Malware-Traffic-Analysis.net - 2017-12-22 - Remcos RAT infection from RTF using CVE-2017-0199 exploit

NOTICE:

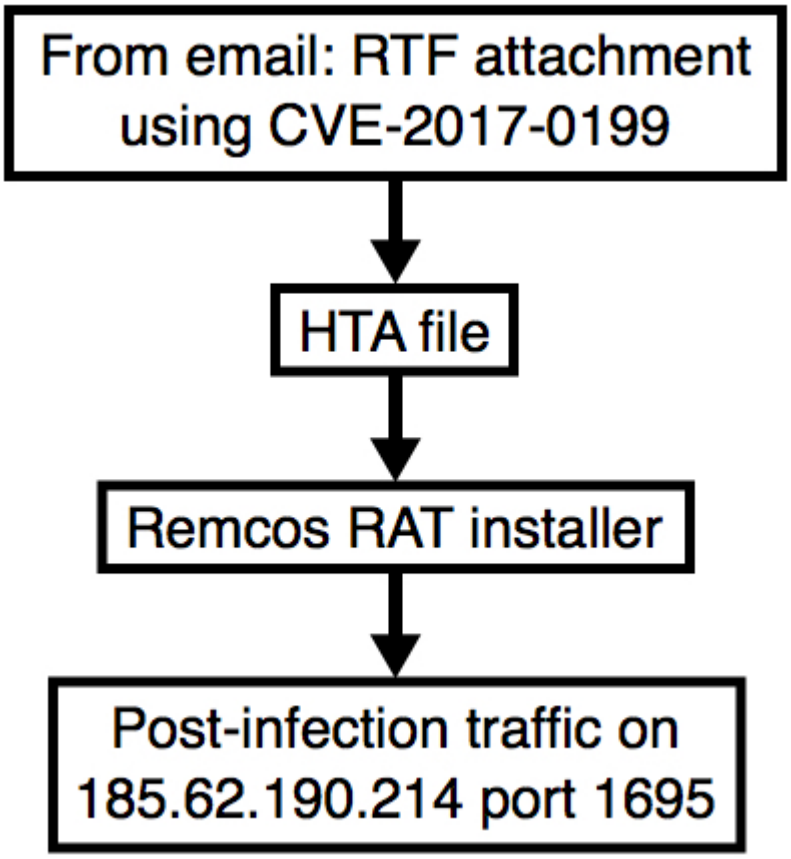
- The zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

ASSOCIATED FILES:

- 2017-12-22-Remcos-RAT-malspam-example.eml.zip 39.9 kB (39,866 bytes)
- 2017-12-22-Remcos-RAT-infection-traffic.pcap.zip 1.0 MB (1,044,961 bytes)
- 2017-12-22-malware-from-Remcos-RAT-infection.zip 1.9 MB (1,880,322 bytes)

NOTES:

- On 2017-12-21, I saw malspam dated 2017-12-21 with an RTF attachment using CVE-2017-0199 to push Remcos RAT.
- Today's post-infection traffic is similar to Remcos RAT post-infection traffic I reported almost 2 months ago on 2017-10-27.



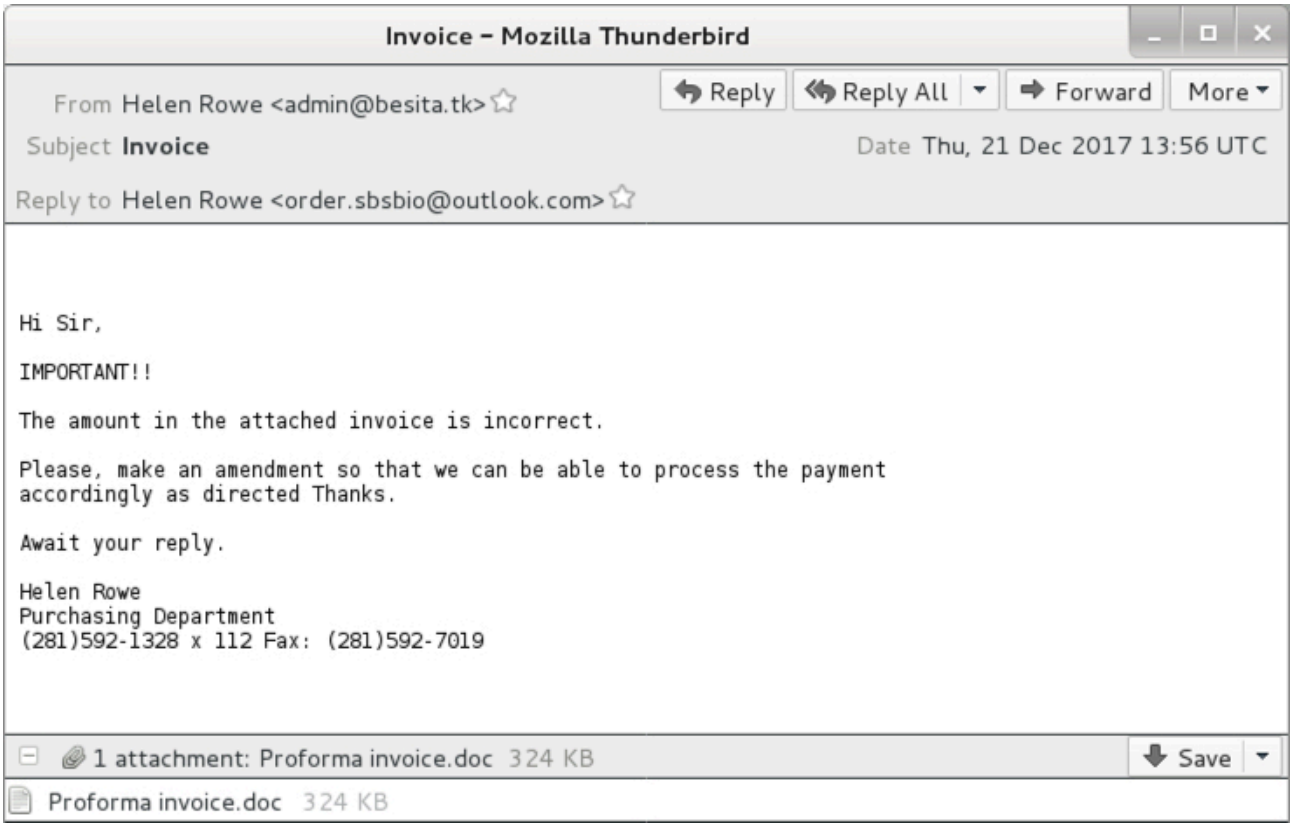
Shown above: Flowchart for today's infection.

WEB TRAFFIC BLOCK LIST

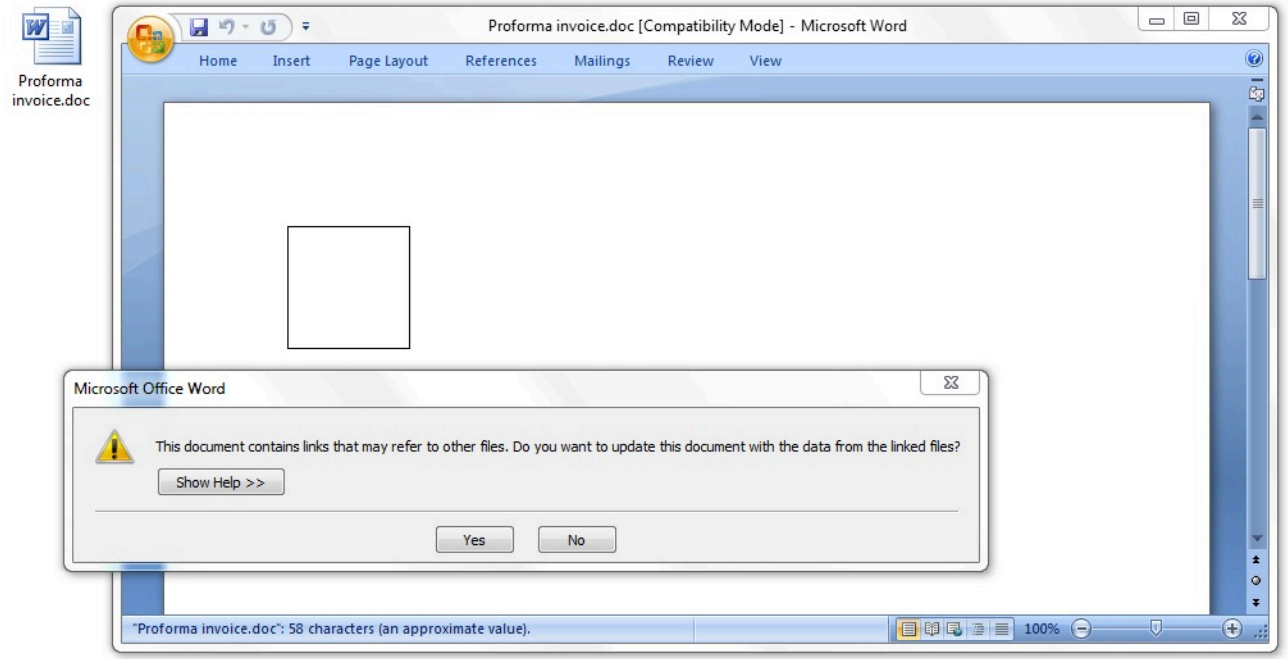
Indicators are not a block list. If you feel the need to block web traffic, I suggest the following domains and URLs:

- hxxps[:]//streetsave[.]club/styles/break/beta.hta
- hxxps[:]//regwide[.]club/images/scale/nile.php
- hxxps[:]//regwide[.]club/images/scale/nite.exe
- darlz.freeddns[.]org

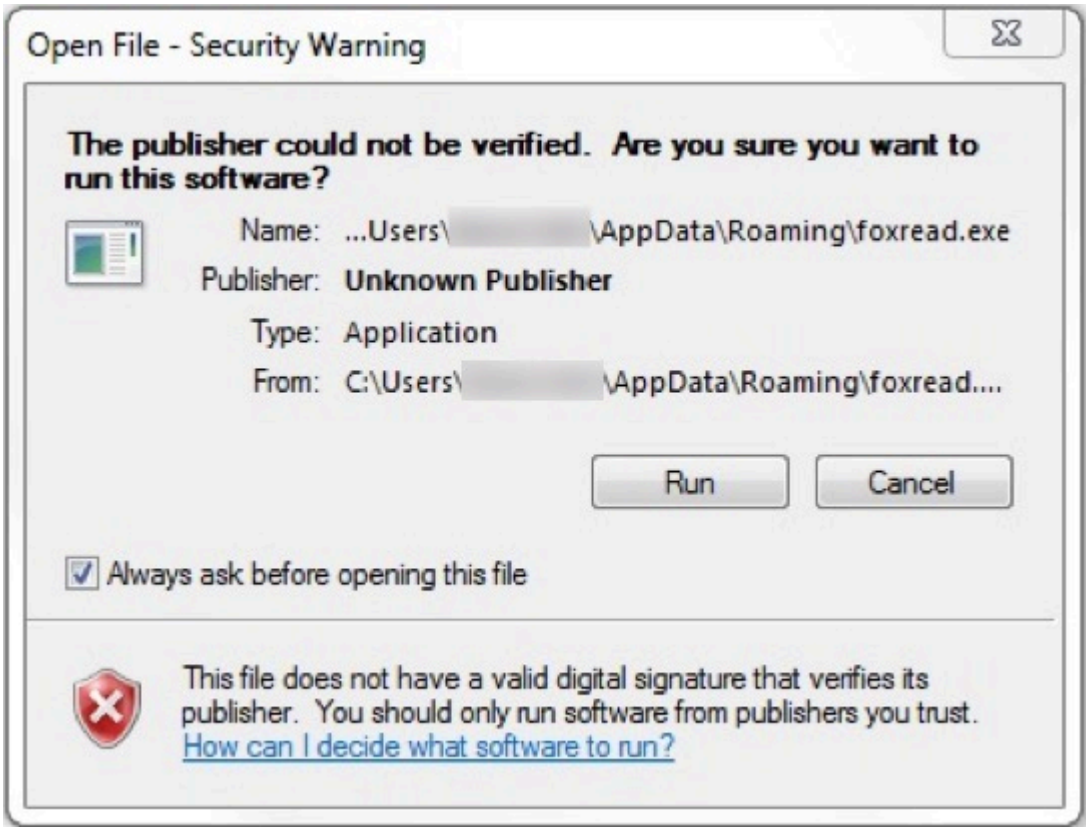
IMAGES



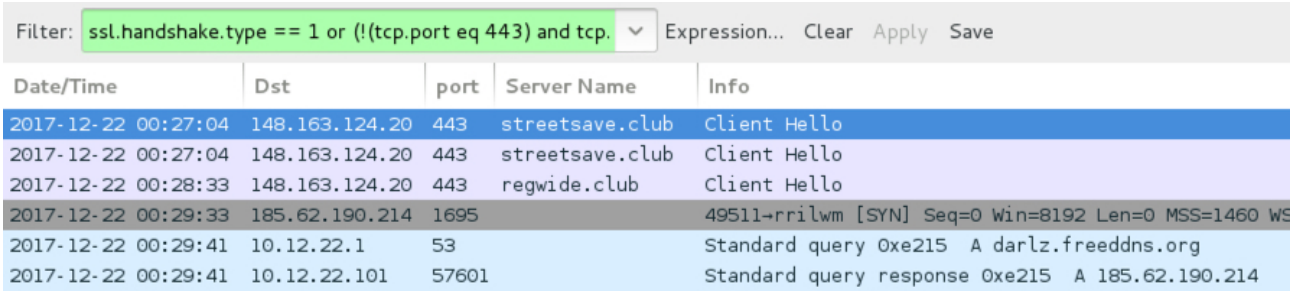
Shown above: Screenshot of the email.



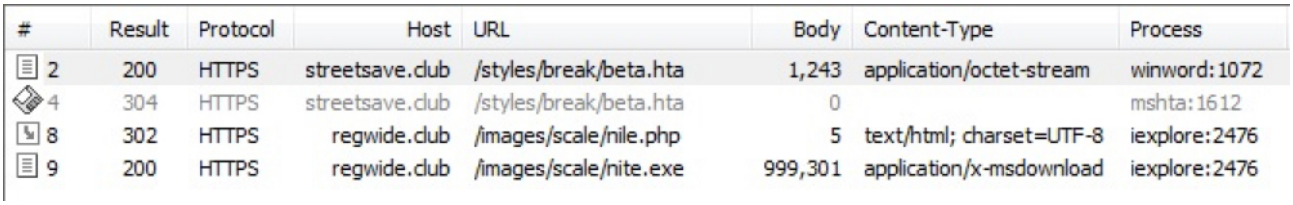
Shown above: The attached .doc file is actually an RTF that uses CVE-2017-0199. I clicked my way "yes" to an infection!



Shown above: The exectuable for Remcos RAT needed my permission to run.



Shown above: Traffic from the infection filtered in Wireshark.



Shown above: HTTPS traffic as seen in Fiddler.

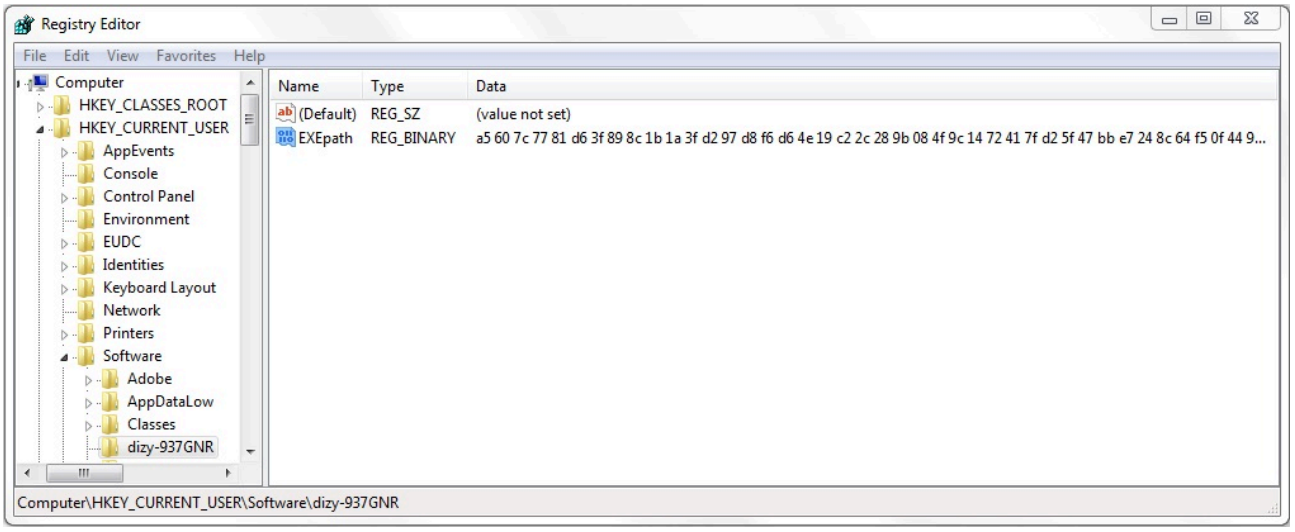
Date/Time	Src	port	Dst	port	Info
2017-12-22 00:29:33	10.12.22.101	49511	185.62.190.214	1695	49511→rrilwm [SYN] Seq=0 Win=8192 Len=0 MSS=1
2017-12-22 00:29:34	185.62.190.214	1695	10.12.22.101	49511	rrilwm→49511 [SYN, ACK] Seq=0 Ack=1 Win=8192 L
2017-12-22 00:29:34	10.12.22.101	49511	185.62.190.214	1695	49511→rrilwm [ACK] Seq=1 Ack=1 Win=65536 Len=0

Follow TCP Stream (tcp.stream eq 3)

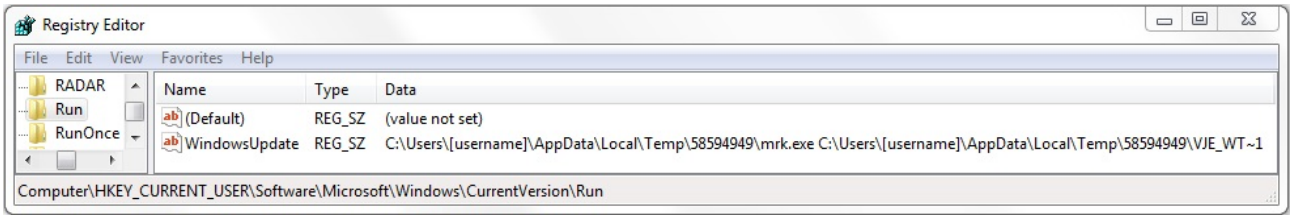
Stream Content

```
.j..'..*.B..N..?.W.!D.....n.Jo
[..u3G.xC.of.......@.Q%)6e4 .'W5..s....b5....*.q.CH..I...?m.......=.."..W.V...
[7...G.-}........P........2...c....>._Jy..w.!..>...t....*......7!(...|fx....Q=x.{/.b..C...U
[2..w..'..6.....{.R.CO......./.j...w.G......^.h.. .....T....@.....H..c.m..8......g.D.Y.q.
{....a.m!.fk.....1.~X[q,...;`|.lm...>.....5t(..6....Tg....K..20.#\..S..
....n...CS.d..5b.7.@g.V.4 ...Y.....U.wR{=.E..J.L...].UP..yeq<...w)31\...
\e..uX...u..a.U......za|.;,...TOS..Z...f.a
V............c..|
S.....'......O.m@....?..........lb..s)....A.....B.a....Y..:g.#..p.......W......v......hz 4.t
\C;........4.........q..7A.....i...+....JV..&k+..o..b.>...>.*b...f{g[|
C...R...T].JL...."e5.2.JB=9...k.X...h.9}M.1...j..v..h...w>..%B..........~.[U.b.l<.~Z.%.K.Y.<..Su.7OC..
.X..D....d.v.(g.-.j..'..*.B..L....].8P.....l.ZzI..j..'..*.B.qL....].8P.....l.Zz8>..DWn...|
=..k..R..).OmGy.f..AzT..O....>\....Zm5."...(..nm.jb....2n..(..c.\..k.
$L..Q..,.....j..'..*.B..L....].8P.....l.ZzI..j..'..*.B.sL....].8P.....l.Zz+>..wW\.
.|=..k..R..%.=mLy.fI.Lz...O.....\....XmQ.....+..n{.`b....<n..*....[..%.%...V./
d........j..'..*.B..L....].8P.....l.ZzI..j..'..*.B.nL....].8P.....l.Zz8>..DWn...|
=..k..R..).OmGy.f..AzT..O....>\....Zm5."...(..ns.jb....7n>......8..%KzT....r/........@
...j..'..*.B..L....].8P.....l.ZzI..j..'..*.B./
L....].8P.....l.Zz4>..lWR...w=..d..6..x.a.J......B....j..'..*.B..L....].8P.....l.ZzI..j..'..*.B./
L....].8P.....l.Zz4>..lWR...w=..d..6..q.b.J......B....j..'..*.B..L....].8P.....l.ZzI..j..'..*.B.oL....].
8P.....l.Zz8>..DWn...|=..k..R..).OmGy.f..AzT..O....>\....Zm5."...(..ns.jb....7n>......8..%
KzT....sd........K
..j..'..*.B..L....].8P.....l.ZzI..j..'..*.B.4L....].8P.....l.Zz>>..DWG..be.S.d..6..u.i^.O.j..'..*.B..
L....].8P.....l.ZzI..j..'..*.B.UL....].8P.....l.ZzN>..-W..L. =R.!..R..2.>mYy.fR.Sz
\..O....8....I...w...}!..j..'..*.B..L....].8P.....l.ZzI..j..'..*.B."L....].8P.....l.Zz)>...WR...m=..a..
```

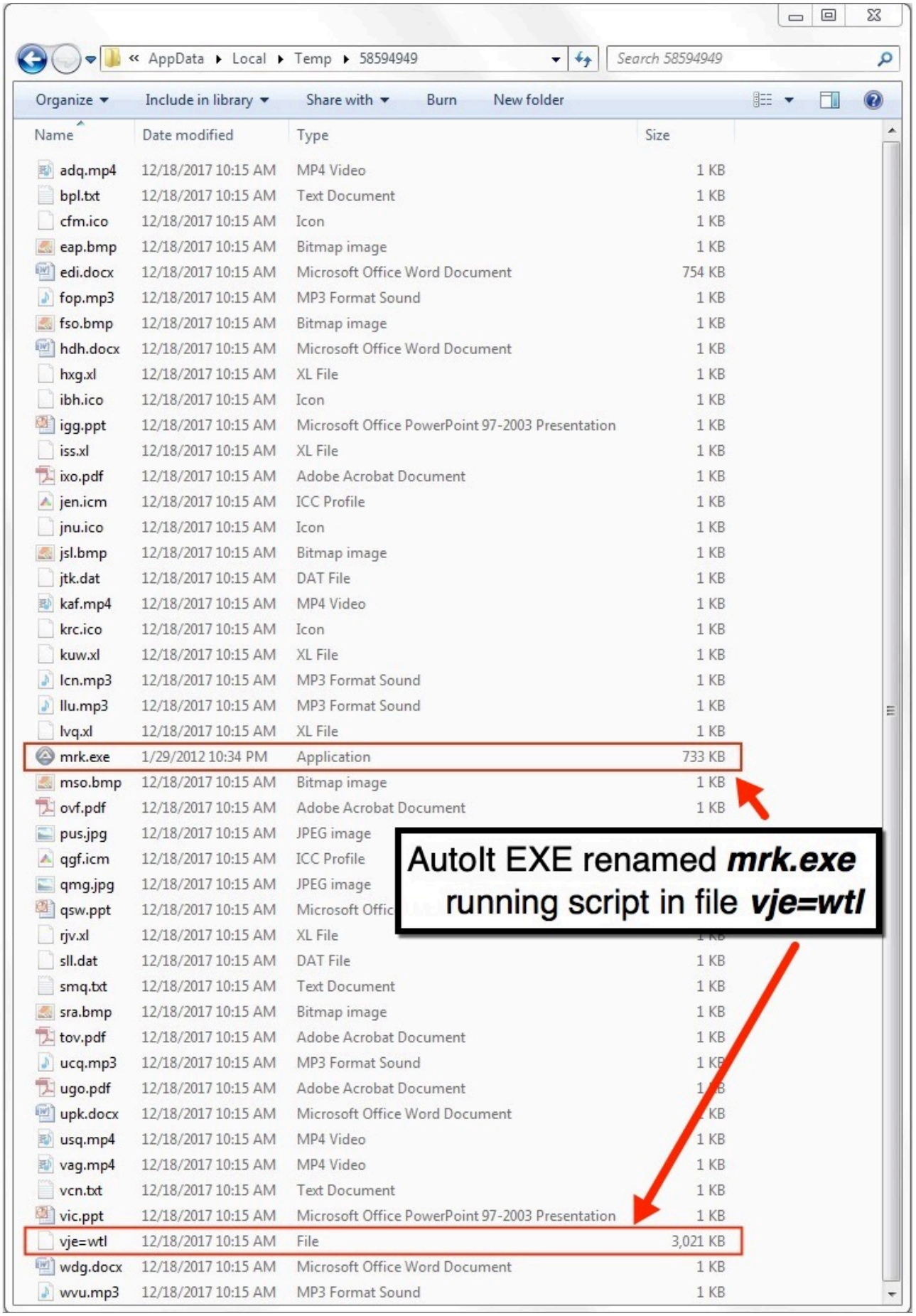
Shown above: Post-infection traffic from the Remcos RAT-infected host.



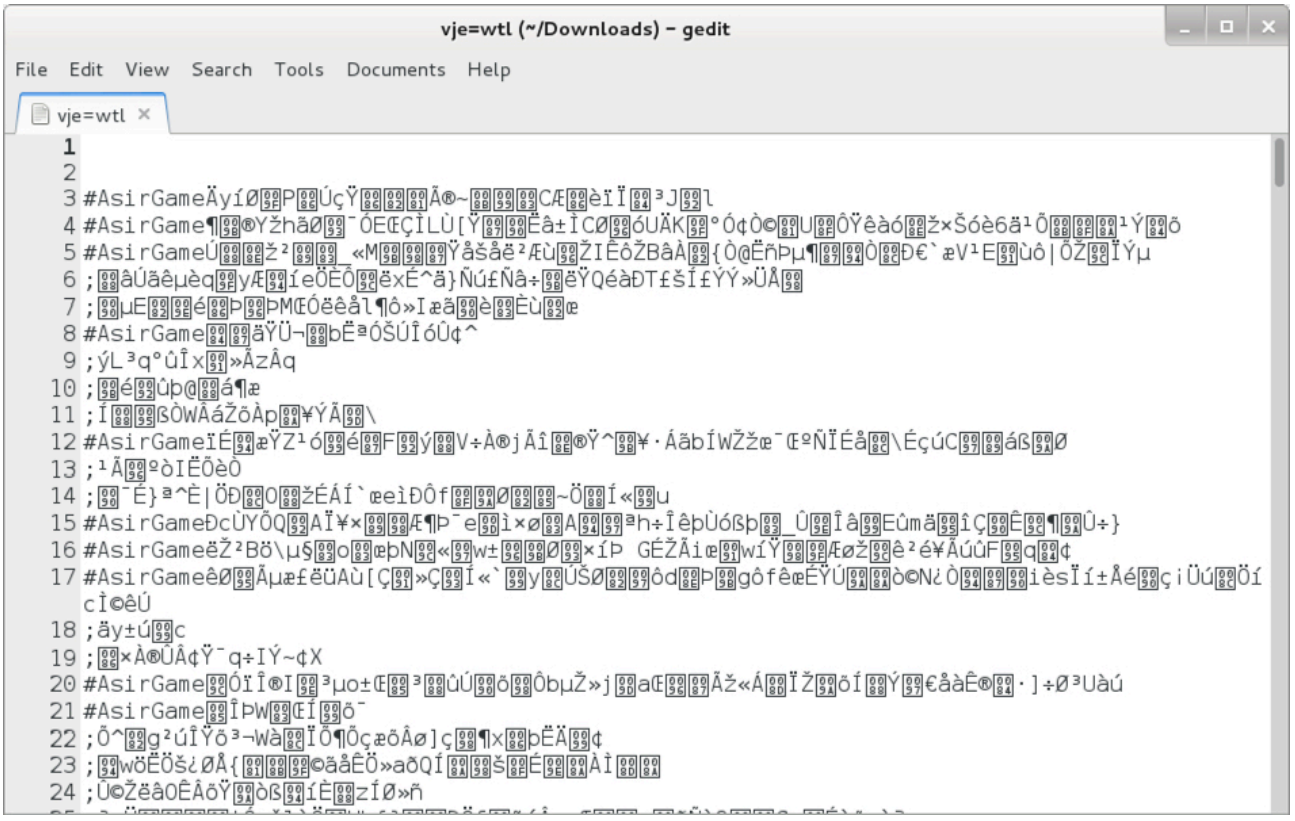
Shown above: Randomly-named key with binary data in the Windows registry.



Shown above: Updated key in the Windows registry to keep the infection persistent.



*Shown above: Folder in the user's **AppData/Local/Temp** directory.*



*Shown above: File run by the AutoIt script engine, **vje=wtl**, as seen in a text editor.*

INDICATORS

EMAIL DATA:

- Date: Thursday, 2017-12-21 at 13:56 UTC
- Subject: Invoice
- From: "Helen Rowe" <admin@besita[.]tk>
- Reply-To: "Helen Rowe" <order.sbsbio@outlook[.]com>
- Message-ID: <b98edd6e87c6201c7056c859bb73b48a.squirrel@212.237.6[.]14>
- User-Agent: SquirrelMail/1.4.22
- Attachment: Proforma invoice.doc

TRAFFIC:

- 148.164.124[.]20 port 443 - **streetsave[.]club** - GET /styles/break/beta.hta (HTTPS)
- 148.164.124[.]20 port 443 - **regwide[.]club** - GET /images/scale/nile.php (HTTPS)
- 148.164.124[.]20 port 443 - **regwide[.]club** - GET /images/scale/nite.exe (HTTPS)
- 185.62.190[.]214 por 1695 - **darlz.freeddns[.]org** - encrypted post-infection traffic caused by Remcos RAT

MALWARE AND ARTIFACTS FROM THE INFECTED WINDOWS HOST:

- SHA256 hash:&bnsp; 1b78b77b4f571548df7d7a7e324bfe38425b901663906d91d7c5ec110a333a07
  File size:&bnsp; 332,066 bytes

File name:&bnsp; Proforma invoice.doc
File description:&bnsp; RTF document using CVE-2017-0199

- SHA256 hash:&bnsp; 402517926305219d9d482063334b9955866fbeb7fadd5fe9e0f72cc04a112173
  File size:&bnsp; 1,243 bytes
  File name:&bnsp; beta.hta
  File description:&bnsp; HTML application (HTA) file to download the next-stage malware

- SHA256 hash:&bnsp; 9717a2ec51316ca3b97d5c379e4b331e03e274dfd6de5433f3382b760f09b51b
  File size:&bnsp; 999,301 bytes
  File location:&bnsp; C:\Users*[username]*\AppData\Roaming\foxread.exe
  File description:&bnsp; RemcosRAT Installer for next stage of the infection

- SHA256 hash:&bnsp; fb73a819b37523126c7708a1d06f3b8825fa60c926154ab2d511ba668f49dc4b
  File size:&bnsp; 750,320 bytes
  File location:&bnsp; C:\Users*[username]*\AppData\Local\Temp\58594949\mrk.exe
  File description:&bnsp; AutoIt v3 script engine (version 3.3.8.1) NOTE: This is a legitimate file. It is not inherently malicious.

- SHA256 hash:&bnsp; fd00256c375f5d744d73a7ddba571f1887779af042bd6cf7100533c68c461a33
  File size:&bnsp; 3,092,687 bytes
  File location:&bnsp; C:\Users*[username]*\AppData\Local\Temp\58594949\vje=wtl
  File description:&bnsp; AutoIt script file executed by mrk.exe

WINDOWS REGISTRY UPDATES:

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
  "WindowsUpdate"="C:\\Users\\[username]\\AppData\\Local\\Temp\\58594949\\mrk.exe C:\\Users\\[username]\\AppData\\Local\\Temp\\58594949\\VJE_WT~1"

- [HKEY_CURRENT_USER\Software\dizy-937GNR]
  "EXEpath"=hex:a5,60,7c,77,81,d6,3f,89,8c,1b,1a,3f,d2,97,d8,f6,d6,4e,19,c2,2c,\
  28,9b,08,4f,9c,14,72,41,7f,d2,5f,47,bb,e7,24,8c,64,f5,0f,44,91,cb,54,5f,1a,\
  ba,bc,67,e6,94,1a,c0,54,66,67,c0,79,55,c1,8f,7c,29,3e,8a,08,bc,ed,f9,3f,5f,\
  6d,17,22,66,b1,c8,c8,a3,e0,27,f2,ac,f3,82,3b,ed,3e,2a,69,56,21,8b,85,f4,c0,\
  35,47,be,02,9f,d0,a0,c7,2a,f0,87,28,83,42,7c,97,2d,90,3b,c3

Click here to return to the main page.
