```
1
2  1 VERSIONINFO
3  FILEVERSION 6,1,7600,16385
4  PRODUCTVERSION 6,1,7600,16385
5  FILEOS 0x40004
6  FILETYPE 0x2
7  {
8  BLOCK "StringFileInfo"
9  {
10         BLOCK "040904B0"
11         {
12                 VALUE "CompanyName", "Microsoft Corporation"
13                 VALUE "FileDescription", "Multiple Provider Router DLL"
14                 VALUE "FileVersion", "6.1.7600.16385 (win7_rtm.090713-1255)"
15                 VALUE "InternalName", "mpr.dll"
16                 VALUE "LegalCopyright", "© Microsoft Corporation. All rights reserved."
17                 VALUE "OriginalFilename", "mpr.dll"
18                 VALUE "ProductName", "Microsoft® Windows® Operating System"
19                 VALUE "ProductVersion", "6.1.7600.16385"
20         }
21 }
22
23 BLOCK "VarFileInfo"
24 {
25         VALUE "Translation", 0x0409 0x04B0
26 }
27 }
```

Una delle ultime minacce ai nostri sistemi digitali è InvisiMole, un potente spyware in grado di trasformare il PC infetto in una videocamera, consentendo ai cyber criminali di vedere e ascoltare ciò che accade nella stanza della vittima o dovunque si trovi il dispositivo infetto.

{loadposition user7}

InvisiMole ha un'architettura modulare e veicola l'infezione attraverso un wrapper DLL che svolge le sue attività utilizzando altri due moduli incorporati. Entrambi i moduli sono backdoor ricche di funzionalità, che insieme danno la possibilità di raccogliere quante più informazioni possibili sull'obiettivo.

Il wrapper DDL viene programmato utilizzando il Free Pascal Compiler, collocato nella cartella Windows e mascherato come file di libreria mpr.dll a 32 o 64 bit. I due moduli di accompagnamento, RC2FM e RC2CL, vengono caricati dal wrapper nel processo explorer.exe che aiuta a tenerlo separato e quindi nascosto durante il normale funzionamento.

Il modulo RC2FM contiene una backdoor e può eseguire 15 comandi che spaziano dal catturare screenshot, attivare il microfono, aprire, chiudere e caricare nuovi file.

Il modulo RC2CL ha capacità molto simili ma è inoltre in grado di raccogliere quanti più dati possibili dalla macchina infetta. È interessante notare che esiste un'opzione nel modulo RC2CL

per disattivare la sua funzionalità backdoor e agire come un proxy.

InvisiMole è attivo almeno dal 2013 ma è stato individuato e analizzato solo dopo essere stato rilevato dalle soluzioni di ESET su computer compromessi in Ucraina e Russia.

La campagna che utilizza InvisiMole è altamente mirata e non sorprende dunque che il malware abbia un basso tasso di infezione, con una manciata di computer colpiti.

Il metodo di diffusione di InvisiMole non è ancora stato individuato e i ricercatori di ESET non escludono alcun vettore di infezione, inclusa l'installazione facilitata dall'accesso fisico alla macchina.

Per l’analisi tecnica di InvisiMole e per ulteriori informazioni sull’argomento è possibile visitare il blog di ESET al seguente link: www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

{jcomments on}

{loadposition user6}