tweets/2020-09-07-Dridex-IOCs.txt

github.com/pan-unit42/tweets/blob/master/2020-09-07-Dridex-IOCs.txt

pan-unit42

pan-unit42/**tweets**

4 Contributors | 0 Issues | 70 Stars | 15 Forks

2020-09-07 (MONDAY) - MALSPAM WITH XLS ATTACHMENT HAS MACRO TO PUSH DRIDEX

NOTES:

- After being absent for approximately one month, we started seeing examples of the Cutwail botnet start sending malicious spam (malspam) pushing Dridex again on Monday 2020-09-07.

- Additional Cutail malspam pushing Dridex (with different indicators/files/URLs/etc) has been reported as of Tuesday 2020-09-08.

EMAIL HEADERS FROM MALSPAM EXAMPLE:

Received: from static-ip-1868148155.cable.net.co ([186.81.48.155])

by [removed] for [removed]; Mon, 07 Sep 2020 10:31:43 -0700

X-RC-FROM: <ampulesid792@pje44093.sac.fedex.com>

X-RC-RCPT: [removed]

Received: from [216.44.195.151] (account complicationj8@pje02305.sac.fedex.com HELO tc.ge.pje44093.sac.fedex.com)

by static-ip-1868148155.cable.net.co (Exim 4.89)

with ESMTPA id eEcFf7Fa for [removed]; Mon, 7 Sep 2020 12:31:44 -0500

Received: from ([103.94.107.77]) by static-ip-1868148155.cable.net.co with SMTP id

D41C734C60; Mon, 7 Sep 2020 12:31:44 -0500

Date: Mon, 7 Sep 2020 12:31:44 -0500

From: Derek Rose <Derek.Rose@fedex.com>

Reply-To: Derek Rose <Derek.Rose@fedex.com>

X-Priority: 3 (Normal)

Message-ID: <357520.122031.626cef@pje44093.sac.fedex.com>

Subject: copy of Invoice

ATTACHMENT INFO:

- SHA256 hash: a46b5d45d8ec0fd6f943d694fc9c42d7ae72d33122fb4c0e790d420c1bb53204

- File size: 65,536 bytes

- File name: 20200907_135061.xls

- File description: XLS file with macros for Dridex

URL FROM AT LEAST 40 POSSIBLE URLS GENERATED BY WORD MACRO FOR DRIDEX INSTALLER DLL:

- hxxps://amaimaging[.]net/wp-content/rjkthgowertgoiwe.zip

- hxxps://agencia[.]fal[.]cl/wp-includes/njdfhgeroig.rar

- hxxps://armomaq[.]com/site/ssfisjgniwerg.pdf

- hxxps://axalta[.]grupojenrab[.]mx/wp-admin/ssfisjgniwerg.pdf

- hxxps://bombshellshow[.]me/wp-content/jdfggo.rar

- hxxps://businessquest[.]com.my/schedule/jdfggo.rar

- hxxps://construtorahabite[.]com.br/wpadmin/rjkthgowertgoiwe.zip
- hxxps://coomiponal[.]com/simulador/zxc.zip
- hxxps://discuss[.]ojowa[.]com/themes/wowonder/javascript/tinymce/js/dkfjgbji.gif
- hxxps://eb3tly[.]online/njdfhgeroig.rar
- hxxps://eduserve[.]sezibwa[.]com/images/njdfhgeroig.rar
- hxxps://emyhope[.]com/wp-content/plugins/jetpack/_inc/blocks/84348fh34hf.pdf
- hxxps://etsp[.]org[.]pk/uploads/jdfggo.rar
- hxxps://getsolar4zerodown[.]info/djfhgeh.pdf
- hxxps://glowtank[.]in/js/ssfisjgniwerg.pdf
- hxxps://heraldfashion[.]store/wp-admin/zxc.zip
- hxxps://idklearningcentre[.]com.ng/wp/wp-content/plugins/jetpack/3rd-party/dkfjgbji.gif
- hxxps://igpublica[.]com.br/asset/zxc.zip
- hxxps://inkrites[.]com/wp-content/themes/zerif-lite/ti-prevdem/img/84348fh34hf.pdf
- hxxps://karyagrafis[.]com/njdfhgeroig.rar
- hxxps://leandrokblo[.]com/wp-content/plugins/w3-total-cache/ini/apache_conf/dkfjgbji.gif
- hxxps://leboudoirstquayportrieux[.]fr/image/ssfisjgniwerg.pdf
- hxxps://maisaquihost[.]com[.]br/teste/rjkthgowertgoiwe.zip
- hxxps://manogyam[.]com/storage/njdfhgeroig.rar
- hxxps://mcciorar[.]iglesiamcci[.]cl/njdfhgeroig.rar
- hxxps://medszoo[.]in/jdfggo.rar
- hxxps://minsann[.]se/NewFolder/ad/style/theme/upload/84348fh34hf.pdf
- hxxps://neocuboarquitetura[.]com.br/viewer/ssfisjgniwerg.pdf
- hxxps://pharmacy[.]binarybizz[.]com/vendor/njdfhgeroig.rar
- hxxps://properties[.]igpublica[.]com.br/excelPo/rjkthgowertgoiwe.zip
- hxxps://quiz[.]walkprints[.]com/wp-includes/js/tinymce/themes/inlite/84348fh34hf.pdf
- hxxps://radiantmso[.]com/wp-content/plugins/smart-slider-3/library/media/dkfjgbji.gif

- hxxps://siebuhr[.]com/pmosker/zxc.zip

- hxxps://sjoeberg[.]nu/a/jdfggo.rar

- hxxps://speakerpedia[.]in/images/zxc.zip

- hxxps://sweepegy[.]com/djfhgeh.pdf

- hxxps://tallermecanicoyllantera[.]grupojenrab[.]mx/wp-admin/rjkthgowertgoiwe.zip

- hxxps://timamollo.co.za/sitepro/jdfggo.rar

- hxxps://glowtank.in/js/ssfisjgniwerg.pdf

- hxxps://vyvanse.co/auth14/zxc.zip

RUN METHOD FOR DRIDEX INSTALLER DLL FILES:

- regsvr32.exe -s [file location].

10 EXAMPLES OF LOCATIONS FOR DRIDEX INSTALLER DLL FILES:

- regsvr32.exe -s C:\XMkkdsZZ\PUBWNG\RNidR2AF.

- regsvr32.exe -s C:\Xvnau9kk\vlAShMf\w2lhlvL.

- regsvr32.exe -s C:\Xd6sfzNp\SqFXmRk\T7qme40.

- regsvr32.exe -s C:\XvI7AP77\g8Xj4d2i\x84wFBc7.

- regsvr32.exe -s C:\XZxja5gf\4hfdIbN\EhdtqGg.

- regsvr32.exe -s C:\XpB4rh11\G2Rdy6ci\TyqzIT.

- regsvr32.exe -s C:\X0NTGUzu\Mk9i8nt\FeGhGhc.

- regsvr32.exe -s C:\XKhZMapW\JXxg9R6\CTKfb7Wz.

- regsvr32.exe -s C:\X9MhbII7\Nj1FvD06\GG0TuIm.

- regsvr32.exe -s C:\XBFEYhON\zOp7K1\vQLCbzO.

EXAMPLE OF DRIDEX INSTALLER DLL:

- SHA256 hash: c22118ef67c9a5f09edab92cecb2c4f03768922373b1078c6a8a3b3418e1efe3

- File size: 335,872 bytes

- File location: hxxps://construtorahabite[.]com.br/wpadmin/rjkthgowertgoiwe.zip

- File location: C:\XUseXl0b\OaJ2ENt\5VqlBbnN

- File description: DLL file retrieved by XLS macros, used to install Dridex

3 LOCATIONS WHERE DRIDEX WAS PERSISTENT ON AN INFECTED WINDOWS HOST IN OUR LAB:

- SHA256 hash: 733f1f153f1ac4de67d435e48a585c8acc9d5701ac1869fb55fadc23e9358d69

- File size: 1,013,760 bytes

- File location: C:\Users\[username]\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Document Themes\1kNIz\VERSION.dll

- File description: Dridex DLL run by copy of legitimate system file sigverif.exe in the same directory, made persistent through a Windows registry update

- SHA256 hash: b7982ba52fa405eb15db53c75390e820a030e64147d236f090c2d21cf0865922

- File size: 1,015,296 bytes

- File location: C:\Users\[username]\AppData\Roaming\Microsoft\Internet Explorer\UserData\Jov5Cwf8Pz3\FVEWIZ.dll

- File description: Dridex DLL run by copy of legitimate system file BitLockerWizard.exe in the same directory, persistent through a scheduled task

- SHA256 hash: 292082e29db3264946e3e6aa1c42e929a76cb3ad4a9a0299d9a881f429c29935

- File size: 1,295,872 bytes

- File location: C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\Kf\DUI70.dll

- File description: Dridex DLL run by copy of legitimate system file msdt.exe in the same directory, persistent through a startup menu shortcut

POST-INFECTION HTTPS TRAFFIC FROM DRIDEX-INFECTED HOST:

- 45.79.8[.]25 port 443 - HTTPS traffic (certificate issuer data follows):

-- id-at-countryName=DE

-- id-at-stateOrProvinceName=Sheso thanthefo

-- id-at-localityName=Berlin

-- id-at-organizationName=Thedelor Tbrra SICAV

-- id-at-organizationalUnitName=5Coiesily Begtherdr istwarscon

-- id-at-commonName=Bath7epran.toshiba

- 54.39.34[.]26 port 453 - HTTPS traffic (certificate issuer data follows):

-- id-at-countryName=TR

-- id-at-stateOrProvinceName=Thereb

-- id-at-localityName=Ankara

-- id-at-organizationName=Atercon Urlelgrks SAS

-- id-at-organizationalUnitName=4ondmusepr and Omibyndtr

-- id-at-commonName=Mecri.swenw.tube