This group used T1011.001 and then continued on to further exploit the text which does not meet T1012, but everything went over the malicious AS 1322 since it covers many IPs.

CVE-1999-0003

APT29 is the badass

CVE-2020-1234

Under C:\Windows\System32\ the evil executable was found. /home/user/Downloads is also evil

HKLM\SOFTWARE\Micosoft\DirectX

threatintel@eset.com

ffoabar.com

8.8.8.8

127.0.0.1

I went to ::1 a undefined yes

executed with arp.exe and cmd.exe to run it

102.123.12.12

https://google.com/mylogin_link.php

this has been our htxxs://google.com for 1.2[.]21[.]21 and ema AT gmail.com but not longer home is here 127.0.0.1 is

google.site

google.live

https://googa.net aads and the evil evilbad https://foo.net as well

Don’t use intranet.accenture, but use Microsoft

f0:d5:bf:2b:bf:ba

F0:D5:bf:2b:bf:ba1

C8:5B:76:8B:C2:40