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

Bulletin: 2021-008

Date: 09/29/2021

Name: Solarmarker Malware Campaign

Classification: SEO Poisoning Attack

Summary

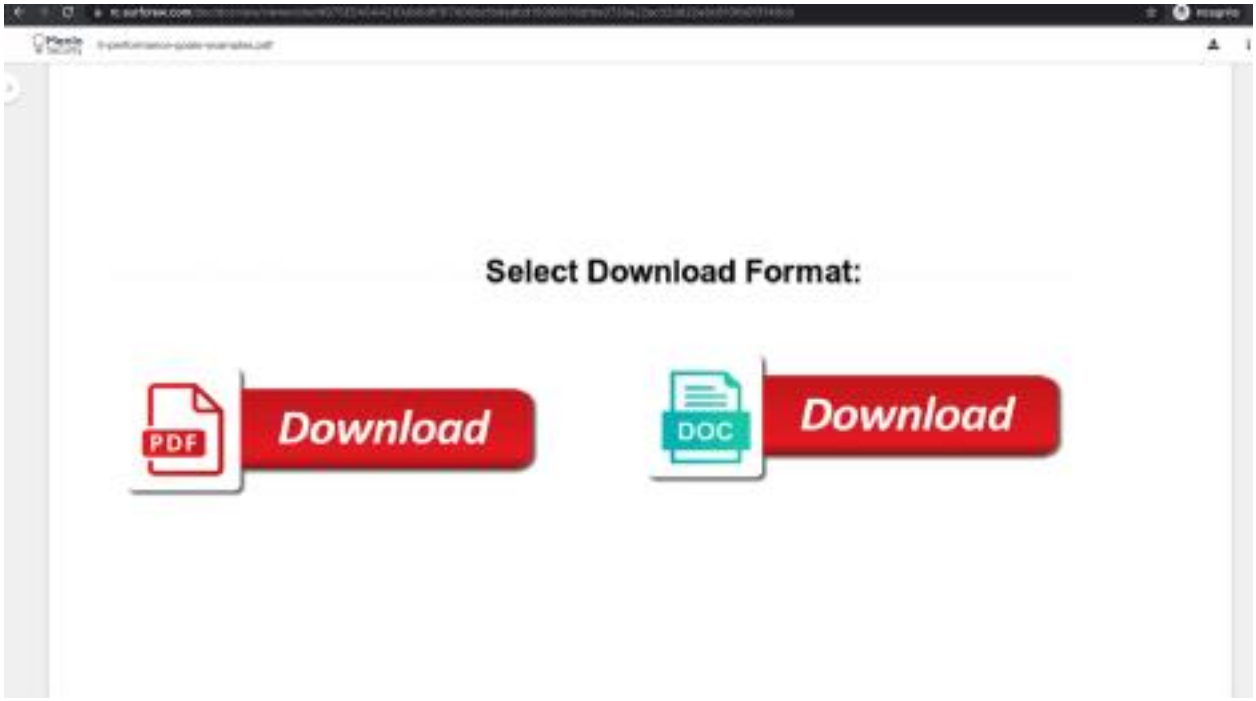
Menlo Labs has been tracking a malware campaign known as the Solarmarker Campaign that delivers a Windows executable from uncategorized websites.

Infection Vector

1. Attackers are compromising wordpress sites and injecting malicious PDFs, via a technique known as SEO poisoning

2. When users search for these terms on popular search engines, the top of the search results show these malicious pages

3. When the user lands on these pages, they are presented with a PDF which is named after the search term they searched for. Below is an example of the screenshot of a PDF file



4. Clicking on either of the Download buttons takes the user through multiple HTTP redirects, after which a malicious Windows Executable is downloaded 5. Currently the executable payloads are > 50MB in size. The largest executable in this campaign is 123MB

6. Once infected the malware is capable of downloading additional malware to the endpoint

Menlo Insights Queries for SOC Teams

The following queries can be used in the Menlo Insights analytics product to help SOC teams hunt for Solarmarker indicators of compromise

1. method=POST ua_type=non_browser user_agent=None protocol=http category=Unknown

dst_ip=('45.42.201.248','37.120.237.251','5.254.118.226','23.29.115.175','216.230.232.134','146.70.24.173') | top(src_ip)

a. The above query identifies CnC communications identified thus far by Menlo research. It provides src_ip of infected systems

2. pathname like "%/wp-content/uploads/formidable%" pathname like "%pdf" file_size < 1MB | top(user)

a. This query provides a list of all users who've landed on the page that displays the malicious PDF

3. pathname like "%/sitedomen/%" | top(user)

a. This query provides a list of all users who've clicked on the malicious link, which eventually downloads the malicious payload

Menlo Policy Recommendations

Based on the characteristics of this campaign, Menlo customers can implement the following policies to prevent both the download and the CnC communications for this specific campaign

- Most of the domains from where malicious files are downloaded are uncategorized. Blocking windows executable file downloads from Uncategorized websites reduces the risk of getting infected

- The CnC communications are categorized as non-browser traffic. Menlo provides robust policies around blocking application traffic. The customer can either set their non browser (application) policies to block all non browser traffic or block traffic matching threat categories
- Most of the domains used in this campaign are either ".tk" or ".site" TLDs. If it's feasible, customers can choose to block access to all domains ending in these tlds

Menlo Protection

Menlo labs is 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.

Customers can choose to avail the below detection technologies to be integrated into the content inspection engine, providing defense in depth on a single platform.

- AV Engines
- Sandboxes

In addition to the above detection methodologies, 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

CnC IP's identified so far

- **45.42.201.248**
- **37.120.237.251**
- **5.254.118.226**
- **23.29.115.175**
- **216.230.232.134**
- **146.70.24.173**