Posted on 2017-05-01

← Previous Next →

Running programs via Proxy & jumping on a EDR-bypass trampoline

The parent-child process relationship is very helpful when it comes to defining detection rules and watchlists. For instance, anytime a winword.exe spawns a cmd.exe, powershell.exe, cscript.exe, wscript.exe, mshta.exe it is an obvious anomaly that may be a sign of an Office macro-based infection.

However, insert an unexpected process in-between and the rule/watchlist fails. Perhaps for this reason, it would be nice to have EDR rulesets that can refer not only to parents, but also to ancestors of the process.

Since this relationship is prone to manipulation let's have a look at a couple of possible examples:

-
  ```
  rundll32 url.dll, OpenURL file://c:\windows\system32\calc.exe
  ```

-
  ```
  rundll32 url.dll, OpenURLA file://c:\windows\system32\calc.exe
  ```

-
  ```
  rundll32 url.dll, FileProtocolHandler calc.exe
  ```

-
  ```
  rundll32 zipfldr.dll, RouteTheCall calc.exe
  ```

Running any of these commands will launch calc.exe with the rundll32.exe as a parent.

Obviously, rundll32.exe is an obvious bad guy too. What about we copy it first?

```
copy c:\windows\system32\rundll32.exe %appdata%\Adobe\adobe.exe
```

Now, we can launch:

-
  ```
  %appdata%\adobe\adobe.exe url.dll, OpenURL file://c:\windows\syste
  ```

-
  ```
  %appdata%\adobe\adobe.exe url.dll, OpenURLA file://c:\windows\syst
  ```

-
  ```
  %appdata%\adobe\adobe.exe url.dll, FileProtocolHandler calc.exe
  ```

-
  ```
  %appdata%\adobe\adobe.exe zipfldr.dll, RouteTheCall calc.exe
  ```

And get the very same result, this time, with the parent process being adobe.exe.

If you know any other EXE/DLL combo that can act as a proxy, I'd be grateful if you could let me know. Thanks!

This entry was posted in **Anti-***, **EDR**, **Incident Response**, **LOLBins** by **adam**. Bookmark the **permalink**.