Cyber Threat Actors Leveraging Right-to-Left Override (RTLO) in Recent Attacks

Threat Bulletins | Aug 09, 2021, 12:57 PM

Cyber security researchers are aware of malicious actors leveraging masquerade and obfuscation techniques to deliver harmful files via email to healthcare organizations. The threat actors are using a legitimate feature of Right-to-Left Override (RTLO) Unicode to email malicious files to potential victims and have them appear benign in an attempt to deliver attacks that leverage the Cobalt Strike toolkit.

Health-ISAC has collected Indicators of Compromise (IOCs), which are included in this bulletin for the purposes of additional review, research and network defense purposes.

Cyber security researchers report that threat actors attempt to deliver malicious files to potential victims using, either independently or in tandem, masquerade and obfuscation techniques to make htm and htm/eml files appear as a mp3, wav, or pdf attachments. Threat actors also attempt to deliver malicious htm files masqueraded as a pdf file. The htm file contains obfuscated JavaScript, which includes a base64 encoded string to a URL that may NOT be blocked by commercial email filter and security products.

At this time we are not aware of any successful compromises. The right to left override (RTLO) character is a special character within unicode, an encoding system that allows computers to exchange information regardless of the language used. Unicode covers all the characters for all writing systems of the world, modern and ancient. It also includes technical symbols, punctuations, and many other characters used in writing text. For example, a blank space between two letters, numbers or symbols is expressed in unicode as “U+0020”.

The RTLO character (U+202e in unicode) is designed to support languages that are written right to left, such as Arabic and Hebrew. The problem is that this override character also can be used to make a malicious file look innocuous.

Mitigation:

- This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection

- Detection methods should include looking for common formats of RTLO characters within filenames such as \u202E, [U+202E], and %E2%80%AE. Defenders should also check their analysis tools to ensure they do not interpret the RTLO character and instead print the true name of the file containing it.

TTPs:
Email subjects:
PASSWORD_EXPIRE_TODAY
Benefit on 30/07
Employee Benefits - Qualified Employee List
RecordedCall on Thu July 22 ,2021
Payment_Instructions for Allflex, Received On, 27, July, 2021

Received On, 23, July, 2021
Received On, 21/07
You Recieved An Audio Recording
Missed Call Notification
Employee Benefits - Qualified Employee List
PASSWORD_EXPIRE_TODAY

Threat Indicator(s):

SHA256:

be60c857b462bb197b0671db06b69b574b3bfd4702d904c3388757c723ed629c
b20d8723dce70af2ee827177d803f92d10e8274a80c846cf42742370d9f11c65
b6efa2b607d5d8e6a7392a8b2fac05cf0f644d69bc3e7f9331456e2bf59c9501
2c661f8145f82a3010e0d5038faab09ea56bf93dd55c1d40f1276c947572597b

URL(s):

hXXps://buywastefree[.]com
hXXp://bnddigital[.]com[.]br
hXXp://radioaracajumix[.]com[.]br
hXXp://beende-dein-schweigen[.]de
hXXp://ellegant[.]eu
hXXp://ies-lucus-solis[.]es
hXXp://bhhs[.]edu[.]bd
hXXp://josefinaastegianomkt[.]com
hXXps://oficinadaconstrucaorj[.]com[.]br
hXXp://convencionipuc[.]com
hXXps://cdn[.]discordapp[.]com/attachments/847773813131182112/868160361466040321/Exploit[.]exe
hXXps://coppershoppe[.]net
hXXp://sbtse[.]gr
hXXp://pamfiok[.]com
hXXps://banilomer[.]com

Email(s):

contacto[@]prosystemsc[.]com
notifications[@]woovly[.]com
qkampf[@]nenonwovens[.]com
noreply-license[@]cri-mw[.]co[.]jp
llaki[@]shiupong[.]com
no-reply[@]unne[.]edu[.]ar
noreply[@]creditosenelacto[.]com[.]ar
support[@]email[.]flowcrm[.]com
noreply[@]paradigmlife[.]net
james[.]boyg[@]schoo[.]jp
no-reply[@]trornbetta[.]com
hello[@]support[.]michi-to-ten[.]com

vipul[@]envi[.]ca

Sources:

‘Right-to-Left Override’ Aids Email Attacks
Masquerading: Right-to-Left Override
“semaG dna nuF” with Right-to-Left Override Unicode Characters

For Questions or Comments: Please email us at toc@h-isac.org

Reference(s)

MitreRed CanaryKrebs on Security