File 2

Filename

clYirg.hta

Md5 Hash

16bfd3ad454a4222de43fc5f1dc494ed

General summary about particular sample (your ideas and ..)

It seems that this is another Trojan Downloader. It is a .hta witch is a HTML file that can be executed via Microsoft HTML Application Host.

General characteristic

- Contain obfuscated code
- The names nemucod and Locky are cited several times in community comments; we can assume that ransomware are the type of malware downloaded by this file

Antivirus detection results

Fairly more than half of the antivirus detected this file as a threat.

https://www.virustotal.com/gui/file/7a6979882d64b349779747a8e87ac4361c8f2f5ec85582f54fb124ab1c3de633

https://www.hybrid-analysis.com/sample/7a6979882d64b349779747a8e87ac4361c8f2f5ec85582f54fb124ab1c3de633

https://cuckoo.cert.ee/submit/post/3175474#

File System IOC (indicator of compromise)

We can find modification in files related to the history, the cache, and the cookies of Internet Explorer, probably to hide its presence.

Network IOC

3 DNS request marked as "malicious":

- www.luigigiordano.org (213.205.40.169)
- www.fmpromedia.com (195.78.215.76)
- www.kreso.it (213.205.40.169)

In addition to resolving this domains names, `fmpromedia` and `kreso` were also contacted.

`Suricata` (network threat detection engine) labelled those connection as malicious in the category `A Network Trojan was detected`

Registry IOC

Modify the proxy settings, and read the `DISABLESECURITYSETTINGSCHECK`for Internet Explorer.

Behavior and control flow

The analyse from `cuckoo.cert.ee` indicate that a thread was resumed because it was potentially an `indication of process injection`.

Seems to use internet cache setting to hide information that could be found in index.dat : we can find a query in the cache settings.

Appendix (links to analyses, etc)

https://www.f-secure.com/v-descs/trojan_js_obfuscated_gen.shtml