Home Services Products & Freebies Search

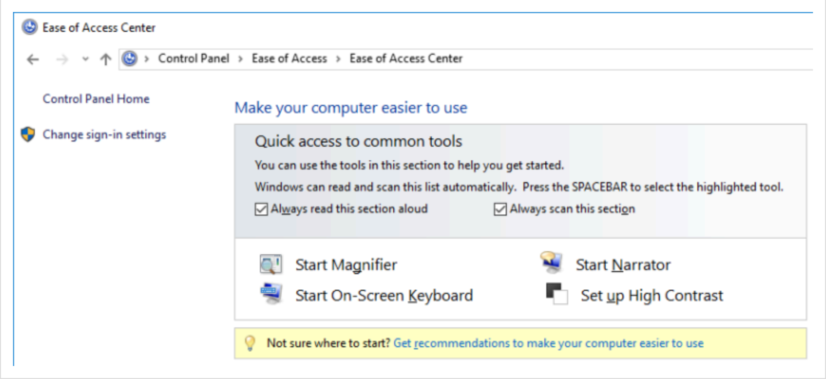
Case Studies Contact Us

Posted on **2016-07-22**

← Previous **Next →**

Beyond good ol' Run key, Part 42

The Ease of Access is a place where a computer user can enable the so-called Assistive Technologies (AT). These technologies make life easier for the users with needs and include OSK (On-Screen Keyboard,) Narrator, Magnifier, and a number of other options that are helping to make the work environment better.



Ease of Access Center

Control Panel › Ease of Access › Ease of Access Center

Control Panel Home

Change sign-in settings

Make your computer easier to use

Quick access to common tools

You can use the tools in this section to help you get started.

Windows can read and scan this list automatically. Press the SPACEBAR to select the highlighted tool.

☑ Always read this section aloud ☑ Always scan this section

Start Magnifier

Start Narrator

Start On-Screen Keyboard

Set up High Contrast

Not sure where to start? Get recommendations to make your computer easier to use

Persistence #1

With Windows 8 Microsoft introduced a way to register third-party Assistive Technology applications on the system. All of them are stored inside the Registry under the following branch:

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs

The same branch exists on Windows 7, but the registration is possible only on Windows 8+.

Interestingly, a user can decide to launch the ATs during the log on process. To do so, the following Registry value needs to be created/modified:

- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\Configuration = …

where *Configuration* is a comma-delimited string list of ATs the user wants to load during the logon process.

As a result, one can achieve persistence by registering the new AT:

and ensuring the *Configuration* value points to it:

Once these are added the c:\test\malware.exe will be launched anytime the user logs on. And as a bonus, it will also run anytime the desktops switch (f.ex. when UAC pops up). The desktops-switch activity is depending on the *TerminateOnDesktopSwitch* value which you can read about in the linked article.

Obviously, elevated privileges are required to register the new AT.

Persistence #2

The obvious modification of the technique above could rely on modification of the existing AT entry and changing the executable path of f.ex. Narrator or OSK.

Sort-of-Persistence #1

If you look at how system launches the ATs you will notice that the process responsible for this task is called (not surprisingly) Windows Assistive Technology Manager and is launched from the AtBroker.exe file:

The AtBroker starts the ATs using the following syntax:

-
  ```
  C:\Windows\System32\ATBroker.exe /start <AT name>
  ```

f.ex.:

-
  ```
  C:\Windows\System32\ATBroker.exe /start malware
  ```

One could add this command line to any of the typical Startup locations (f.ex. Run key) which – on the surface at least – would appear as if pointing to a legitimate, signed OS binary. Most of security products or analysts looking at such entry would assume it's a legitimate, clean binary, and unless they understand the context and the connection/relationship with the AT Registry entries they would most likely ignore it (I didn't test any security product though).

There is another aspect of launching malware this way – AtBroker is spawn by winlogon.exe so if the malware was executed via AtBroker proxy, the process parent wouldn't point to Explorer which is a parent process to most processes launched manually via GUI. This could give an impression that the malware is a process spawn not by the user, but some system component (which is actually true). As a result someone reviewing process tree could mistakenly assume it's legitimate.

Sort-of-Persistence #2

As a side note – the interface of the Easy Access applet in Control Panel (or via Win+U) can be modified using the settings described in the article I linked to. I have not explored it. Also, the applet itself could be leveraged as a 'hidden' persistence mechanism that would activate only when the user launched any of the available ATs manually (either registered, or modified to point to malware). Even if I am not using any of the ATs I do occasionally launch a Magnifier, or OSK. Such user-dependent persistence mechanism could be a 'last resort' persistence mechanism used to re-introduce malware on the system somewhere in the future.

As mentioned earlier, elevated privileges are required for all this, but this is not impossible – Escalation Of Privileges is not that hard to achieve as many exploits show.

This entry was posted in **Anti-Forensics**, **Autostart (Persistence)**, **Compromise Detection**, **Incident Response**, **Malware Analysis** by **adam**. Bookmark the **permalink**.

Privacy Policy | **Proudly powered by WordPress**