Backdoor.Linux.DOFLOO.AB

ALIASES:

Backdoor.Linux.Dofloo.c (KASPERSKY); ELF/Dofloo.C!tr(FORTINET)

OVERVIEW

INFECTION CHANNEL: Dropped by other malware, Downloaded from the Internet

This Backdoor arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

It executes commands from a remote malicious user, effectively compromising the affected system.

TECHNICAL DETAILS

FILE SIZE: 1,001,465 bytes

FILE TYPE: ELF

MEMORY RESIDENT: Yes

INITIAL SAMPLES RECEIVED DATE: 04 Jun 2020

PAYLOAD: Launches DoS/DDoS attacks, Steals information

**Arrival Details**

This Backdoor arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

**Installation**

半人工斷成一整句 (no.5)

一

This Backdoor adds the following processes:

* sed -i -e '/exit/d' /etc/rc.local
* sed -i -e '/^\r\n|\r|\n$/d' /etc/rc.local
* sed -i -e '/%s/d' /etc/rc.local
* sed -i -e '2 i%s/%s' /etc/rc.local
* sed -i -e '2 i%s/%s start' /etc/rc.d/rc.local
* sed -i -e '2 i%s/%s start' /etc/init.d/boot.local

**Backdoor Routine**

This Backdoor executes the following commands from a remote malicious user:

* Initiate DDoS attacks:
  + TCP flood
  + Challenge Collapsar (CC) attack
* Stop DDoS attack
* Execute shell commands

半人工斷成一整句 (no.7)

一

**Information Theft**

This Backdoor gathers the following data:

* CPU information
* Memory statistics
* IP address of infected machine
* Reads the following information from /proc:
  + /proc/stat
  + /proc/meminfo
  + /proc/cpuinfo
  + /proc/net/dev
  + /proc/self/exe
  + /proc/self/maps
  + /proc/sys/vm/overcommit\_memory
  + /proc/sys/kernel/rtsig-max
  + /proc/sys/kernel/ngroups\_max
  + /proc/sys/kernel/osrelease
  + /proc/self/fd/%d/%s
  + /proc/self/fd
  + /proc/net

**Other Details**

半人工斷成一整句 (no.8)

一

This Backdoor opens the following files:

* /etc/host.conf
* /etc/resolv.conf
* /etc/nsswitch.conf
* /etc/suid-debug
* /etc/ld.so.cache

SOLUTION

MINIMUM SCAN ENGINE: 9.850

FIRST VSAPI PATTERN FILE: 15.910.04

FIRST VSAPI PATTERN DATE: 04 Jun 2020

VSAPI OPR PATTERN FILE: 15.911.00

VSAPI OPR PATTERN DATE: 05 Jun 2020

Scan your computer with your Trend Micro product to delete files detected as Backdoor.Linux.DOFLOO.AB If the detected files have already been cleaned, deleted, or quarantined by your Trend Micro product, no further step is required. You may opt to simply delete the quarantined files. Please check the following Trend Micro Support pages for more information:

Home and Home Office Support

Business Support