Emotet Spam Abuses Unconventional IP Address Formats to Spread Malware

trendmicro.com/en_us/research/22/a/emotet-spam-abuses-unconventional-ip-address-formats-spread-malware.html

January 21, 2022

Malware

We found waves of Emotet spam campaigns using unconventional IP addresses to evade detection.

By: Ian Kenefick

We observed Emotet spam campaigns using hexadecimal and octal representations of IP addresses, likely to evade detection via pattern matching. Both routines use social engineering techniques to trick users into enabling document macros and automate malware execution. Upon receiving these standards, operating systems (OS) automatically convert the values to the dotted decimal quad representation to initiate the request from the remote servers. Users and businesses are cautioned to detect, block, and enable the relevant security measures to prevent compromise using Emotet for second stage delivery of malware such as TrickBot and Cobalt Strike.

Routine using hexadecimal IP addresses

The samples we found start with an email-attached document using Excel 4.0 Macros, a dated feature used to automate repetitive tasks in Excel that malicious actors have abused to deliver malware. Abuse of the feature in this case allows the malware to execute once the document is opened using the *auto_open* macro.

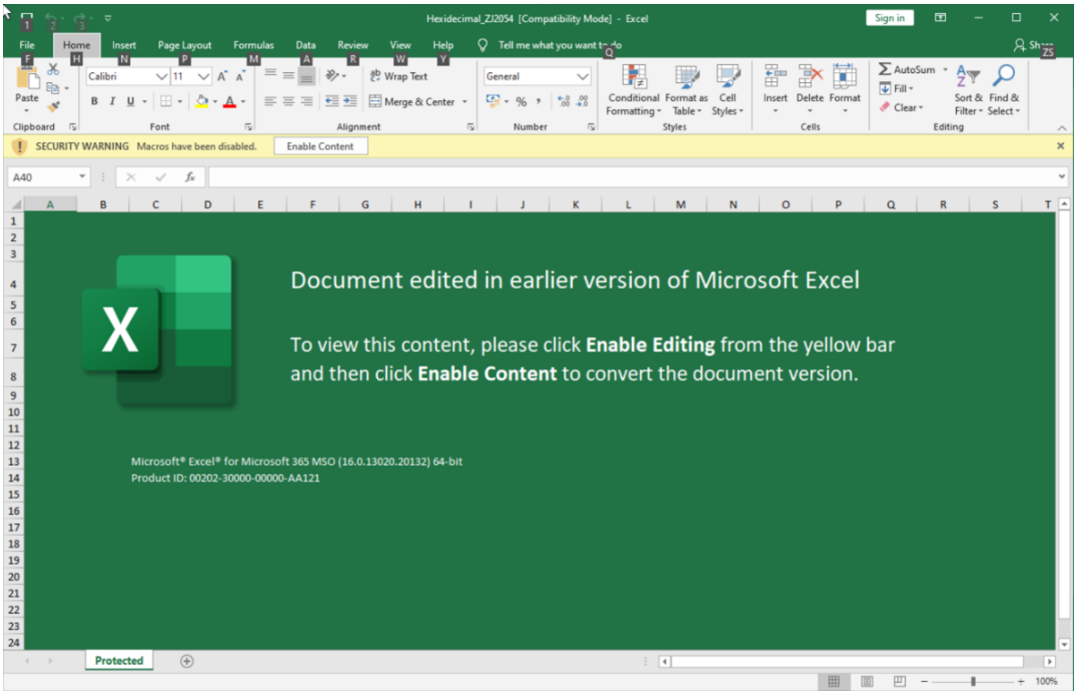

Figure 1. Attached document in the emails lures users into enabling the macros

The URL is obfuscated with carets and the host contains a hexadecimal representation of the IP address. Using CyberChef, we converted the hexadecimal numbers to find the more commonly used dotted decimal equivalent, 193[.]42[.]36[.]245.

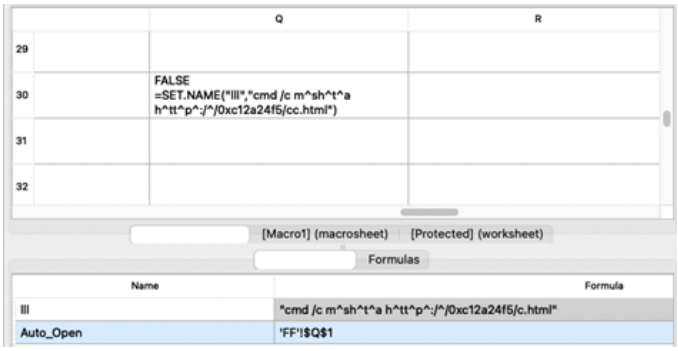

Figure 2. Using carets for obfuscation

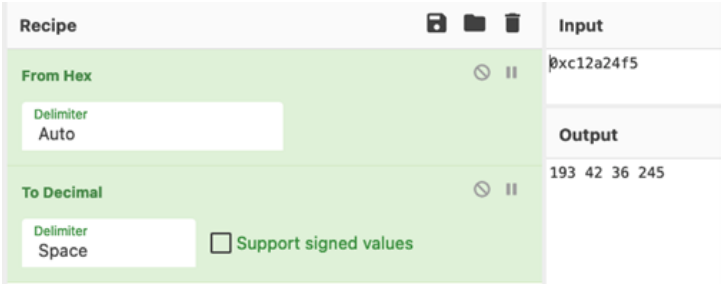

Figure 3. Converting the hexadecimal numbers to dotted decimal representation

Once executed, the macro invokes *cmd.exe* > *mshta.exe* with the URL containing the hex representation of the IP address as an argument, which will download and execute an HTML application (HTA) code from the remote host.

Figure 4. Downloading and executing an HTA code

Routine using octal IP addresses

Much like the hexadecimal representation sample, the document also uses Excel 4.0 Macros to run the malware once the document is opened and enabled. The URL is also obfuscated with carets but the IP contains an octal representation. We also used CyberChef to decode this IP address into a dotted quad format, 46[.]105[.]81[.]76.

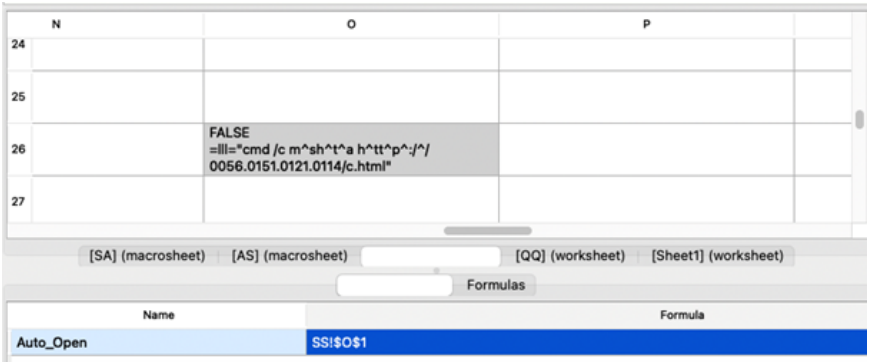

Figure 5. Using similar techniques with the hex decimal routine but with octal representation for obfuscation

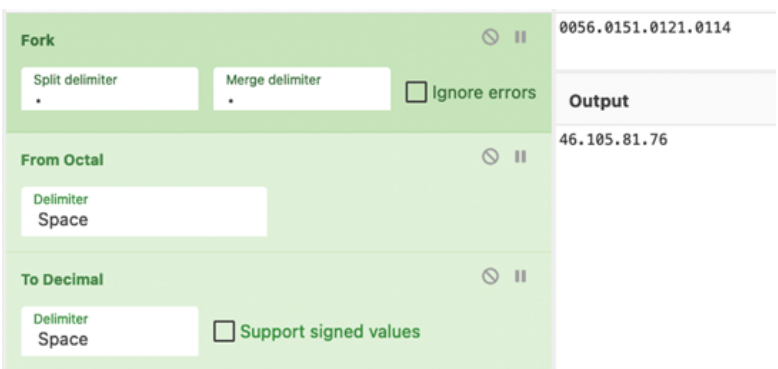

Figure 6. Converting the octal numbers to dotted decimal representation

As observed in the process tree, once executed, the macro also invokes *cmd.exe* > *mshta.exe* with the URL as an argument to download and execute an HTA code from the remote host.

Figure 7. Downloading and executing an HTA file

Conclusion

Traces of Emotet were observed as arbitrarily dropping Cobalt Strike beacons between November and December 2021. Earlier this year, however, operators became noticeably selective on which targets the beacons were dropped. Evasion techniques like these could be considered evidence of attackers continuing to innovate to thwart pattern-based detection solutions.

Moreover, the unconventional use of hexadecimal and octal IP addresses may result in evading current solutions reliant on pattern matching. But in the same vein, the unusual technique in the command lines can be used as a detection opportunity, with security teams using filters as leverage that can be enabled to treat such IP addresses as suspicious and associate them with malware.

Indicators of compromise (IOCs)

SHA256	Description	Detections
e492f31ca20d99888b2434dcb4d9af1f93ed4c485b9bd2bc550ce8ae8021b9cd	Hexadecimal IP address sample	Trojan.XF.HIDDBOOK.SMTH
3e9701129f13f13f7b873f55dc3d43d04cbd1dd3f85814270bb1b177394926b5	Octal IP address sample	Trojan.XF.EMOTET.SMYXBLAA

URLs

193[.]42[.]36[.]245

46[.]105[.]81[.]76