

Forum:[Hack Forums](#)

Thread: [\[MRT-X Academy\] OTL: Custom Scans \[Legacy Tool\] \[Optional\]](#)

Tha Sneak - February 13, 2025, 11:36 pm

Old Timer's Tools: OTL – Custom Scans Guide

1. Introduction

OTL (Old Timer's List-It) is a powerful diagnostic tool used for custom system scans to detect malware, system changes, and other anomalies. If you understand how OTL logs work and what the various commands do, you can extract more detailed information about an infected system.

Custom scans allow you to input specific scripts to analyze targeted areas of the system. By using custom scripts, you can identify malware, corrupted system files, and hijacked settings with precision.

2. Why Use Custom Scans?

Today's malware infections are more advanced and can:

- Take over systems

- Modify core system files

- Cause system crashes or prevent booting

- Disable security tools

Some common system files that malware can infect include:

- Code atapi.sys

- iastr.sys

- scecli.dll

- netlogon.dll

- eventlog.dll

- cngaudit.dll

- user32.dll

By setting up OTL custom scans to search for these files, you can retrieve detailed logs similar to what SystemLook provides.

? Important: If you need quick results or are not using OTL, then SystemLook can be an alternative.

3. Key OTL Commands and Their Functions

Each OTL command serves a specific function:

Code netsvcs - Lists all services.
msconfig - Lists any changes in MSCONFIG.
safebootminimal - Detects Safe Mode errors.
safebootnetwork - Detects Safe Mode errors.
activex - Lists all ActiveX entries for Internet Explorer.
drivers32 - Lists all drivers.

Additional Custom Scan Commands:

Code c:\\$recycle.bin*.*/s? Scans the Recycle Bin for files and folders.
? The \s\` flag lists subfolders and their contents.

Code

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install\LastSuccessTime /rs? Checks when the last successful Windows Update installation occurred.

Code %systemroot%\system32*.dll /lockedfiles? Scans for locked DLL files in the System32 folder.

Code %systemroot%\Tasks*.job /lockedfiles? Scans for locked scheduled tasks in the Tasks folder.

4. How to Perform an OTL Custom Scan

Step 1: Download OTL

Download [OTL](#) and save it to your Desktop.

Step 2: Run OTL Double-click the OTL.exe icon.

Ensure all other windows are closed.

Let it run uninterrupted.

Step 3: Paste the Custom Scan Script

Under the Custom Scan box, paste the following script:

Code netsvcs
msconfig
safebootminimal
safebootnetwork
activex
drivers32
%SYSTEMDRIVE%*.exe
%systemroot%*. /mp /s
c:\\$recycle.bin*.*/s
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install\LastSuccessTime /rs
/md5start

eventlog.dll
scecli.dll
netlogon.dll
cngaudit.dll
scecli.dll
ntelogon.dll
logevent.dll
iaStor.sys
nvstor.sys
nvstor32.sys
atapi.sys
IdeChnDr.sys
viasraid.sys
AGP440.sys
vaxscsi.sys
nvatabus.sys
viamraid.sys
nvata.sys
nvgts.sys
iastorv.sys
ViPrt.sys
eNetHook.dll
explorer.exe
svchost.exe
userinit.exe
qmgr.dll
ws2_32.dll
proquota.exe
imm32.dll
kernel32.dll
ndis.sys
autochk.exe
spoolsv.exe
xmlprov.dll
ntmssvc.dll
mswsock.dll
Beep.SYS
ntfs.sys
termsrv.dll
sfcfiles.dll
st3shark.sys
ahcix86.sys
srsvc.dll
nvr32.sys
/md5stop
%systemroot%\system32*.dll /lockedfiles
%systemroot%\Tasks*.job /lockedfiles
Step 4: Run the Scan Click the Quick Scan button.

Do not change any settings unless instructed to.

The scan should complete within a few minutes.

Step 5: Retrieve the Logs When the scan completes, two Notepad windows will open:

- OTL.Txt (main log)
- Extras.Txt (additional system information)

These files are saved in the same location as OTL.exe.

Copy the contents of these files:

- Edit -> Select All
- Edit -> Copy

Paste them into your response for analysis.

5. Analyzing OTL Scan Results

Once you receive the OTL logs, analyze them for:

- ? Unknown system changes
- ? Malicious files or registry modifications
- ? Startup entries linked to malware
- ? Hijacked ActiveX controls and system services

Use ThreatExpert.com, VirusTotal.com, Jotti.org to check suspicious MD5 hashes.

6. Additional Resources

? More in-depth tutorial on OTL:

<https://hackforums.net/showthread.php?tid=6292262>

Tha Sneak - March 1, 2025, 8:32 pm

Please do NOT reply to this thread in case information needs to be added or edited.

If you have a questions about the contents of the thread or other tutorials please go to this thread and post your question in this thread: <https://hackforums.net/showthread.php?tid=6293473>

Thanks,

Tha Sneak