File 2

Filename

27423.jse

Md5 Hash

f7cdc866e97ff90b37108dcd3622eba1

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

It's a `.jse` script, or more precisely a `VBScript Encoded scrip`, the term `Cryxos` is found several time in the name of the threat detected by the antiviruses. The name `nemucod` is also cited in the comments and the analyses, but it is a very generic name.

General characteristic

- Distribution method : Compromised websites, rogue online pop-up ads, potentially unwanted applications
- Type of message displayed : "Computer / web browser has been blocked due to a virus infection", "Data has been stolen", "Threat detected on the computer"
- Idea is to scare the user so he act without thinking
- It is a call support call : the user is asked to call a number in order to respond to the threat / protect his data or remove the virus

Antivirus detection results

Most of the antivirus detect the trojan.

https://www.virustotal.com/gui/file/c0880cb0044d0a226b55e6f40a07e4c563c39c5eeb4824f0e3d95389d0b79691

https://www.hybrid-analysis.com/sample/c0880cb0044d0a226b55e6f40a07e4c563c39c5eeb4824f0e3d95389d0b79691

https://cuckoo.cert.ee/submit/post/3175275

File System IOC (indicator of compromise)

Nemucod touches several files in `%WINDIR%%\System32\`

Network IOC

Contact `centweek.top` (DNS request made to resolve this domain name)

Registry IOC

Read the computername and the machineGUID registry. Also read the langage used by the system.

Behavior and control flow

- Display false virus or error alert, asking the user to call a phone number in order to protect their data / computer (phone number is supposed to be technical support)
- The aim is to trick the user into paying for the assistance or to make the user purchase a software

Appendix (links to analyses, etc)

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