



Remediating Hosts Compromised by the Kraken BotArmy

April 4, 2008

Purpose

This document provides instructions for remediating hosts compromised by the Kraken BotArmy. It also provides network-level methods for confirming that a given host is still compromised with Kraken without physically accessing it.

1. Preliminaries

Using its bot malware repository, Damballa has identified the family of malware instances that correspond to the Kraken BotArmy. Following identification, Damballa has performed an in-depth binary analysis of these instances to create host-level instructions for removing the bot malware from a compromised system.

2. Compromise Confirmation

For a number of reasons (e.g., antivirus signature updates), an asset determined to be compromised with Kraken weeks prior may no longer be compromised at the time of inspection. Before proceeding with remediation, confirm that the host is still compromised by running a packet sniffer (e.g., tcpdump, ethereal) and looking for the following network-level symptoms:

- ❖ DNS (domain) lookups to domains ending in *.yi.org, *.dyndns.org, and *.mooo.com
- ❖ Outgoing UDP packets with destination port 447 (encrypted payload)

Note that observation of either of these symptoms is sufficient to conclude that the host is still compromised with Kraken.

3. Remediation

Upon confirming that the host is still compromised with Kraken, it can be remediated by using a simple process, which consists of:

1. Identifying the process name and location of the Kraken bot malware on the host
2. Terminating the Kraken process
3. Deleting the Kraken bot malware and
4. Restarting the system

3.1 Identifying Kraken Process Name and Location

The name of the Kraken malware process will consist of between one and twelve randomly generated alpha characters (i.e. dmdfscsehebx). Using Windows TaskManager, look for an out-of-place process name running on the host that matches this description. For an example, refer to Figure 1 below.

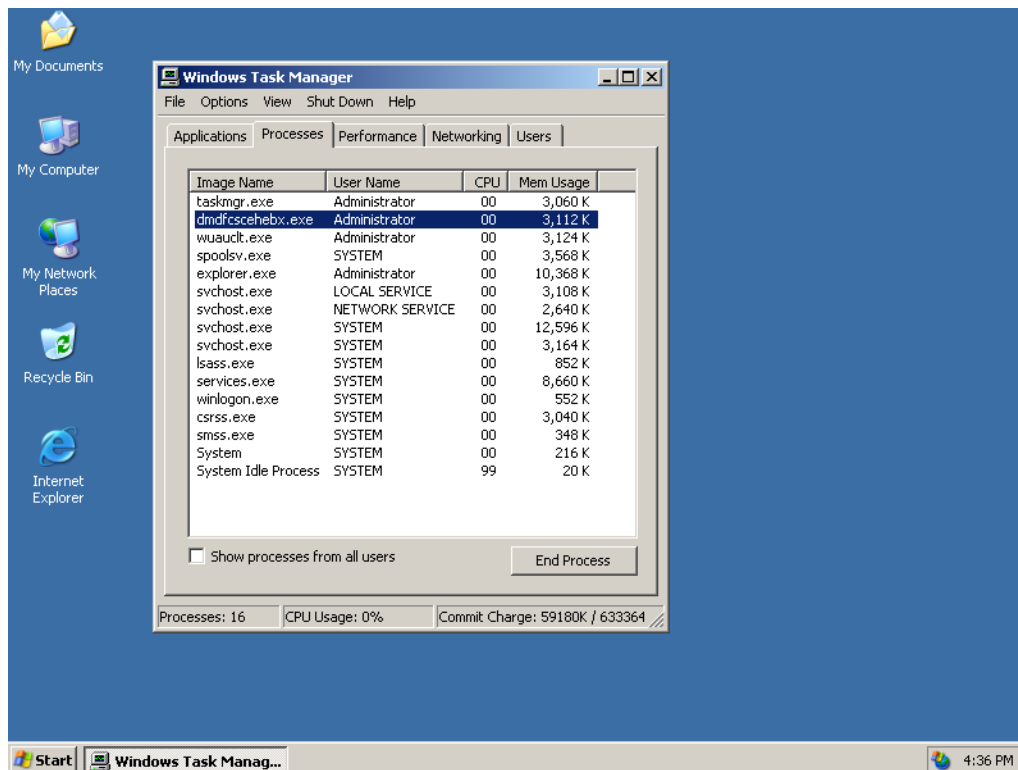


Figure 1: Looking for the Kraken malware randomly generated process name. In this example, the process name is highlighted in blue.

After identifying a candidate Kraken malware process name, confirm its identity by looking for an executable of the same name in the system32 directory (e.g., C:\WINDOWS\system32\). The executable will also have an image file icon, as shown in Figure 2.

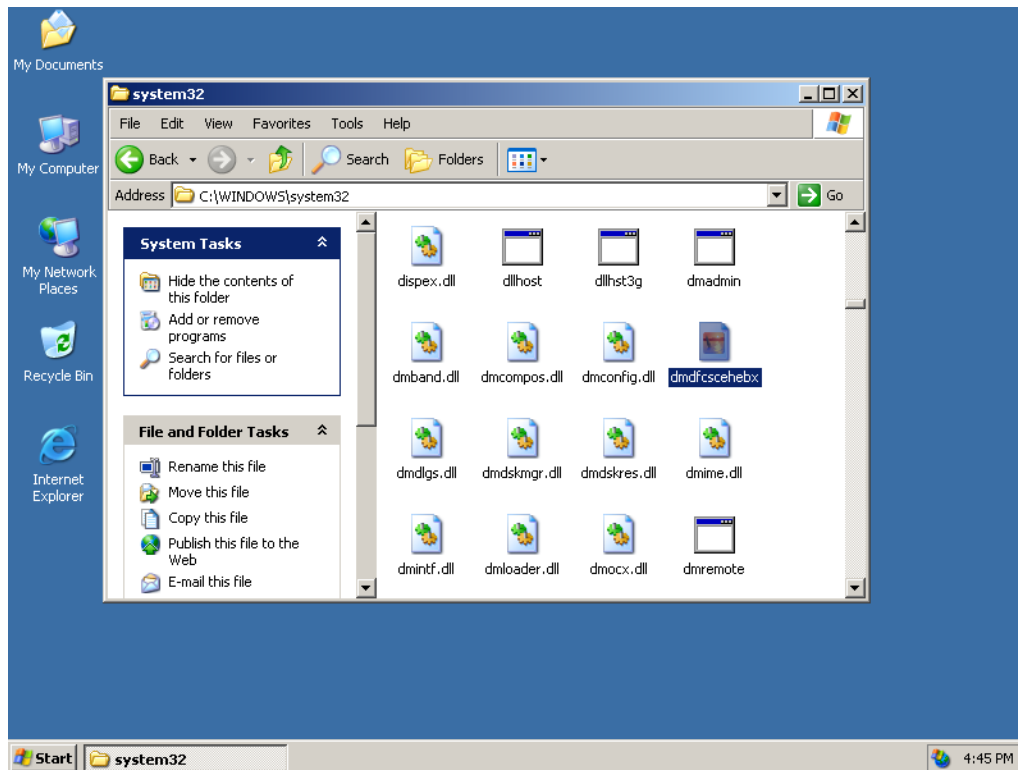


Figure 2: Confirming that the suspected process name corresponds to the Kraken bot malware. In this example, the bot malware executable is highlighted in blue.

3.2 Remediating the Host

Upon confirming the identity of the candidate process name and executable file location, remediate the host by doing the following:

1. Terminate the Kraken malware process. Using Windows TaskManager, right click on the target process and select “End Process”. The process name should disappear from the list in Windows TaskManager.
2. Delete the Kraken malware executable file. Enter the system32 directory containing the executable file, right click on the file, and select delete. If necessary, enter the Windows Recycle Bin and permanently delete the file.
3. Reboot the system.

After rebooting the host, confirm that it no longer exhibits the network-level symptoms described in Section 2. Remediation is complete.

About Damballa, Inc.

Damballa protects businesses from targeted attacks used for organized, online crime. Our unique, global approach rapidly isolates the command-and-control needed to launch multi-network attacks. These signatureless solutions improve security both inside and outside the network perimeter, to stop threats other technologies miss and restore control to legitimate owners. Damballa identifies the severity and intent of targeted attacks such as BotArmies, even when malware can't be detected. These products and services provide a critical window for orderly remediation, and integrate easily into existing infrastructure without requiring additional headcount or complexity. Damballa is privately held, and is headquartered in Atlanta, Georgia.

Copyright © 2008, Damballa, Inc. All rights reserved worldwide.

This page contains the most current trademarks for Damballa, Inc., which include Damballa, the Damballa logo, BotArmy and BotMaster. The absence of a name or logo on this page does not constitute a waiver of any and all intellectual property rights that Damballa, Inc. has established in any of its products, services, names, or logos. All other marks are the property of their respective owners in their corresponding jurisdictions, and are used here in an editorial context, without intent of infringement.