

SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

 isc.sans.edu/diary/25934

Published: 2020-03-23

Last Updated: 2020-03-23 18:31:52 UTC

by [Didier Stevens](#) (Version: 1)

I have other samples like the malware I covered in yesterday's diary entry.

All with the same body and attachment, it's just the sender that varies. The PowerShell scripts are the same and download from show1[.]website. Like I wrote yesterday, three files are downloaded:

1. A legitimate, signed [Autolt interpreter](#) (this is not malware)
2. A heavily obfuscated [Autolt script, that is encoded as a PEM certificate](#)
3. An [encrypted EXE](#): KPOT info stealer

The PowerShell script uses certutil to BASE64-decode the "certificate" to the Autolt script, and then launches the Autolt interpreter with the script as argument.

The Autolt script contains process hollowing shellcode (known as [frenchy_shellcode](#)), that decrypts the encrypted PE file as guest and uses 32-bit dllhost.exe as host (as process hollowing host, not as dll host).

The PH shellcode contains mutex name "frenchy_shellcode_06", but this name is randomized by the Autolt script before it is injected and executed.

As the decrypted KPOT EXE is never written to disk, it was unknown by VirusTotal. I did [submit](#) it today.

KPOT is an infostealer, as can be guessed from the strings found inside the executable:

```
SANS ISC C:\Demo>strings.py guest.exe.vir | tail -n 20
IMAP Password
POP3 Server
POP3 Port
POP3 User
POP3 Password
IMAP_Server
IMAP_User_Name
IMAP_Password2
POP3_Server
POP3_User_Name
POP3_Password2
account*.oeaccount
%s\s\s.vdf
%s\s\s.vdf
Name: %1s
Comment: %1s
User: %1s
Data:
%2.2X
%-50s %s

SANS ISC C:\Demo>
```

More interesting strings are simply XOR-encoded (1-byte key).

Like the C2:

```
SANS ISC C:\Demo>xorsearch guest.exe.vir http
Found XOR 16 position 2D80: http://%s.....<.....R+...E.....P
Found XOR 4C position 2ACF: http.dlllnpwpw|m7}uuLx.20.-8>xLLL.....LLL$;%LLLL.
Found XOR 95 position 3854: http://krt1.site;http://krt2.site;http://krt3.site
Found XOR 95 position 3865: http://krt2.site;http://krt3.site;.....
Found XOR 95 position 3876: http://krt3.site;.....
Found XOR A7 position 2D60: https://%S/r/%S.....K^^T^^^T".....<.
Found XOR D6 position 2D70: https://%S/a/%S.....Mjvq?% V.....
Found XOR D7 position 2E36: http...-*.scONTENT.lENgTH.

SANS ISC C:\Demo>
```

And the targets:

```
SANS ISC C:\Demo>xorsearch -n 30 -i guest.exe.vir "|%s|"
Found XOR 42 position 37AE(-30): .....BBBB2|NordVPN| %s %s |..B.....BB....
Found XOR 42 position 37B1(-30): .....BBBB2|NordVPN| %s %s |..B.....BB....
Found XOR 49 position 372C(-30): .....IIII1|TotalCommander %s %s |..IIII.....
Found XOR 49 position 372F(-30): .....IIII1|TotalCommander %s %s |..IIII.....
Found XOR 49 position 3732(-30): .....IIII1|TotalCommander %s %s |..IIII.....
Found XOR 4D position 3764(-30): .....MMMM3|Pidgin %s %s |..MMMM.P|_E...P...P...P
Found XOR 4D position 3767(-30): .....MMMM3|Pidgin %s %s |..MMMM.P|_E...P...P...P!&M
Found XOR 4D position 376A(-30): .....MMMM3|Pidgin %s %s |..MMMM.P|_E...P...P...P!&MMMM
Found XOR 50 position 2F8A(-30): .....P.....PPNormal %s %s |%02d/%04d| %s..P.....
Found XOR 50 position 2F8D(-30): .....P.....PPNormal %s %s |%02d/%04d| %s..P.....
Found XOR 5C position 381E(-30): .....\\5|Windows Mail %s %s |..\\JU>HKXj}Cc~.ld~y\\
Found XOR 5C position 3821(-30): .....\\5|Windows Mail %s %s |..\\JU>HKXj}Cc~.ld~y\\
Found XOR 5C position 3824(-30): .....\\5|Windows Mail %s %s |..\\JU>HKXj}Cc~.ld~y\\
Found XOR 61 position 377C(-30): |EHKEBP..P..P!&aaaa3|Psi(+) %s %s |..aaaa.....
Found XOR 61 position 377F(-30): KEBP..P..P!&aaaa3|Psi(+) %s %s |..aaaa.....
Found XOR 61 position 3782(-30): P..P..P!&aaaa3|Psi(+) %s %s |..aaaa.....
Found XOR 96 position 37CD(-30): .....E.JE.jE.JE.JE.JE.J43..0 %s %s |%S...`u#,u#,u#,u#|J
Found XOR 96 position 37D0(-30): .....E.JE.jE.JE.JE.JE.J43..0 %s %s |%S...`u#,u#,u#,u#|JZ...
Found XOR 96 position 37D3(-30): .....E.JE.jE.JE.JE.JE.J43..0 %s %s |%S...`u#,u#,u#,u#|JZ...=
Found XOR 96 position 37D6(-30): .....E.JE.jE.JE.JE.JE.J43..0 %s %s |%S...`u#,u#,u#,u#|JZ...=tG}
Found XOR 9E position 3803(-30): }+}$)+$)+$UR...5|Outlook %s %d %s %s |.....
Found XOR 9E position 3806(-30): }+}$)+$UR...5|Outlook %s %d %s %s |.....
Found XOR A0 position 374C(-30): .....4|Remote Desktop %s %s |.....
Found XOR A0 position 374F(-30): .....4|Remote Desktop %s %s |.....
Found XOR A0 position 3752(-30): .....4|Remote Desktop %s %s |.....
Found XOR A6 position 2FA6(-30): .....Masked %s %s |%02d/%04d| %s %s %s.....
Found XOR A6 position 2FB3(-30): .....Masked %s %s |%02d/%04d| %s %s %s.....
Found XOR A6 position 2FB6(-30): .....Masked %s %s |%02d/%04d| %s %s %s.....
Found XOR AF position 37B9(-30): 4bm.....0 %s %s |%S...E.jE.JE.JE.JE.
Found XOR AF position 37BC(-30): .....0 %s %s |%S...E.jE.JE.JE.JE.j43
Found XOR AF position 37BF(-30): .....0 %s %s |%S...E.jE.JE.JE.JE.j43..Y
Found XOR AF position 37C2(-30): .....0 %s %s |%S...E.jE.JE.JE.JE.j43..Y.L
Found XOR BE position 3797(-30): .....2|EarthVPN| %s %s |.....!
Found XOR BE position 379A(-30): .....2|EarthVPN| %s %s |.....!m4b
Found XOR C6 position 370C(-30): FBnWEAm4bm4bm4Bm.....1|WinSCP %s %s |.....
Found XOR C6 position 370F(-30): WEAm4bm4bm4Bm.....1|WinSCP %s %s |.....
Found XOR C6 position 3712(-30): m4bm4bm4Bm.....1|WinSCP %s %s |.....
Found XOR C6 position 37E1(-30): L..L.dc..`u, u#,u#,u#,u.#.JZ..0 %s %s |%S...m$.-,4773$)+b}<
Found XOR C6 position 37E4(-30): L..L.dc..`u, u#,u#,u#,u.#.JZ..0 %s %s |%S...m$.-,4773$)+b}<($)+
Found XOR C6 position 37E7(-30): c..`u, u#,u#,u#,u.#.JZ..0 %s %s |%S...m$.-,4773$)+b}<($)+$)+
Found XOR C6 position 37EA(-30): `u, u#,u#,u#,u.#.JZ..0 %s %s |%S...m$.-,4773$)+b}<($)+$)+$UR
Found XOR D7 position 36F4(-30): uFCCNS.\.\S.\S.|S"%..1|WS_FTP %s %s |.....mFx.BRAm4bm4bm4bm
Found XOR D7 position 36F7(-30): CNS.\.\S.\S.|S"%..1|WS_FTP %s %s |.....mFx.BRAm4bm4bm4bm...
Found XOR D7 position 36FA(-30): .\.\S.\S.|S"%..1|WS_FTP %s %s |.....mFx.BRAm4bm4bm4bm.....
Found XOR F8 position 36E1(-30): .....1|FileZilla %s %s |%S|.....Sx|pi{.S.\S.\S.|S"%...
Found XOR F8 position 36E4(-30): .....1|FileZilla %s %s |%S|.....Sx|pi{.S.\S.\S.|S"%...B
Found ADD A0 position 374C(-30): .....4|.emote .esktop %s %s |MJ.....
Found ADD A0 position 374F(-30): .....4|.emote .esktop %s %s |MJ.....
Found ADD A0 position 3752(-30): .....4|.emote .esktop %s %s |MJ.....

SANS ISC C:\Demo>
```

Usually, I explain in detail my analysis steps, so that you can reproduce them. I will do this too for this executable in one or more upcoming diary entries.

Didier Stevens
Senior handler
Microsoft MVP
blog.DidierStevens.com DidierStevensLabs.com

DEV522 Defending Web Application Security Essentials **LEARN MORE**
Learn to defend your apps before they're hacked