

RE: investigating misuse of the internet

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-07/0050.html>

From: InfoSec (*infosec_at_hpjt.net*)

Date: 07/09/03

To: "'Reava, Jeffrey [IT/0200]'" <jeffrey.reava@pharmacia.com>, "'ICT User'" <ictuser2002@yahoo.com>
Date: Wed, 9 Jul 2003 15:38:30 -0400

Jeff is on the right track.

Another good place to look is the swap/page file, especially if the user is cleaning the history or cache regularly (e.g. setting history retention to 0 days).

Also, going over unallocated clusters for URL entries is a great source of detail that remains even if the user has emptied the receptacles Jeff mentions below.

I would note that if contraband is a possibility on the target machine, you should not be using Ghost. DD will give you a forensically identical bit-stream image of the original drive, as will other digital forensics specific tools (for example EnCase, Safeback). The last testing I saw of Ghost, resulted in unreliable production of forensically identical images.

Pursuing criminal or civil action based on a forensic duplicate of the media will put you in a far better position than a duplicate that has been contaminated by your investigative activities.

There are some software vendors that have released products that allow in-place evidential discovery and investigation across networks by using a servlet on the remote machine to preview and then acquire the data. Depending on the size and in-house expertise, this may be an option worth considering.

As for a checklist, I would take Jeff's suggestions, the locations I listed above, and add to your checklist that you should work from of a duplicate of the media unless it is impossible, or you know it is a matter that will never be passed to law enforcement or the courts.

Hugh

Hugh Pierce, MCP, CISSP
Principal
ForenSec, Ltd.
www.forensec.com

-----Original Message-----

SecurityFocus Microsoft: RE: investigating misuse of the internet

From: Reava, Jeffrey [IT/0200] [mailto:jeffrey.reava@pharmacia.com]
Sent: Wednesday, July 09, 2003 8:53 AM
To: 'ICT User'; focus-ms@securityfocus.com
Subject: RE: investigating misuse of the internet

Assuming that you're using IE, here is a list that will be a fair indicator:

Temporary Internet Files
History
Cookies
Index.dat – use pasco, spider, datalifter (\$), bintext or strings.exe to
retrieve saved browsing history

then some registry keys may be important to check also:

typed URLs from Internet Explorer Address Bar (unaffected by 0-day History
setting)
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Windows Explorer OpenSaveMRU list (If any files are saved to other locations
using the File|Save common control dialog box)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg3
2\OpenSaveMRU

Contents of the Run line
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

If legality is a concern here, its best to use these tools on a ghost or dd
image of the drive, not the original system.

Depending on how much time it takes you to gather and present the
information, it may make sense to automate the imaging and data extraction
for this specific type of investigative request. The registry piece may be a
bit dicey, but everything else can be automated using Sleuthkit forensic
tools. I'm working on a process to do that; if you think it would be helpful
drop me a note and I'll share what I've got.

Jeff

-----Original Message-----

From: ICT User [mailto:ictuser2002@yahoo.co.uk]
Sent: Wednesday, July 09, 2003 4:22 AM
To: focus-ms@securityfocus.com
Subject: investigating misuse of the internet

Hello all,

Occasionally our monitoring software alerts us that
someone has tried to access a dodgy web site. If it
is deemed serious enough then as well as the reports
the we can generate from the software, we are asked to

RE: investigating misuse of the internet

SecurityFocus Microsoft: RE: investigating misuse of the internet

actually go and check out the user's machine for any evidence of misuse.

Does anyone know of a formal check list of stuff to go through when doing this on a Windows PC (98 or 2000). I have found lots of info about what to look for when investigating a hacked PC, but what about when looking for signs of a user's internet activity? Temporary internet files, history, cookies, search for jpegs, mpegs, etc. These are the sort of things we normally look at, but I want to make sure that I don't miss anything important just in case it goes legal.

Also, if the user had set Internet Explorer options to keep 0 days history then does this mean all evidence has gone, or is there anything else I can look at, e.g. any registry keys?

Thanks,

Andy

Yahoo! Plus – For a better Internet experience
<http://uk.promotions.yahoo.com/yplus/yoffer.html>

-

--
This communication is intended solely for the use of the addressee and may contain information that is legally privileged, confidential or exempt from disclosure. If you are not the intended recipient, please note that any dissemination, distribution, or copying of this communication is strictly prohibited. Anyone who receives this message in error should notify the sender immediately and delete it from his or her computer.

-

--

