

MALWARE ANALYSIS

- REPORT -

Infection:

Trojan-Proxy.Win32.Horst.af

Category: *Trojan*

MD5 Hash:

e6e46cefe27a74a49fdb0b247772f7a1

Size (bytes): *55511*

Files added during the infection:

- *%system%\nsvcd.exe*
- *%windows%\system\smss.exe*
- *%temp%\tmp1.tmp*

Changes on the Windows Registry:

- *HKLMSOFTWARE\Microsoft\Windows\CurrentVersion\Run ".nsvc" = C:\WINDOWS\system\smss.exe /w*

Analyst's comment:

Original file is packed with NSPACK.

Once ran, it creates tmp1.tmp under %temp% directory. Tmp1.tmp is then copied under %System% directory as nsvcd.exe. This file is harmless, it's a service management software.

Original file is then copied as smss.exe under C:\Windows\system directory - which isn't the legitimate directory.

Smss.exe is a IRC backdoor.

Once executed, smss.exe is injected in svchost.exe process. Then it tries to connect to a remote server that

acts as IRC channel. Local tcp port is random choosed.

Windows firewall rules are changed to allow svchost.exe to connect to internet.

Research and analysis done by Marco Giuliani - marco@hwupgrade.it

This analysis is provided only for educational knowledge. It is illegal to reproduce this analysis, or manipulate it for malicious intent. This analysis is property of Marco Giuliani and is protected under international copyright laws. Infringments regarding this analysis (including copying, modifying, or reproducing without prior consent of the author) will result in criminal or civil penalties. The author is not responsible for any damages or misinformation in this analysis. The analysis is presented as is and is, to best of the authors knowledge, correct.