Beyond good ol’ Run key, Part 125

hexacorn.com/blog/2020/07/30/beyond-good-ol-run-key-part-125

July 30, 2020 *in Autostart (Persistence), Living off the land, LOLBins*

Update

Turns out @0gtweet posted about it in January and I missed that!!!

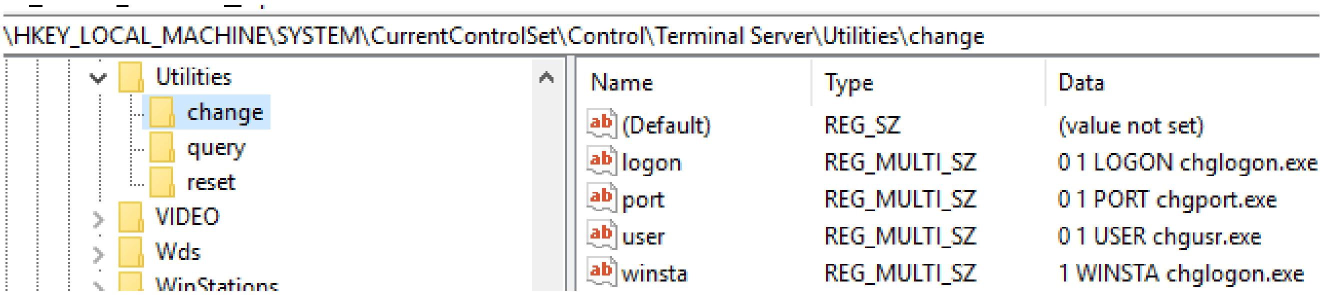
Old Post

Been awhile since I posted in this series, so here comes a new trick.

It is not your typical executable for sure, *change.exe* that is. When I looked at it for the first time I was perplexed — within first few lines of code it literally executes other executables. Must be something good I thought, and good it was indeed.

When launched, change.exe does something very strange – it enumerates Registry entries under this location:

> HKLM\System\CurrentControlSet\Control\Terminal Server\Utilities\change



\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Utilities\change

Name	Type	Data
(Default)	REG_SZ	(value not set)
logon	REG_MULTI_SZ	0 1 LOGON chglogon.exe
port	REG_MULTI_SZ	0 1 PORT chgport.exe
user	REG_MULTI_SZ	0 1 USER chgusr.exe
winsta	REG_MULTI_SZ	1 WINSTA chglogon.exe

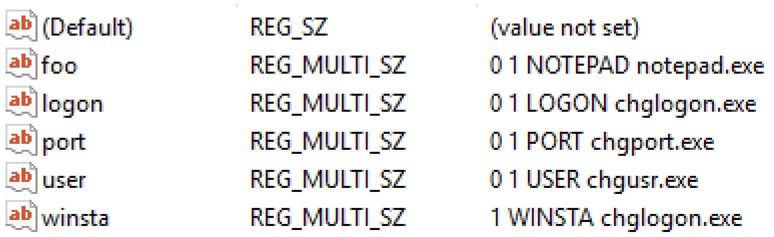
These entries are … interesting, because they look like some stringified flags followed by executable names. Possible abuse opportunity?

When you run ‘change /?’ you get the following help information:

```
CHANGE { LOGON | PORT | USER }
```

Do you see the pattern? — no? look at these Registry entries again.

In my first attempt I added ‘foo|0 1 NOTEPAD notepad.exe’:



(Default)	REG_SZ	(value not set)
foo	REG_MULTI_SZ	0 1 NOTEPAD notepad.exe
logon	REG_MULTI_SZ	0 1 LOGON chglogon.exe
port	REG_MULTI_SZ	0 1 PORT chgport.exe
user	REG_MULTI_SZ	0 1 USER chgusr.exe
winsta	REG_MULTI_SZ	1 WINSTA chglogon.exe

I then ran 'change notepad' and … notepad executed.

Now, if you paid attention there are other registry keys listed on the first screenshot:

```
change -> change.exe
query -> query.exe
reset -> reset.exe
```

They all follow the same pattern and fetch command list from Registry!

So you can either add a new entry, or modify an existing one. Access rights are in place and the key is owned by TrustedInstaller, but… well… once on the box, always on the box.

Last, but not least – it's a persistence mechanism and a LOLBIN in one.