IcedID - A New Threat In Office Attachments

blog.minerva-labs.com/icedid-maas

Minerva Labs Blog

News & Reports

- Tweet
-

IcedID is somewhat of a veteran in the MaaS industry, being actively developed and distributed since 2017. The malware-as-a-service, also called Bokbot, has been in extensive use in the last couple of months by malspam distributors. Its latest version is delivered using a malicious Microsoft office attachment, which eventually drops and executes the IcedID payload.

The specific Excel document used in the recent wave of attacks is using XLM macros to download and execute its payload. Although the XLM macro technology is quite old, it is only recently that Microsoft added detection capabilities for XLM macros. This explains why so many threat actors have chosen to spread their malware using this archaic capability.

The malicious document uses the windows API URLDownloadToFile in order to download the IcedID payload to the path C:\Users\Public\microsoft.security, which it later executes using the WMIC binary.

This is a sample of the de-obfuscated macro:

The latest update to IcedID also saw a significant change to its first stage loading mechanism, which was dubbed “gziploader” by Binary Defense’s researchers. The new update uses a custom encryption algorithm to decrypt the actual bot which is hidden inside the file “licenses.dat”.

The malware’s development is especially concerning because of its collaboration with Sodinokibi (aka REvil) ransomware group, as reported by the DFIR Report. Their latest blog post’s details a breach starting with an IcedID infection that was escalated to a full-on ransomware attack in just under 6 hours, fully encrypting the fake corporate network used by the researchers.

Minerva Prevents IcedID latest development with our Memory Injection Prevention & Malicious Macro Prevention modules:

IOCs:

275a8e24dab9b523accb7205dc161a715216f7878f20adf7254cb640984f2edc (gziploader)

c5444c7252d6e22f4a2de2168a4afeb08e1f841aeba675e6e632e2c64fcd71ca (excel file)

References:

https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/

https://www.microsoft.com/security/blog/2021/03/03/xlm-amsi-new-runtime-defense-against-excel-4-0-macro-malware/

https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775123(v=vs.85)

https://www.binarydefense.com/icedid-gziploader-analysis/

https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

To learn more about Minverva Labs' Memory Injection Prevention module and how to protect yourself from malware, contact us.

« Previous Post
Next Post »

Interested in Minerva? Request a Demo Below