Jan 2013 - Linux SSHDoor - sample

contagiodump.blogspot.com/2013/02/linux-sshdoor-sample.html

Just a few accumulated samples here found and shared by others. This one is for Linux SSHDoor malware, which can steal your SSH passwords. ESET covered that in detail in Linux/SSHDoor.A Backdoored SSH daemon that steals passwords (24 JAN 2013)

The related Linux.Chapro.A sample was posted earlier this year as well

Download

Download. Email me if you need the password

Automatic Scans

https://www.virustotal.com/en/file/ebfd9354ed83635ed38bd117b375903f9984a18780ef86dbf7a642fc6584271c/analysis/1361067116/

SHA256: ebfd9354ed83635ed38bd117b375903f9984a18780ef86dbf7a642fc6584271c
SHA1: cb7a464aa8d58f26f6561c32ef4a1464c583a7ca
MD5: 90dc9de5f93b8cc2d70a1be37acea23a
File size: 469.9 KB (481200 bytes)
File name: 90DC9DE5F93B8CC2D70A1BE37ACEA23A
File type: ELF
Detection ratio: 22 / 46
Analysis date: 2013-02-17 02:11:56 UTC (0 minutes ago)
Avast ELF:SSHDoor-A [Trj] 20130217

AVG BackDoor.Generic_c.FDN 20130216
ClamAV UNIX.Trojan.SSHDoor 20130217
Comodo UnclassifiedMalware 20130217
DrWeb Linux.BackDoor.Ssh 20130215
eSafe Win32.Trojan 20130211
ESET-NOD32 Linux/SSHDoor.A 20130216
F-Secure Backdoor:Linux/SSHDoor.A 20130217
Fortinet Linux/SSh.M!tr.bdr 20130217
GData ELF:SSHDoor-A 20130217
Ikarus Backdoor.Linux.SSh 20130216
Jiangmin Backdoor/Linux.gu 20130216
Kaspersky Backdoor.Linux.SSh.m 20130216
Microsoft Backdoor:Linux/SSHDoor.A 20130217
Norman SSHDoor.A 20130215
PCTools Malware.Linux-SSHDoor 20130217
Symantec Linux.SSHDoor 20130216
TrendMicro ELF_SSHDOOR.A 20130217
TrendMicro-HouseCall ELF_SSHDOOR.A 20130217