BKDR_SARHUST.A

trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr_sarhust.a

Analysis by: Abraham Latimer Camba

- Threat Type: Backdoor
- Destructiveness: No
- Encrypted: No
- In the wild: Yes

OVERVIEW

Infection Channel: Dropped by other malware

This backdoor may be dropped by other malware.

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

It creates an event.

TECHNICAL DETAILS

File Size: 38,400 bytes

File Type: EXE

Memory Resident: Yes

Initial Samples Received Date: 20 Sep 2012

Payload: Connects to URLs/IPs, Compromises system security

Arrival Details

This backdoor may be dropped by the following malware:

TROJ_ARTIEF.PT

Installation

This backdoor drops the following non-malicious files:

- %Temp%\Debug.log - malware's log file
- %Temp%\wmiprvse.ini

(Note: *%Temp%* is the Windows Temporary folder, which is usually C:\Windows\Temp or C:\WINNT\Temp.)

It adds the following mutexes to ensure that only one of its copies runs at any one time:

HUSSARINI

Other System Modifications

This backdoor adds the following registry entries:

HKEY_CURRENT_USER\Software\Microsoft
IntervalTime = "{random number}"

HKEY_CURRENT_USER\Software\Microsoft
ServerID = "{random number}"

Backdoor Routine

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

- Create files
- Read files
- Modify files
- Execute files
- Get file information
- Download additional components

It connects to the following URL(s) to send and receive commands from a remote malicious user:

http://{BLOCKED}i.{BLOCKED}s-mail.com

It posts the following information to its command and control (C&C) server:

- User name

- Computer name
- OS information
- CPU information

Other Details

This backdoor creates the following event(s):

HussarCreate

SOLUTION

Step 1

For Windows XP and Windows Server 2003 users, before doing any scans, please make sure you disable *System Restore* to allow full scanning of your computer.

Step 2

Remove the malware/grayware file that dropped/downloaded BKDR_SARHUST.A

TROJ_ARTIEF.PT

Step 3

Identify and terminate files detected as BKDR_SARHUST.A

[Learn More]

1. If the detected file is displayed in either Windows Task Manager or Process Explorer but you cannot delete it, restart your computer in safe mode. To do this, refer to this link for the complete steps.
2. If the detected file is *not* displayed in either Windows Task Manager or Process Explorer, continue doing the next steps.

Step 4

Delete this registry value

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft article first before modifying your computer's registry.

- In *HKEY_CURRENT_USER\Software\Microsoft*
  IntervalTime = "{random number}"
- In *HKEY_CURRENT_USER\Software\Microsoft*
  ServerID = "{random number}"

Step 5

Search and delete these files

[Learn More]

There may be some component files that are hidden. Please make sure you check the *Search Hidden Files and Folders* checkbox in the "More advanced options" option to include all hidden files and folders in the search result.

- %Temp%\Debug.log
- %Temp%\wmiprvse.ini

Step 6

Scan your computer with your Trend Micro product to delete files detected as BKDR_SARHUST.A. 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 this Knowledge Base page for more information.

Did this description help? Tell us how we did.