Huff’s Analysis of Qusla.exe Malware

By Josh Huff on Jan 30, 2018

Qusla’s Hash

00670F2B9631D0F97C7CFC6C764DD9D9

Qusla’s Yara Signature

```
rule qusla
{
  strings:
        $str1=”qusla”
        $str2=”hau”
  condition:
        $str1 or $str2
}
```

Qusla’s Naughty Behavior

The malware that constitutes the above hash and is identified by the yara rule above seeks to establish two harmful executables named “hau.exe” and “qusla.exe”. For the sake of brevity and simplicity, we’ll henceforth call this sample “qusla” (curiously, according to Google translate, “qusla” is the Azerbaijani word for “vomit”).

In addition to standard privilege escalation, Qusla uses the ol’ attrib command trick.

Handle->0x00000078		
ApplicationName->C:\Windows\system32\attrib.exe	CommandLine->attrib +r +s +h c:\qusla.exe	CreationFlags->0x00080000
Handle->0x00000078		

True to malware form, Qusla is interested in persisting in an infected system and does so by silently creating a batch file called Dx:

SUCCESS	0x00000000	FileHandle->0x00000070	DesiredAccess->0x00100080	FileName->\??\c:\Users\Admin\Desktop\Dx.bat	ShareAccess->3

Typically, malware will operate as covertly as possible, either uploading files via ftp or uploading them to a website owned by the attacker, or by sending messages to itself via SMTP in the background. Qusla is a bit more brazen than some samples, as it makes a strange URL the user’s homepage.

```
","Registry->0x80000001","SubKey->Software\Microsoft\Internet Explorer\Main","Class->","Access->2","Handle->0
."Handle->0x00000268","ValueName->Start Page","Type->1","Buffer->http://www.3392.cn/?999_20180131\\x00"
```

It’s easy to avoid Qusla, as it likely relies on a user visiting untrustworthy websites, opening e-mail attachments from strange senders, or downloading files without running Cuckoo or FileInsight beforehand.