Malware Trying to Avoid Some Countries

By Pierre-Marc Bureau

Malware

15 Jan 2009 • , 2 min. read

There are different techniques that can be used by a program to identify in which country it has been installed. It can check for time zone information, public IP addresses or even domain names. Lately, we have seen two different malware families trying to discover their geographic location in an effort to avoid infecting PCs in specific countries.

We have found some variants of the The Win32/TrojanDownloader.Swizzor using the following code:

```
call    GetSystemDefaultLangID ; Indirect Call Near Procedure
[...]
mov     edi, eax
[...]
cmp     di, 419h
jz      end_function
```

This code calls the GetSystemDefaultLangID function and compares the result to a constant, 0x419. Browsing through MSDN documentation reveals that this constant's value translates to LANG_RUSSIAN. It turns out that these variants of Win32/TrojanDownloader.Swizzor will exit before infecting a computer, if they find out that the default system language is Russian.

We have also identified the following code in the earliest variants of the Win32/Conficker malware:

```
push    edi             ; lpList
push    esi             ; nBuff
call    ebx ; GetKeyboardLayoutList
cmp     esi, eax
jnz     short list_not_found
dec     esi
cmp     word ptr [edi+esi*4], 422h
jz      short dont_install
```

Here, the malware tries to retrieve a list of keyboard layouts and works through that list. If a layout is found with the language identifier of 0x422, the routine terminates and the malware is not installed. This means that some variants of the Win32/Conficker family will not install on a computer that uses an Ukrainian keyboard layout.

Please note that this behavior is only present in W32/Conficker.A. Later variants of this malware infect any PC they can access without checking the keyboard layout.

What we are seeing now is probably the beginning of a new trend. Malware authors will try to avoid infecting PCs in specific countries to limit the risk of legal actions taken against them. In most countries, there often needs to be a victim or complaint before law enforcement agencies take legal action against an offender in cases of malware infection. In cases where an attacker only targets victims outside of his country, it is much harder for law enforcement agencies to take action.

Special thanks to Sebastien Doucet and Volodymyr Pikhur for their help.

Pierre-Marc Bureau
Researcher