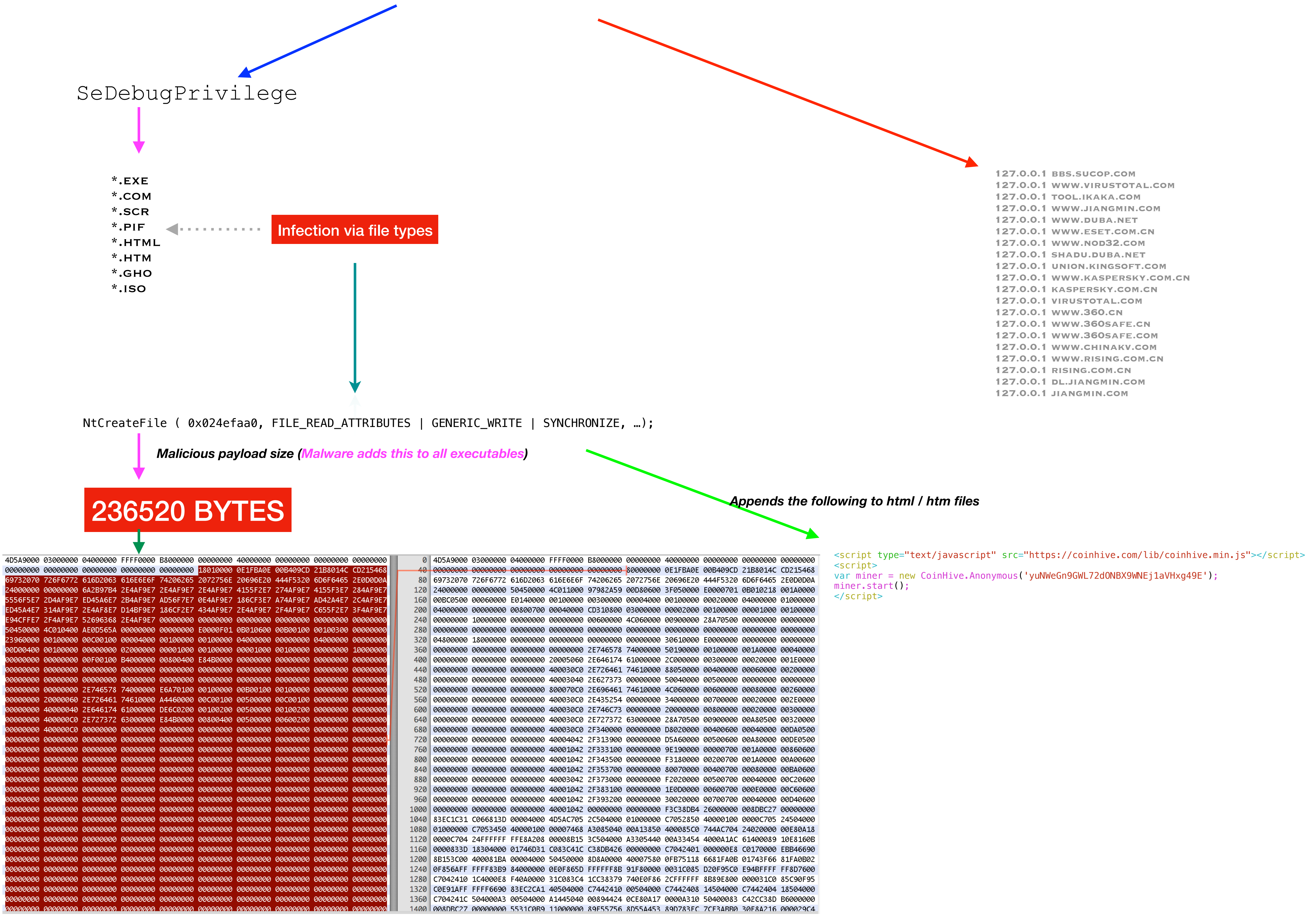
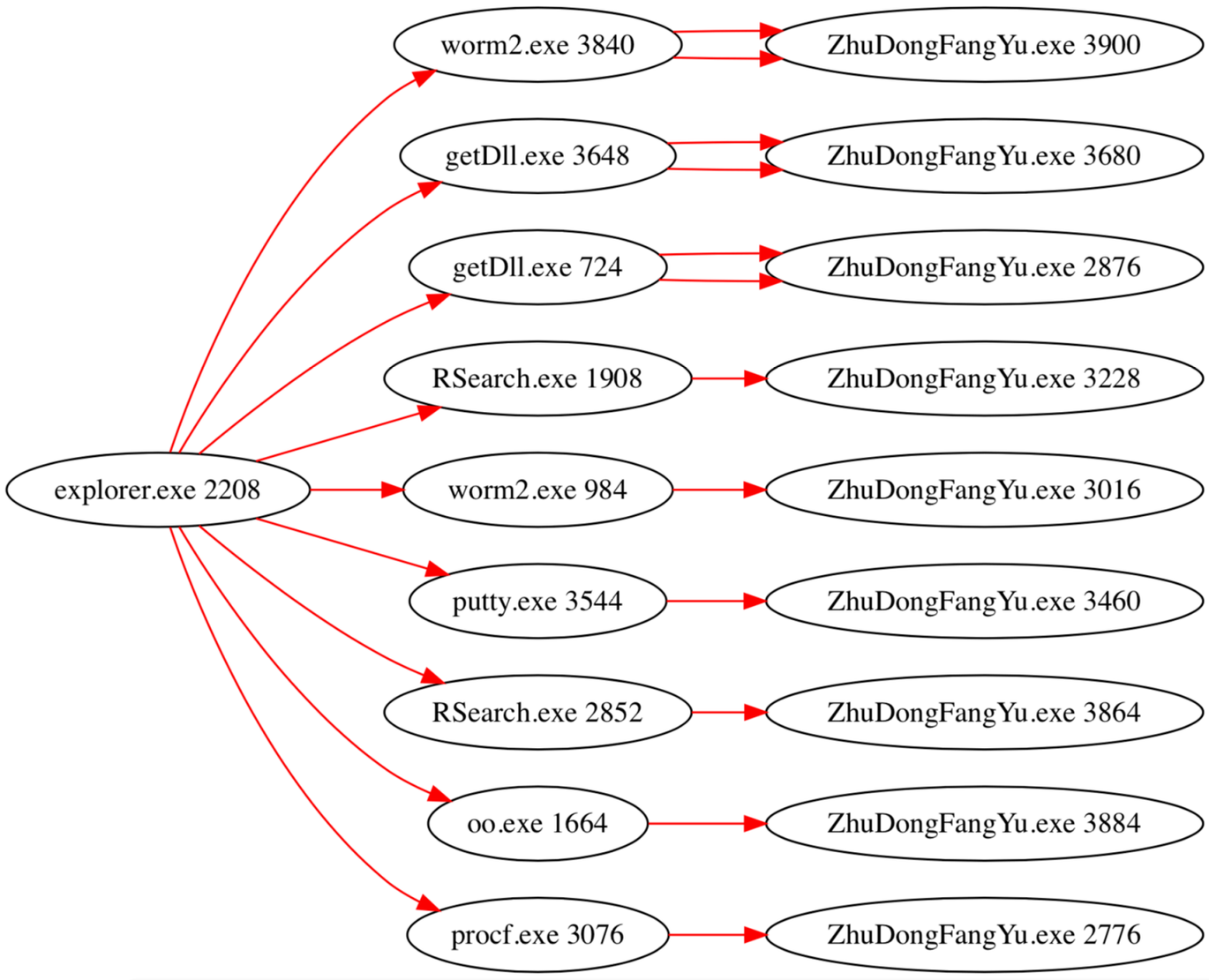
Payload infects other files and changes the hosts file



Flow

Once infection takes place, all executables are modified with the malicious payload. In the following flow you can see that putty is launching the malicious payload



Each payload enumerates through files and check for new files for infection

```
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\17a63397\foo123.exe ** 510952
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\17b43859\conf.exe ** 2125635
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\17b43859\hlow.exe ** 1370692
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\17b43859\smsniff.exe ** 327864
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\193d367d\EXP01\foo.exe ** 1268906
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\1a0125b8\i.exe ** 770536
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\1b382e32\P_AV.exe ** 1386472
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\1b392dac\wanaCry.exe ** 3959784
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\1d3979a6\Project1.exe ** 2005520
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\1db2398e\onlyDataNew.exe ** 1840104
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\1fa42b11\504lab-32bit.exe ** 3539002
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\20c7356f\svchost_brute.exe ** 1221310
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\21e8301b\ee.exe ** 523752
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\22fd7b98\lsm0.exe ** 1983254
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\2361256c\Compiled\Furutaka.exe ** 334312
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\24d8328d\sidf32.exe ** 1831400
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\25c475c9\ntertmgr64.exe ** 1072104
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\25fe766e\ABCDE.exe ** 717090
F: \Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\265f33c8\drop_32.exe ** 1239766
```

Traffic flow (COIN-HIVE)

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.145      TO IP ADDRESS 217.182.164.13
        PORT INFORMATION (49301, 443)
        SEQUENCE INFORMATION (2290020932, 3425430946)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (174)
    16 03 01 00 73 01 00 00 6F 03 01 5A A6 62 70 27         ....s...o..Z.bp'
    AE 33 54 9B 92 35 6D D9 03 50 BE 79 76 F8 47 D6         .3T..5m..P.yv.G.
    B7 C5 EF 71 81 85 04 83 22 0D C0 00 00 18 00 2F         ...q...."....../
    00 35 00 05 00 0A C0 13 C0 14 C0 09 C0 0A 00 32         .5.............2
    00 38 00 13 00 04 01 00 00 2E 00 00 00 11 00 0F         .8..............
    00 00 0C 63 6F 69 6E 68 69 76 65 2E 63 6F 6D 00         ...coinhive.com.
    05 00 05 01 00 00 00 00 00 0A 00 06 00 04 00 17         ................
    00 18 00 0B 00 02 01 00                                 ........


    16 03 01 00 58 02 00 00 54 03 01 D5 90 0A 43 ED         ....X...T.....C.
    5B FE 9F DA FD 86 AC DE 12 CC B1 EE EF 81 D3 C8         [...............
    D2 82 2C 64 5C 2C AC B3 DD 00 DD 20 81 59 73 D0         ..,d\,..... .Ys.
    E5 DF 46 8D 94 24 9A FA E1 2F ED 9D AF 14 84 0F         ..F..$.../......
    3F 53 2F 22 B7 11 D7 A0 3D B9 A2 5C C0 13 00 00         ?S/"....=..\....
    0C 00 00 00 00 00 0B 00 04 03 00 01 02 16 03 01         ................
    10 E9 0B 00 10 E5 00 10 E2 00 05 55 30 82 05 51         ...........U0..Q
    30 82 04 39 A0 03 02 01 02 02 10 0A E1 E6 BD 51         0..9...........Q
    FB 3D 8F 06 BE 0D B5 5E BD E9 DF 30 0D 06 09 2A         .=.....^...0...*
    86 48 86 F7 0D 01 01 0B 05 00 30 81 90 31 0B 30         .H........0..1.0
    09 06 03 55 04 06 13 02 47 42 31 1B 30 19 06 03         ...U....GB1.0...
    55 04 08 13 12 47 72 65 61 74 65 72 20 4D 61 6E         U....Greater Man
    63 68 65 73 74 65 72 31 10 30 0E 06 03 55 04 07         chester1.0...U..
    13 07 53 61 6C 66 6F 72 64 31 1A 30 18 06 03 55         ..Salford1.0...U
    04 0A 13 11 43 4F 4D 4F 44 4F 20 43 41 20 4C 69         ....COMODO CA Li
    6D 69 74 65 64 31 36 30 34 06 03 55 04 03 13 2D         mited1604..U...-
    43 4F 4D 4F 44 4F 20 52 53 41 20 44 6F 6D 61 69         COMODO RSA Domai
    6E 20 56 61 6C 69 64 61 74 69 6F 6E 20 53 65 63         n Validation Sec
    75 72 65 20 53 65 72 76 65 72 20 43 41 30 1E 17         ure Server CA0..
    0D 31 37 30 39 32 38 30 30 30 30 30 30 5A 17 0D         .170928000000Z..
    31 38 30 39 32 38 32 33 35 39 35 39 5A 30 5B 31         180928235959Z0[1
    21 30 1F 06 03 55 04 0B 13 18 44 6F 6D 61 69 6E         !0...U....Domain
    20 43 6F 6E 74 72 6F 6C 20 56 61 6C 69 64 61 74          Control Validat
```