.

Integrate detection technologies like **AV Engines** and **Sandboxes** into a customer’s content inspection engine to provide additional defense on one isolated platform.

The Menlo platform provides an additional layer of security against zero days and new malware campaigns by opening documents in a “safe” mode and letting the customer download a safe version of the document

IOC

650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

ICEID HASHES:

6E3CB4977444C2759E307B3A4FAE39D0C7B676EA52E3FD0782DD4F57CD34D869

08b90df0446c89677b6a2041bf83e7ed3a465c0660237b4e16a36688aa403b24

fafede350d9713a8b0543b391bb2b65019ae3f72e9fc2af42e1ac7f3f4bff9f4

34dd197f4689bcb03614a4ea30d12ade0daf0157c3a767bee1aec4de1302f161

GOOGLE SITES LANDING PAGE HASHES:

1bb732e67fffb76e61639d8a592d200323429a5128949bf8d5c27a86079b045c

e006b943d4b049a29b75759ef8ad77c1ad7ab5f26ce75e7519c401386586afca

2c4f518b1967ab5961ca445c7f75d5cdb408b35c821c155be2a4233c258da88a

7e3fc8c7b811faac9a1a083b72fe271c7f0541956e0e4889fc237e7d42f19b88

b8c8953ebaca7abe6921c787b7555008de6e39d6817a20aedd543ae390565914

47b6e022ea55bb5e7f52c12984d2d59d5bfa9447509bdb73ea01912e0b9311d2

8f31170ab425f463d28aa364f3f3eb534d2b951e200b080f67eb853561d66e34

1bb732e67fffb76e61639d8a592d200323429a5128949bf8d5c27a86079b045c

041cbfe566cb094f77b9f9f480ed298ee4ed2db75eae61e73719627acc78eef4

46cc1b32bac2ca63a23539b1931c41e7e455d23279b2b2604cd1283addca84e0

e98183ae8adc10a320c7d0714a8356efcdc7cf1a91c71e30e1f86512df88756c

a4822a95f5f5bf7f6760cb7193e4e4f082ec7a829b9f3abbf933b50f0f52e18a

9d42e34191454243415195d40fcda9181104016c10c947f1581787aab44082da

029c49ece0239a6b604da278fb0c5aa57d37956b200abe7d04ea1e4f412d0bf1

650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

EMAIL:

mphotographer550@yahoo[.]com

mephotographer890@hotmail[.]com

mgallery487@yahoo[.]com

mephoto224@hotmail[.]com

megallery736@aol[.]com

mshot373@yahoo[.]com

GOOGLE SITES PAGE:

104.21.14.159 - bigeront[.]top/jb39fj6kke/

STOLEN IMAGES EVIDENCE.JS:

104.21.16.223 - bediloper[.]top/034g100/index.php

104.21.16.223 - bediloper[.]top/034g100/main.php

INSTALLER DLL:

172.67.198.112 - lascakatheather[.]top

650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

ICEDID C2 HTTPS traffic:

45.147.228.198 - garrozalibbo[.]click

45.147.228.198 - marslayot[.]top

45.147.228.198 - roponavi[.]online

45.147.228.198 - twistcolseza[.]top

45.147.228.198 - trinaa3[.]fun

45.147.228.198 - devicescout[.]space

185.70.184.41 - disponfirules[.]top

185.70.184.41 - ytoptila[.]website

185.70.184.41 - mislinororv[.]top

185.70.184.41 - frangimingi[.]top