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 AutoIt interpreter (this is not malware)
2. A heavily obfuscated AutoIt script, that is encoded as a PEM certificate
3. An encrypted EXE: KPOT info stealer

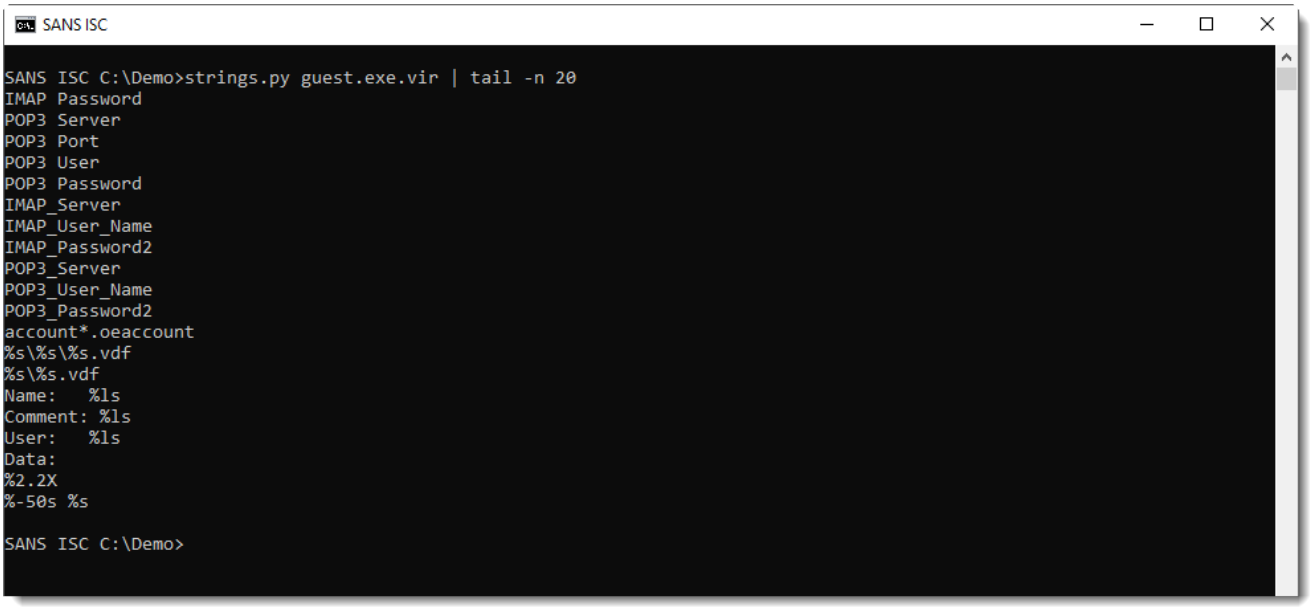
The PowerShell script uses certutil to BASE64-decode the "certificate" to the AutoIt script, and then lauches the AutoIt interpreter with the script as argument.

The AutoIt 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 AutoIt script before it is injected and executed.

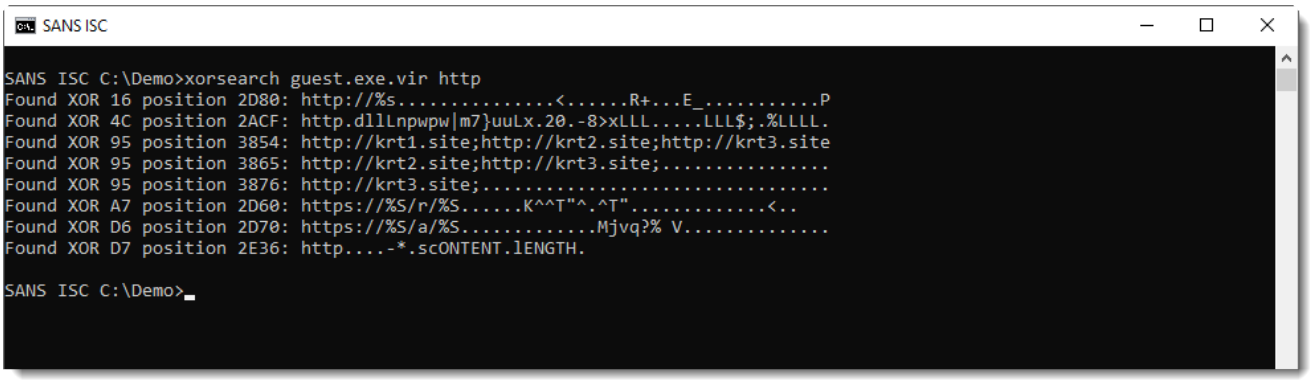
As the decrypted KPOT EXE is never written to disk, it was unknown by VirusTotal. I did submit it today.

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

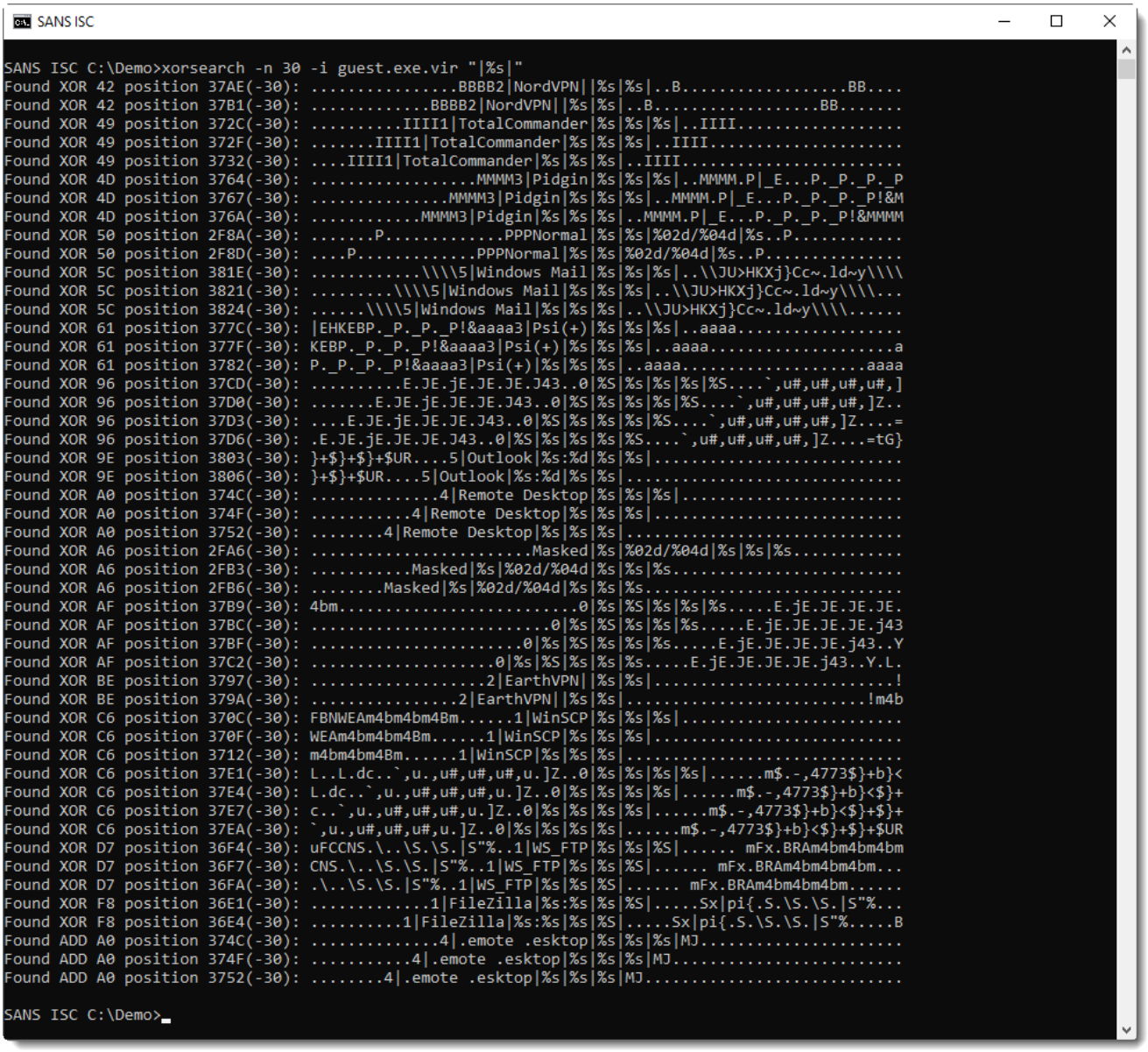


More interesting strings are simply XOR-encoded (1-byte key).

Like the C2:



And the targets:



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