**Registry Attacks**

**Description 1**

A current trend in fileless malware attacks (a category of attacks that take advantage of operating system features) is to inject code into the Windows registry. Most of these attacks enter a system as a file or link in an email message. When the link or attachment is clicked, the malware writes its payload into the Windows registry and then disappears. The payload written into the Windows registry contains a script hidden by several layers of tricks. The script is masked from view by removing the user’s access privileges or including a null character in the registry key name. **The script calls a legitimate Windows program such as PowerShell to insert malicious code into the memory space of standard Windows processes such as svchost, dllhost, or regsvr32, so that the code cannot be detected by scans for malicious processes.**

Examples that McAfee Labs has seen so far, including Kovter and Powelike, connect with websites and click-through ads, transforming the infected system into a click bot. The more resources the system has, the more ad traffic it generates, and the **more money it makes for the criminals**. Some analyzed variants have also **downloaded ransomware payloads**. [1]

**Description 2**

Windows Operating system is a very complex software program that performs innumerable operations behind the scene so that your programs get installed on your computer and run smoothly. Quite unknown to most of ordinary users, Windows operating system needs to consider hundreds of things so that the programs you run behave predictably. For example, you must have observed that when you make changes to your Word file configurations, you will find that all these changes are found implemented even when you switch on the computer next time. Windows operating system needs to keep track of all such changes to configuration and many other parameters of every program that run on the computer. Windows Registry is the tool which stores all such vital information about the programs and is managed by Windows operating system.

Since the registry is the most important program that runs your computer, the creators of malicious software target the registry to wreck the working of your system in the following ways.

1.Virus and other malicious programs are designed to tamper the values stored in the registry.

2.This can result in **slowed down system**, **corrupt software** (many of your programs behave in funny manner) and **fatal blue screen**!

3.Not every virus attack involves damage to the registry, but there are some who do the damage.

**Reference**

**[1]** <http://www.darkreading.com/partner-perspectives/intel/detecting-the-undetectable-windows-registry-attacks/a/d-id/1323571>

**[2]** <http://combofix.org/what-is-system-registry-and-how-virus-attacks-the-system-registry.php>