Osiris, the god of afterlife...and banking malware?!

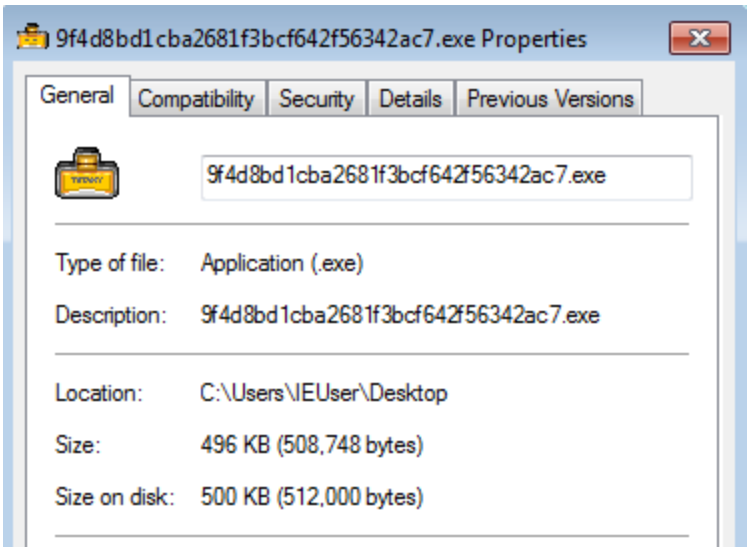
dissectingmalwa.re/osiris-the-god-of-afterlifeand-banking-malware.html

Thu 29 August 2019 in Banking-Malware

After coming back from the Chaos Communication Camp two days ago I thought it would be a good idea to check on the current malware events out there, so come along for the ride

I came across this sample after this tweet by @James_inthe_box :

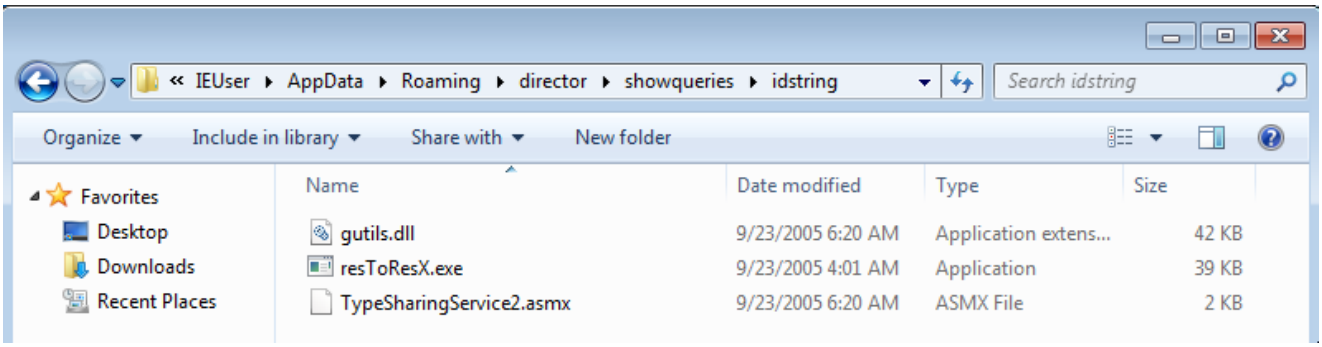
> Found by @FewAtoms at:
> borel[.]fr/notices/CanadaPost.zip -> vbs drops:
> https://naot[.]org/cms/file/fixed111.exe
>
> I'd like to say with confidence: I have no idea what this is. https://t.co/z18z17Kau8 pic.twitter.com/68zg3HpkRI
>
> — James (@James_inthe_box) August 28, 2019



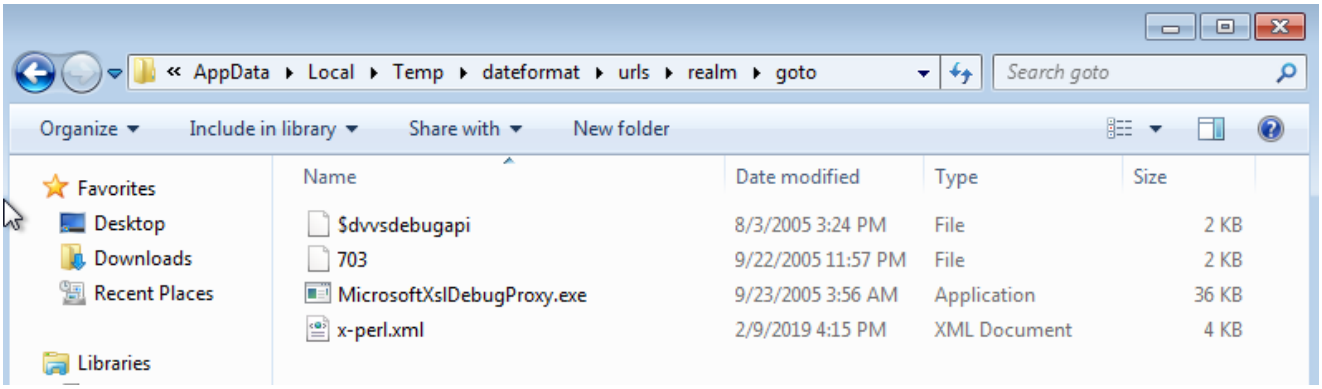
A short disclaimer: downloading and running the samples linked below will compromise your computer and data, so be f$cking careful. Also check with your local laws as owning malware binaries/ sources might be illegal depending on where you live.

Get your sample today from:

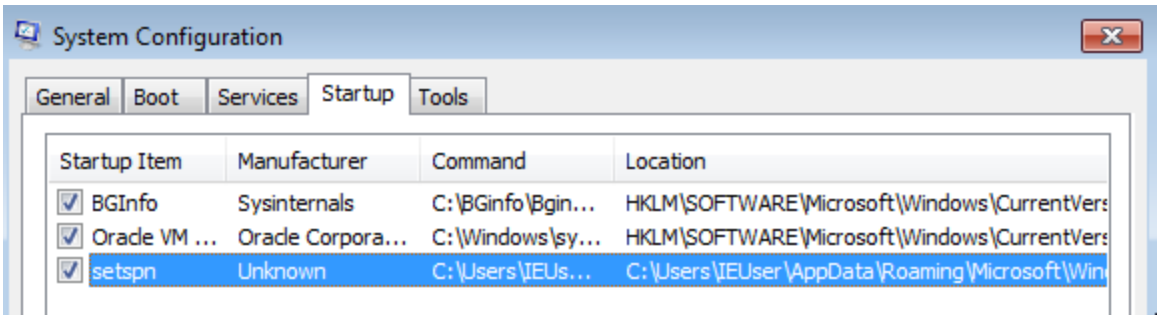
Osiris available @ https://malshare.com/sample.php?action=detail&hash=9f4d8bd1cba2681f3bcf642f56342ac7 `sha256` `0325714eeb2af235a0f543ad9e11b5d852a61be78c9ece308c651412d97edd39`



Files dropped in %APPDATA%\Roaming

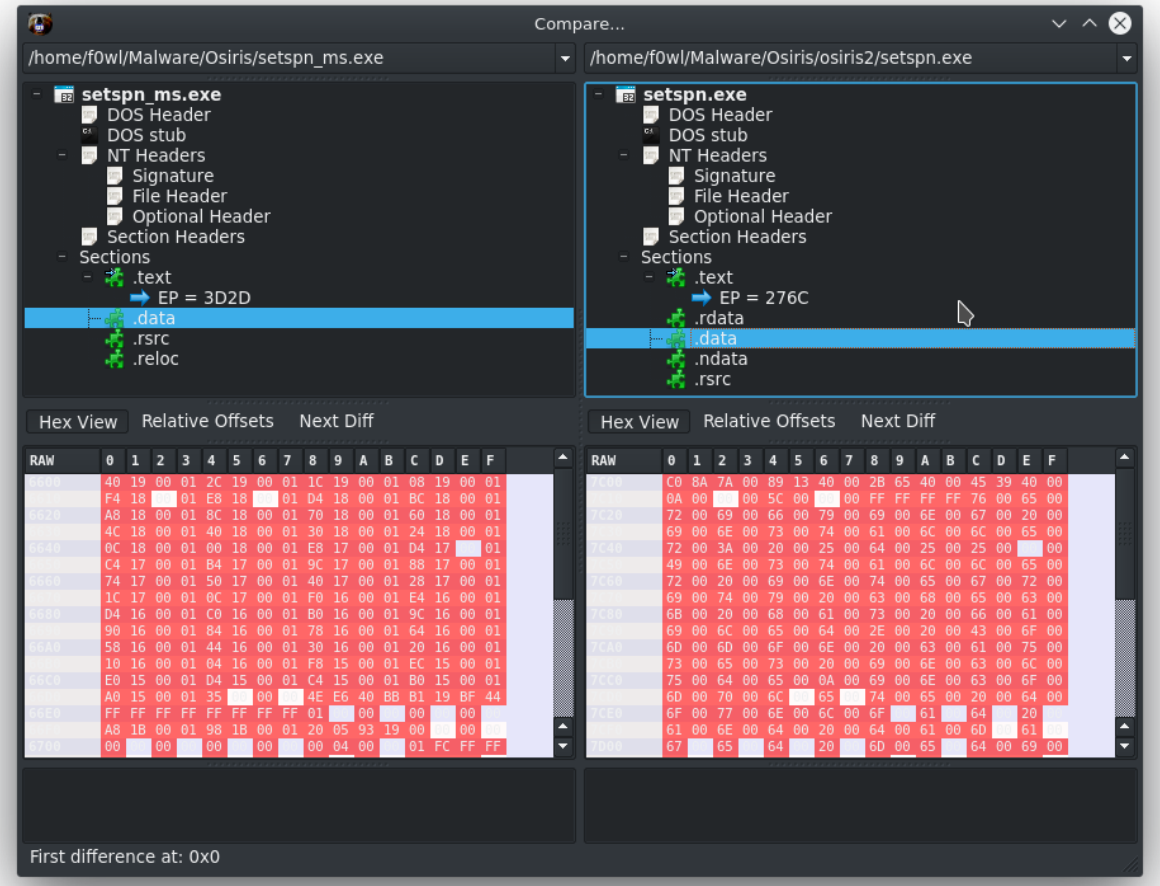


Files dropped in %temp%



After running the sample for the first time it adds itself to system startup and copies itself to *%appdata%\Roaming\Microsoft\Windows\Protected\setspn.exe*. Comparing the malicious setspn.exe with the Microsoft Original (which is normally found at C:\Windows\System32\setspn.exe) with the help of PEBear it is obvious that the files are not

the same.



To jump straight to the *Hybrid-Analysis* report for fixed111.exe click here. I picked out a couple of interesting findings for you:

fixed111.exe

This report is generated from a file or URL submitted to this webservice on August 28th 2019 12:45:05 (CEST) and action script *Heavy Anti-Evasion*
Guest System: Windows 7 64 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.30 © Hybrid Analysis - learn more

Overview | Sample (478KiB) | Downloads | External Reports | Re-analyze | Hash Seen Before | Show Similar Samples | Report Abuse

Incident Response

Risk Assessment

Spyware	Contains ability to open the clipboard Sets a global windows hook to intercept keystrokes
Fingerprint	Reads the active computer name
Evasive	Marks file for deletion
Network Behavior	Contacts 4 hosts. View all details

One thing that stands out is that Osiris uses components of the Nullsoft Scriptable Installer. I did not look into it that far yet, but it seems like it is used for a headless install only.

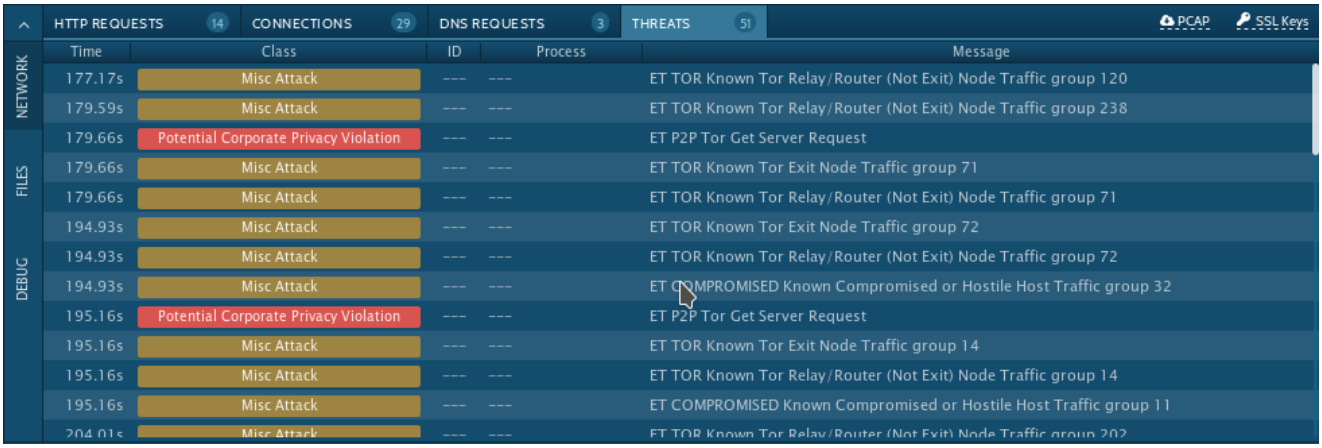
Contains PDB pathways

details	"%USERPROFILE%\Desktop\Summary\mini-tor\mini-tor\bin\Release\x64\GetX64BTIT.pdb" "f:\binaries.x86ret\bin\i386\ResToResX.pdb" "Microsoft.XslDebugProxy.pdb"
source	String
relevance	1/10
research	Show me all reports matching the same indicator

A quite interesting find: this Osiris sample uses a POC implementation called Mini-Tor for communication with the Tor network. Pretty convenient for the malware author as it keeps the size of the binary small, but still allows data exfiltration over an anonymized protocol. Click here for the Any.Run analysis.

As the Twitter Discussion about this sample started multiple theories about the Tor Requests were brought up. My explaination for this behaviour is that the malware is exfiltrating data over the Tor network. Because of the URL format of the requested sites

IPAddress/tor/servers/fp/-HASH- one can assume that the contacted servers are *Directory Servers* which hold the Server Descriptor Files for known Nodes. This is why I'd classify this behaviour as more or less standard client communication.



IOCs

Files

```
fixed111.exe --SHA1--> a1887f8b29ef20a6e0d7284521c40eee77d47dd0
setspn.exe --SHA1--> a1887f8b29ef20a6e0d7284521c40eee77d47dd0
GetX64BTIT.exe--SHA1--> 7f08febf0fdb7fc9f8bf35a10fb11e7de431abe0
Majorca.dll --SHA1--> 47d9371a0dd3369d89068994d5d18bb54a0d7433
System.dll --SHA1--> 48df0911f0484cbe2a8cdd5362140b63c41ee457
gutils.dll --SHA1--> ab92a9a74c55c5e5d05f1f3dde518371dda76548
resToResX.exe --SHA1--> b5114de8c2e78d72ec8ddb6ab7bcb02b1bb5291f
79.opends60.dll --SHA1--> ec9946684d5e72dbc5bdcffa31167ad1a19e29bd
MicrosoftXslDebugProxy.exe --SHA1--> 2d9b200ea1d9fb6442f21bb5441072bd4b9d1968
UserInfo.dll --SHA1--> 0bd28183a9d8dbb98afbcf100fb1f4f6c5fc6c41
TypeSharingService2.asmx --SHA1--> f28868e733bfdcf68cee93509f84694df50bbdf4
libfontconfig1amd64.triggers --SHA1--> 6ca8f520c10214648f88a8ba08ccdfcc53b124a3
349f9714.lnk --SHA1--> fe08da4fd09dbab64d4e4d23b9a935468ef05f8b
703 --SHA1--> bb5d6f6ba8155899d0017ce2edc1bf2622ad5b3b
x-perl.xml --SHA1--> 32404eab9098db64af17b6e5862b0b563f57c2dd
x64btit.txt --SHA1--> cd8fff32832f8a8f20b88a2f32c04800535d060e
Paragraphia --SHA1--> 360071bee9bae26834006615d0fb711d25f4a4af
_dvvsdebugapi --SHA1--> f5db6c9fed4cb80461502bb6d25532e8f0c1f064
win.ini --SHA1--> f939c7deb74637544a09df6d0a096f5719b227d1
```

URLs

```
httpx://naot[.]org/cms/file/fixed111.exe
httpx://borel[.]fr/notices/CanadaPost.zip
```