1 650.614.1705
support@menlosecurity.com
www.menlosecurity.com

Bulletin: 2021- 010

Date: 11/16/2021

Name/Group: TA551

Classification: Hacker Tool

Summary

Menlo Labs is tracking a new campaign from threat group TA551, that is possibly targeting a small group of victims. The first email from the attacker is meant to look like a potential new client inquiry. We assess this email is to validate that the inbox is monitored. Once confirmed the attacker sends another email. Subject of the email in this campaign: "(USERNAME) sent you files (project details) with TransferNow". This campaign sends an email to the victim that includes a malicious link in the message body. The email misleads the user into clicking the link by suggesting a potential client has sent them project information. However, clicking the link delivers a malicious iso file that contains a malicious shortcut LNK file and a malicious DLL.

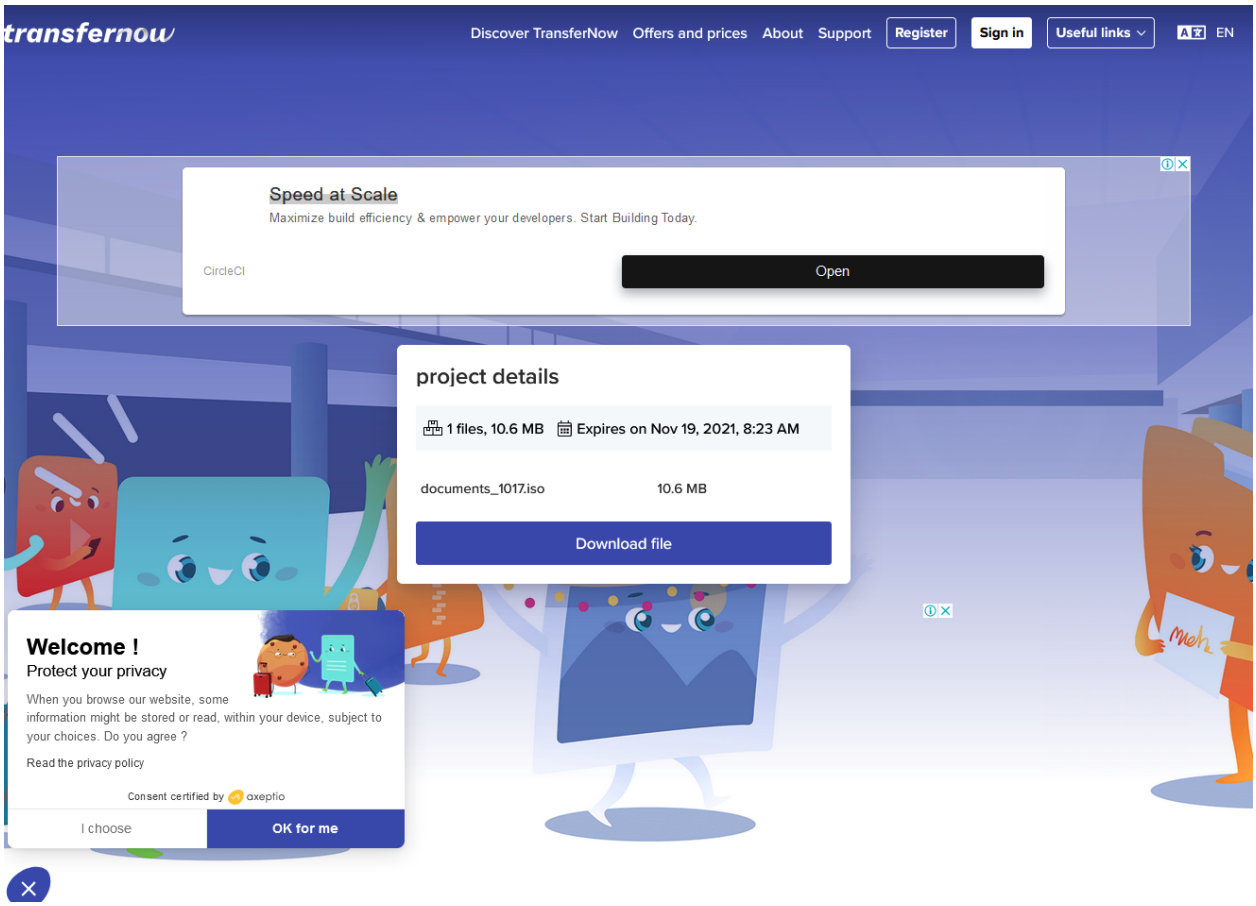
Menlo Labs is thus far tracking two separate attacks from TA551 over the last 3 weeks and is investigating if there were any others and their related TTPs. TA551 has used the seen TTPs from these attacks to ultimately deliver ransomware to the victims.

Infection Vector

1. Attackers are impersonating Saudi Aramco's American branch by sending out spoofed emails claiming to want to have product consultation.
    a. Inspection of the email header reveals true email coming from a "porkbun[.]com" domain.
2. After responding to the initial request, attackers send a malicious link via email that appears to be a shared file.

a. The email subject is “(USERNAME) sent you files (project details) with TransferNow”

3. When users click the link it takes them to a download file landing page.



4. Clicking on the Download button downloads a malicious .iso file that contains a malicious lnk file and a malicious DLL..
5. If the user double clicks the shortcut LNK file or runs the .iso file this will cause the malicious DLL file to run.
   a. The malicious DLL is named “store.dll” and the export that is loaded to run it is “StoreApp”.
6. The DLL is 10.6 MB and may be installed in the “C:\programdata\” file location.
   a. When run, the file will attempt to connect to a C2.

1 650.614.1705
support@menlosecurity.com
www.menlosecurity.com

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. This requires a backend capability called “enforce_policy_in_archives” that needs to be enabled, which then exposes the policy options to block archives with suspicious embedded files. The customer can either choose to block a ‘ISO’ file type or configure a more granular policy to block .lnk files contained within .ISO files
- Ensure that all non browser traffic categorized as a threat is blocked.

Menlo Protection

Menlo Labs is monitoring the campaign and updating the platform accordingly with IOCs. IOCs in this campaign have been 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

IOCS

FILE HASHES:

1. LNK:AD2908988CB585D6FB1DC583C8F943C5BF5B4CEDD4B4BC90FD56C3FBBCD0A3CC
2. DLL:ACF838CF0FE15C20F3321EEA5156E74410376542C17B22A194798CD0E054BF5D
3. ISO:EB83CD63B575E15173D7F117D2A890982A536D4E641AFDF52720AD00983A047F
4. SIMILAR DLL:9622b99618ceea9ecbb93d54380235919ac99abcd5e2bd56c7ae8aa5e8650a9b

LANDING PAGE:

hxxps[://]www[.]transfernow[.]net/en/dltransfer?utm_source=20211112J294PllV&utm_medium=FjaYmYdy

C2:

172.241.27.209 - hxxps[://]kirute[.]com:443

EMAIL:

abdul.jabbar@porkbun[.]com