Trezor Bridge - 2.0.27

(Windows)

August 09th, 2019.

Description:

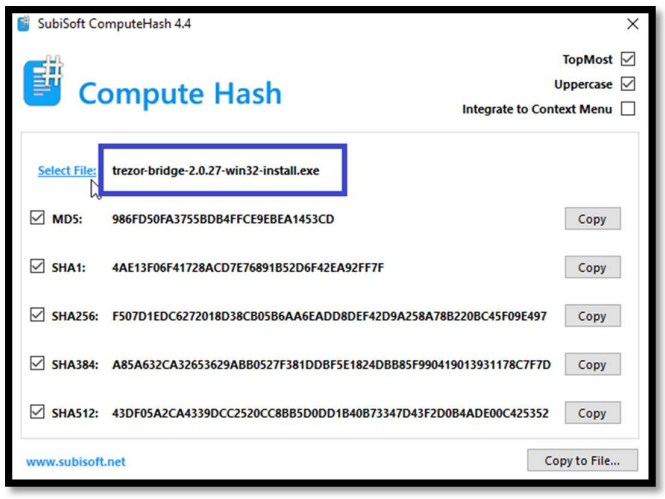
The Trezor wallet is used to secure digital assets (e.g. bitcoin and crypto currency). However, the Trezor Bridge an application (i.e. Windows version) used to connect the hardware device and the internet browser was considered vulnerable in the aspect of privilege escalation. This vulnerability is related to functions such as SeDebugPrivilege and SeLoadPrivilege enabled by the application. For instance, an offensive package (i.e. mimikatz) is able to identify the presence of this type of privilege.

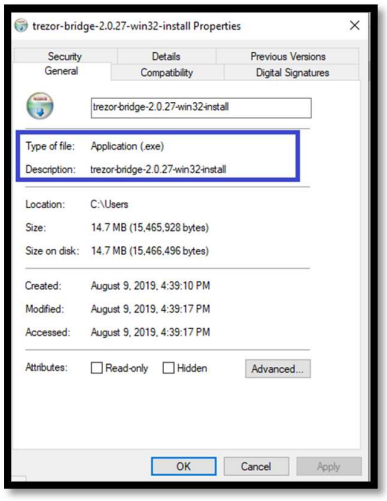
Attack Method: Malware could perform code injection in the process used by the Trezor Bridge application.

Exploit reference: at the www.exploit-db.com there is a reference to "Abusing Token Privileges For LPE".

General mitigation strategy: limit the access of debug privileges to specific programs and users through group policy.

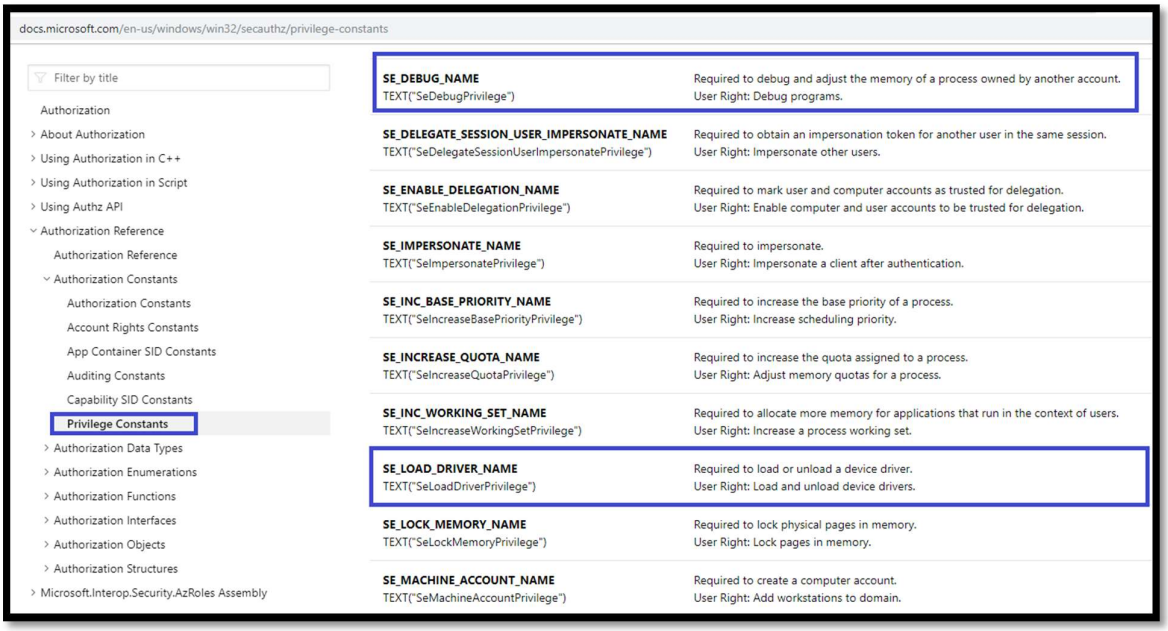
File identification



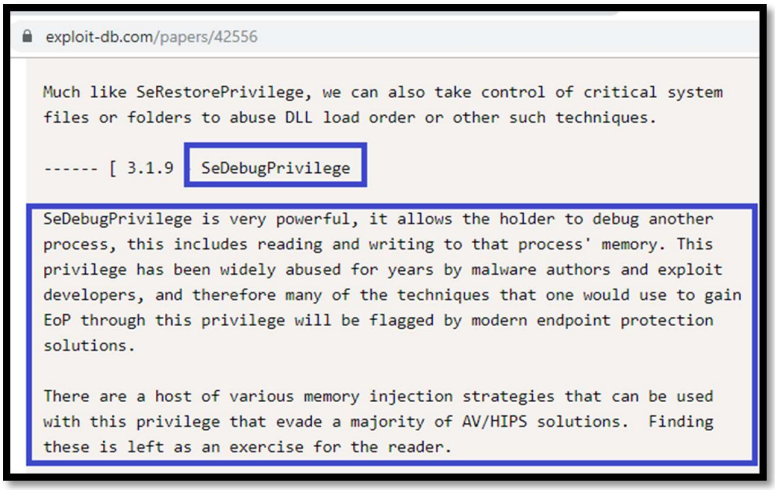


Permissions requested

Definition of permissions

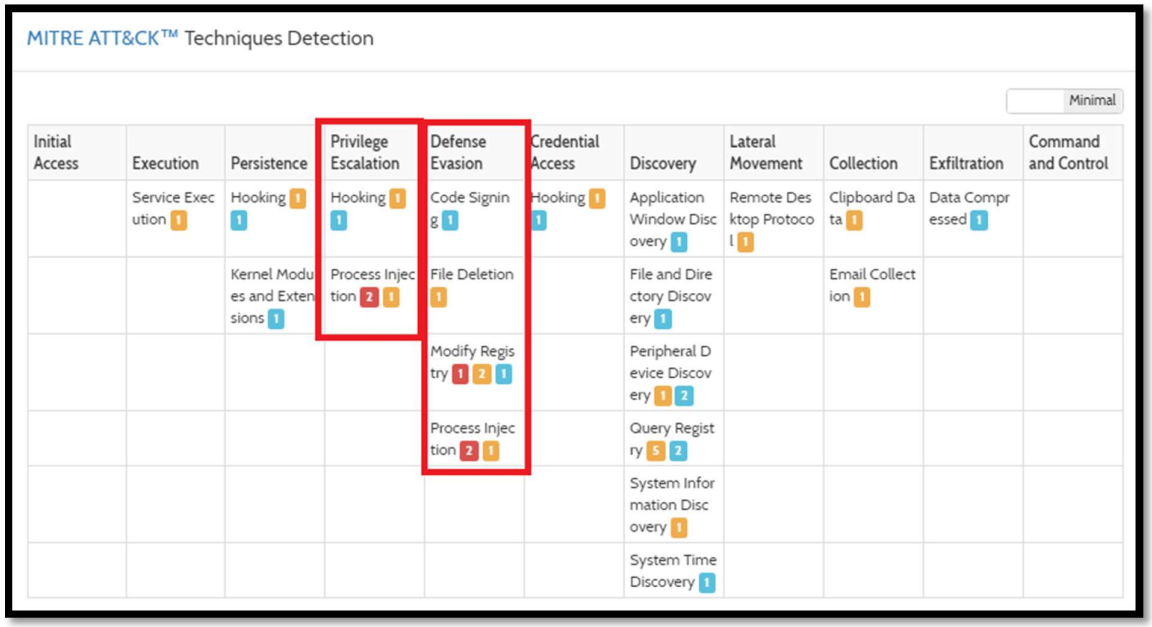


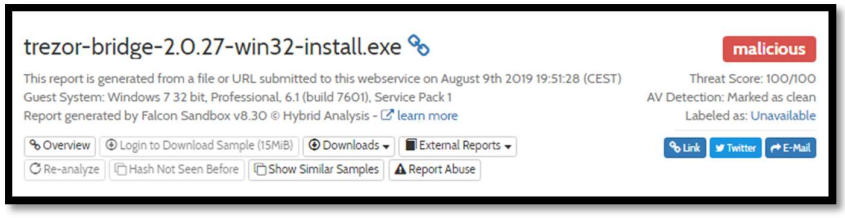
Exploit Reference



```
----[ 2.2 - Relevant Exploitation Strategies

Previous, related work that provided influence and indirect guidance for this
article's strategy is presented here.  These related techniques are briefly
detailed to provide background and to pay homage to those who came before
us.

Cesar Cerrudos Easy Local Windows Kernel Exploitation paper released at
Blackhat 2012 [1] introduced three different privilege escalation
strategies, and pointed many exploit devs towards the power of abusing
process tokens.  The first technique demonstrated in the paper details the
NULL ACL strategy, now partially mitigated, in which an arbitrary
write could be leveraged to NULL a privileged object's ACL.  This was and is a
very common strategy for effectively migrating into more privileged
processes.

The second Cerrudos strategy is a carpet bombing version of ours, in which an
arbitrary write could enable all privileges in a process token.  With these
privileges enabled, one could exploit SeDebugPrivilege and migrate into a
more privileged process, create tokens with SeCreateTokenPrivilege, or load
kernel drivers with SeLoadDriverPrivilege.
```

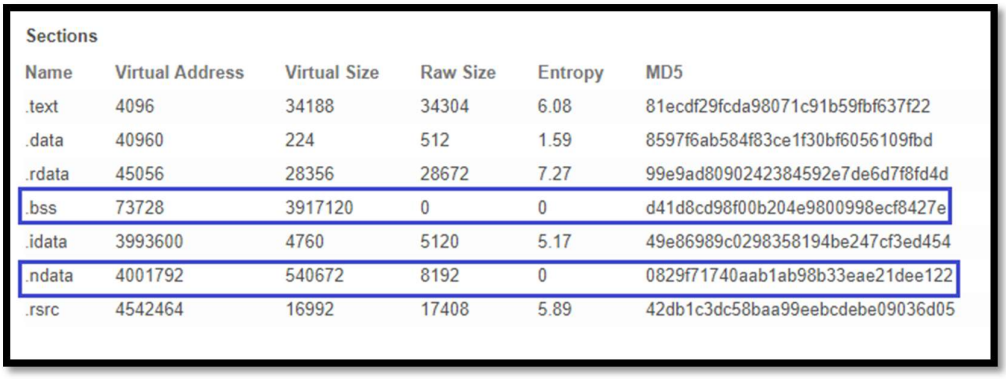
Behavior Analysis and Techniques





Other Aspects

Interesting aspects that may require further review are the overlay (file-ratio), the raw size of the .bss section and the analysis of the Nullsoft Scriptable Install System (NSIS), which could be in some cases be related to dynamic link library attacks.



Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	34188	34304	6.08	81ecdf29fcda98071c91b59fbf637f22
.data	40960	224	512	1.59	8597f6ab584f83ce1f30bf6056109fbd
.rdata	45056	28356	28672	7.27	99e9ad8090242384592e7de6d7f8fd4d
.bss	73728	3917120	0	0	d41d8cd98f00b204e9800998ecf8427e
.idata	3993600	4760	5120	5.17	49e86989c0298358194be247cf3ed454
.ndata	4001792	540672	8192	0	0829f71740aab1ab98b33eae21dee122
.rsrc	4542464	16992	17408	5.89	42db1c3dc58baa99eebcdebe09036d05

References:

1. https://wallet.trezor.io/#/bridge
2. https://trezor.io/
3. https://www.virustotal.com/gui/file/f507d1edc6272018d38cb05b6aa6eadd8def42d9a258a78b220bc45f09e497c1/behavior/Tencent%20HABO
4. https://www.hybrid-analysis.com/sample/f507d1edc6272018d38cb05b6aa6eadd8def42d9a258a78b220bc45f09e497c1
5. https://medium.com/palantir/windows-privilege-abuse-auditing-detection-and-defense-3078a403d74e
6. https://docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants
7. https://www.exploit-db.com/papers/42556