

Bulletin: 2022-01

Date: 02/09/2022 - updated

Name: GootLoader Malware Campaign

Classification: SEO Poisoning Attack

Summary

Menlo Labs has been tracking a malware campaign known as the GootLoader Campaign that delivers an archive file with an embedded JS to the endpoint.

Infection Vector

1. Attackers are compromising wordpress sites and injecting some popular search terms into compromised pages to artificially increase the page rank in search results 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 link which is named after the search term they searched for. For instance if one searched for bilateral agreements, then the link would be named bilateral_agreement
4. When the user clicks on it, a zip file with an embedded JS gets downloaded to the endpoint
5. The user has to click on the JS for their endpoint to get infected
6. Once infected the malware is capable of downloading additional malware to the endpoint

Recommendation

- The Menlo Security Platform has a capability called ***“Enforce Policy in Archives”*** that provides customers the ability to enforce policies on files in an archive. **Please contact Menlo customer support to enable this capability**
- Once the capability is enabled, for JS files specifically, customers can follow the following steps to successfully block archives containing JS files.
- Step 1 - Web policy -> Document/Archives
 - > under “Archives and Compressed Packages” section, edit “Archive Isolation Options”

← Edit Default Archives Isolation Options

Archives and Compressed Packages Default Isolation Options

Customizes default rules for [archives](#) and [compressed packages](#).

Original Download of Isolated Archives

Block download of original archive

Sharing of Isolated Archives

Allow sharing of original download URL


Modal Dialog for Isolated Archives

Open archive viewer in a modal dialog

Enforce Policy in Archives

Apply policy to files in archives

Timeout for inspection of archive contents (minutes)
5

Nested archive depth
16 

Action on encrypted archive child

Action on failure (timeout/depth)

- Step 2 – Web Policy -> Policy Exceptions
-> Create a File Download Exception

← Create File Download Exception

Rule Details and Action

Specify source

Name
Block JS files

Treat file downloads from **isolated** sites differently from **non-isolated** sites.

Action (Isolated Sites)	Action (Non-Isolated Sites)
<input checked="" type="radio"/> Block	<input checked="" type="radio"/> Allow

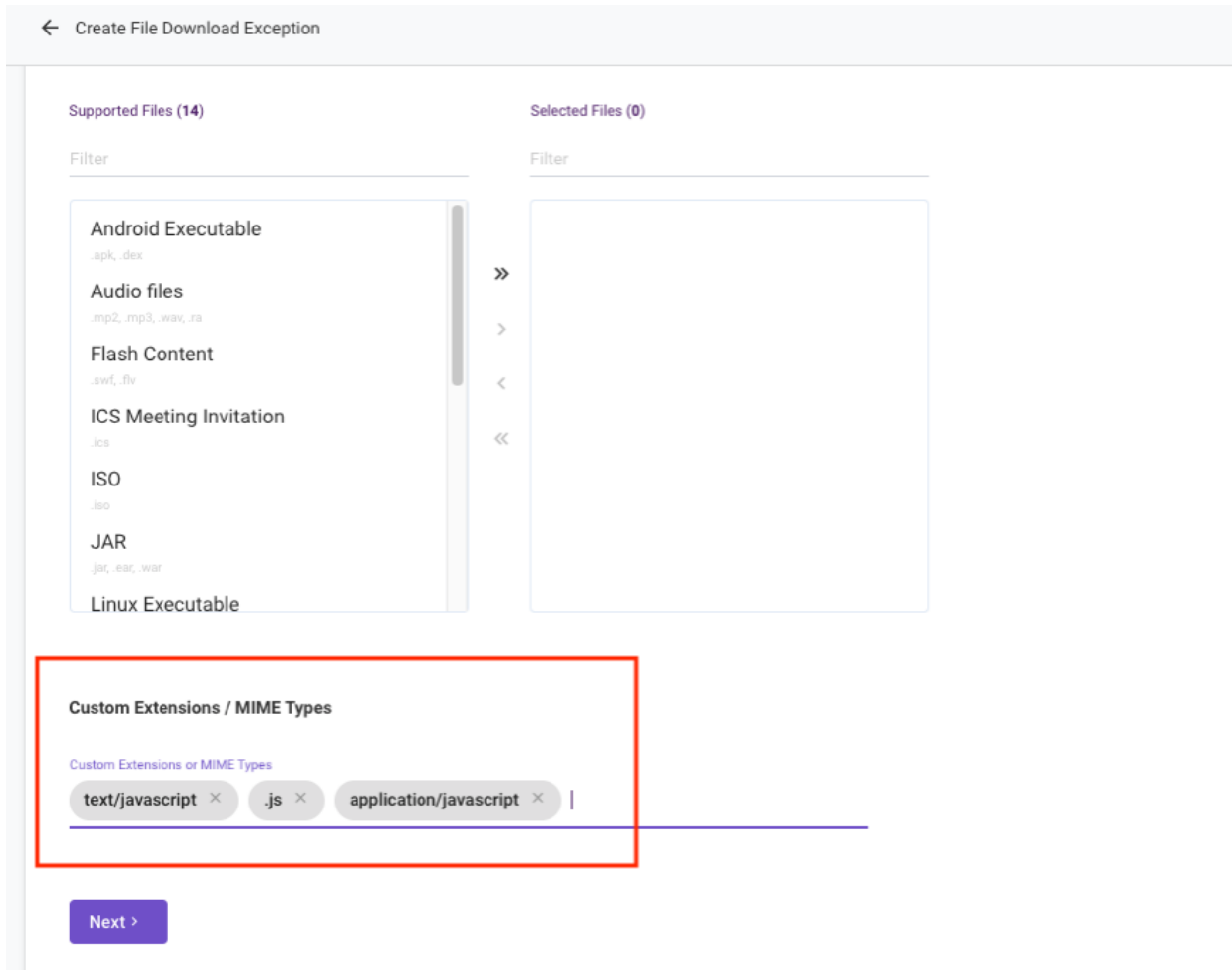
Description (optional)
This rule will block JS files that are downloaded via Isolation - its not recommended for Non-Iso sites|

Next >

- Since JS is not a default file type it needs to be added as a custom type in the exception rule as shown below. The following MIME types will cover all cases of JS files and need to be added to the Custom Extensions section as shown in the screenshot below

- *text/javascript*
- *.js*

- *application/javascript*



← Create File Download Exception

Supported Files (14) Selected Files (0)

Filter Filter

Android Executable
.apk, .dex

Audio files
.mp2, .mp3, .wav, .ra

Flash Content
.swf, .flv

ICS Meeting Invitation
.ics

ISO
.iso

JAR
.jar, .ear, .war

Linux Executable

Custom Extensions / MIME Types

Custom Extensions or MIME Types

text/javascript × .js × application/javascript × |

Next >

Menlo Protection

Menlo labs is monitoring the threat 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.

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 Domains
 - Jonathanbartz[.]com
 - junk-bros[.]com