Information Assurance

Using Honeyclients for Detection and Response Against New Attacks

Kathy Wang

MITRE Corporation

knwang@mitre.org

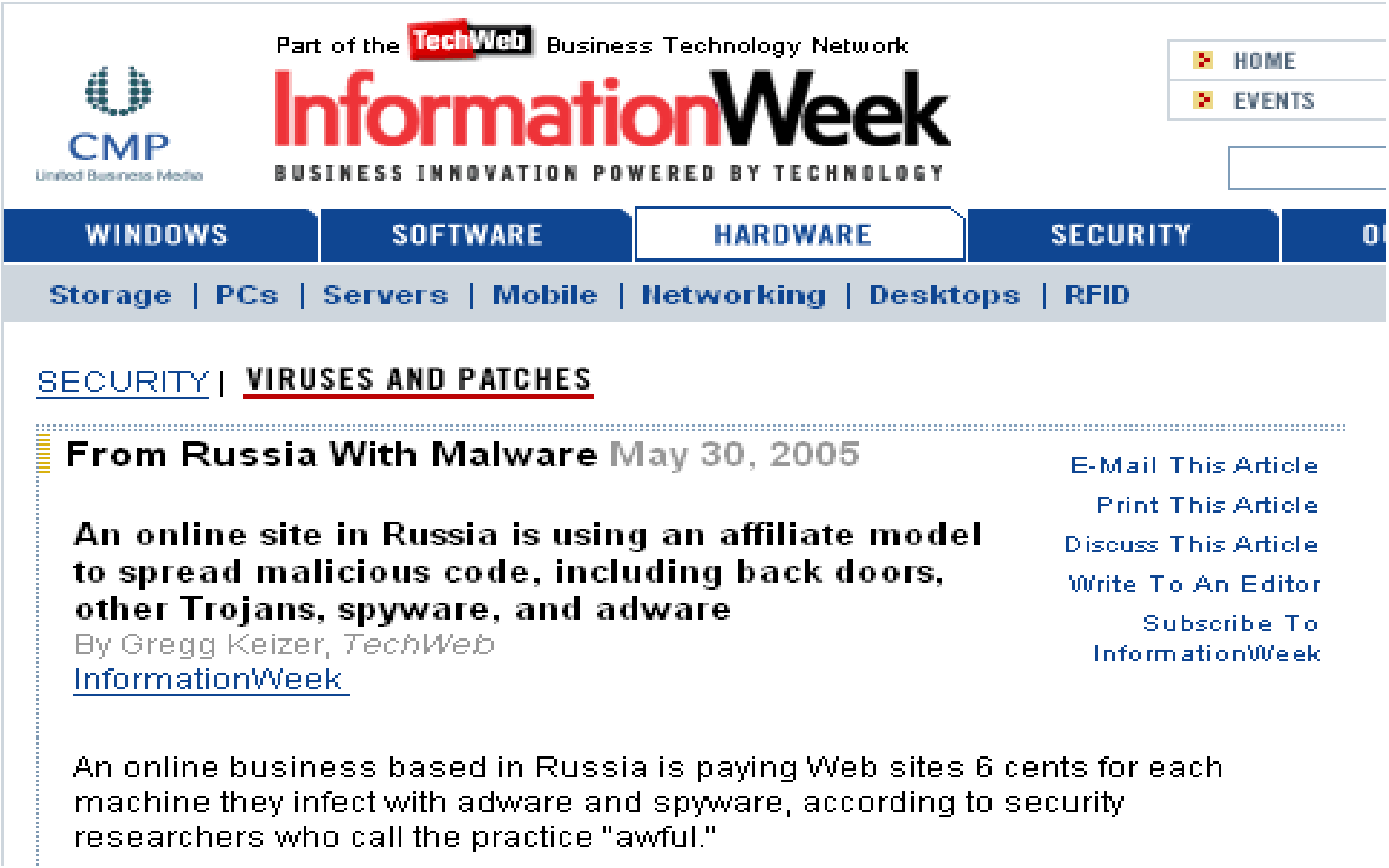
MITRE Technology Program

Problem

We lack a proactive detection technology for client-side attacks

- **Client-side exploits are a growing threat**
  - **Lots of client-side vulnerabilities**
    - **Microsoft Internet Explorer has more than 50 serious vulnerabilities in last 6 months (SecurityFocus database)**
  - **Lots of client-side exploits**
    - **90% of all PCs harbor spyware (Webroot, 2006)**
- **We need to be able to proactively detect and characterize client-side attacks before we get hit**

A New 'Business' Model


CMP
United Business Media
Part of the TechWeb Business Technology Network
InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY
HOME
EVENTS
WINDOWS
SOFTWARE
HARDWARE
SECURITY
O
Storage | PCs | Servers | Mobile | Networking | Desktops | RFID
SECURITY | VIRUSES AND PATCHES
E-Mail This Article
Print This Article
Discuss This Article
Write To An Editor
Subscribe To InformationWeek

From Russia With Malware May 30, 2005

An online site in Russia is using an affiliate model to spread malicious code, including back doors, other Trojans, spyware, and adware

By Gregg Keizer, *TechWeb*
InformationWeek

An online business based in Russia is paying Web sites 6 cents for each machine they infect with adware and spyware, according to security researchers who call the practice "awful."

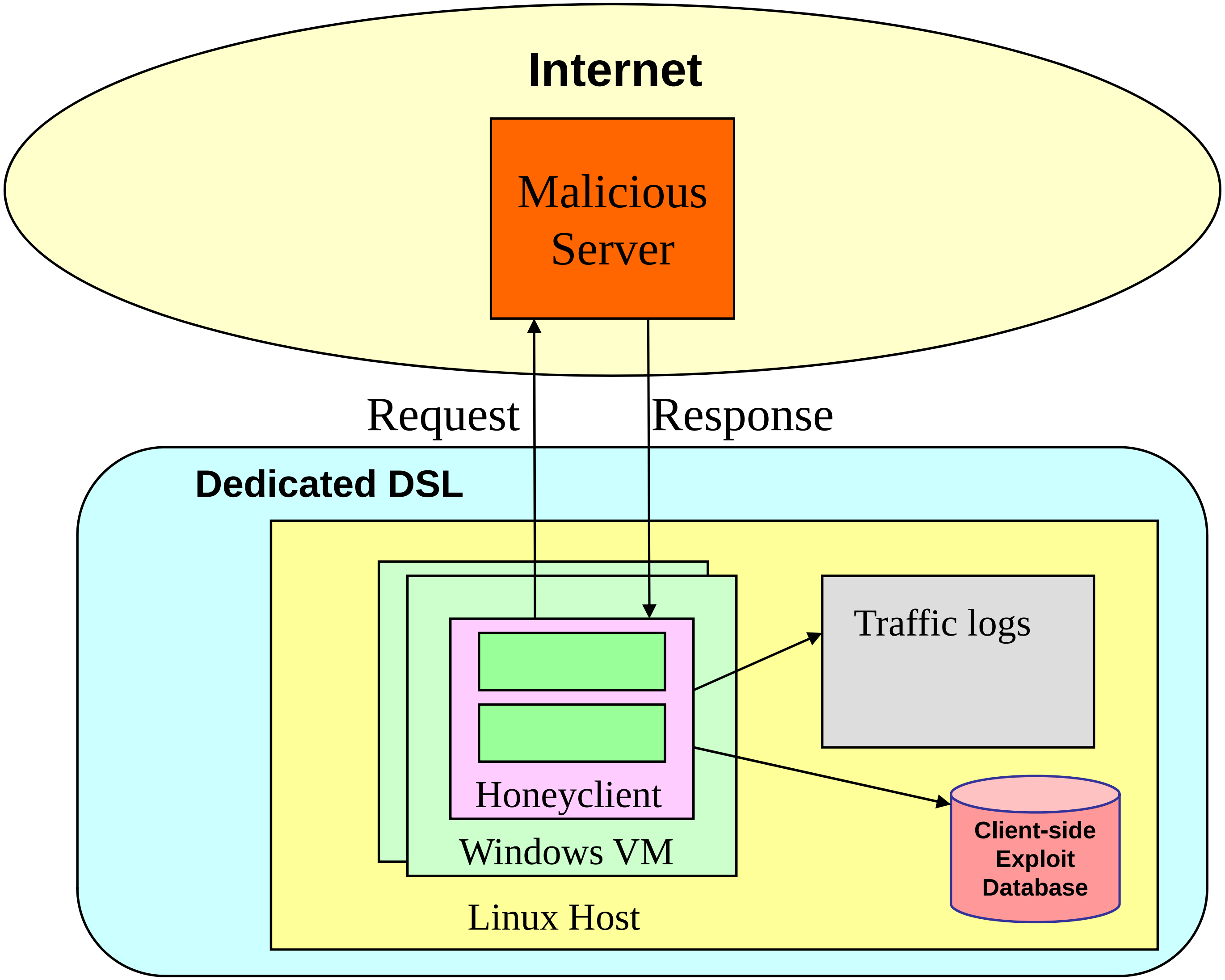
Current Situation

- Current coverage of client-side exploits is inadequate
  - Over 50% of recent vulnerabilities are client-based (SecurityFocus)
  - Only 1.5% of Snort Intrusion Detection System signatures are based on client-side attacks (www.snort.org)
- Honeypots
  - Detect server-side attacks
  - Passive devices
- Current methods of client-side exploit detection are reactive
  - Anti-virus
  - Anti-spyware
  - Clueful users

Background - Honeyclients

- Honeyclients provide capability to proactively detect client-side exploits
  - A honeyclient is a system that drives a client application to potentially malicious servers
  - Any changes made on honeyclient system are unauthorized – no false positives!
  - We detect exploits even without prior signatures

Basic Honeyclient Package



Prototype Capabilities

- Integrity checks
- Drive IE
- Extract URLs
- Recurse (Internal)
- Recurse (External)
- Virtual host
- Protective firewall
- Exploit DB
- Image rotation
- Modular clients
- Traffic history
- Secure logging
- Memory checks

New Honeyclient Project Capabilities

- Active content site module
  - Automates Macromedia Flash site spidering
- Keyword scoring module
  - More intelligent browsing of links
- Comprehensive honeyclient database module with CGI-based web front-end
  - Easy querying for malware-related activity and characteristics
  - Quick demo
- Real-time integrity checks
  - Significant integrity check time improvement
- Fully operational honeyclients
  - 7 honeyclients operating on 24/7 basis
- Extensive honeyclient project website deployed
  - SVN repository, wiki, ticketing system, weblogs
  - Google Analytics

Additional Project Information

- Our project website
  - http://honeyclient.mitre.org
- Send us email, and we will add you to the mailing list
  - honeyclient@mitre.org
  - knwang@mitre.org
- We need beta testers!
  - http://www.honeyclient.org/trac/wiki/download
- Developers are welcome too!
  - SVN repository is available, let us know if you'd like access

Additional Information

Why Should You Run Honeyclients?

- Operational benefits
  - Increase your visibility of emerging client-side threats
  - Malware collection and analysis
  - Share your results, and obtain other organizations' results

- Networking benefits
  - Group forum meetings
  - Government, industry, academic participation
  - Discussion on latest trends in client-side exploits

Why Should You Run Honeyclients?

- Cost benefits
  - HoneyClient package and Linux OSes are open-sourced
  - VMWare Server is free
  - Your costs: hardware, Internet connection, Windows license, analysts

- Other factors to consider
  - Your private data will not be leaked
  - Opportunity to provide public service through data sharing

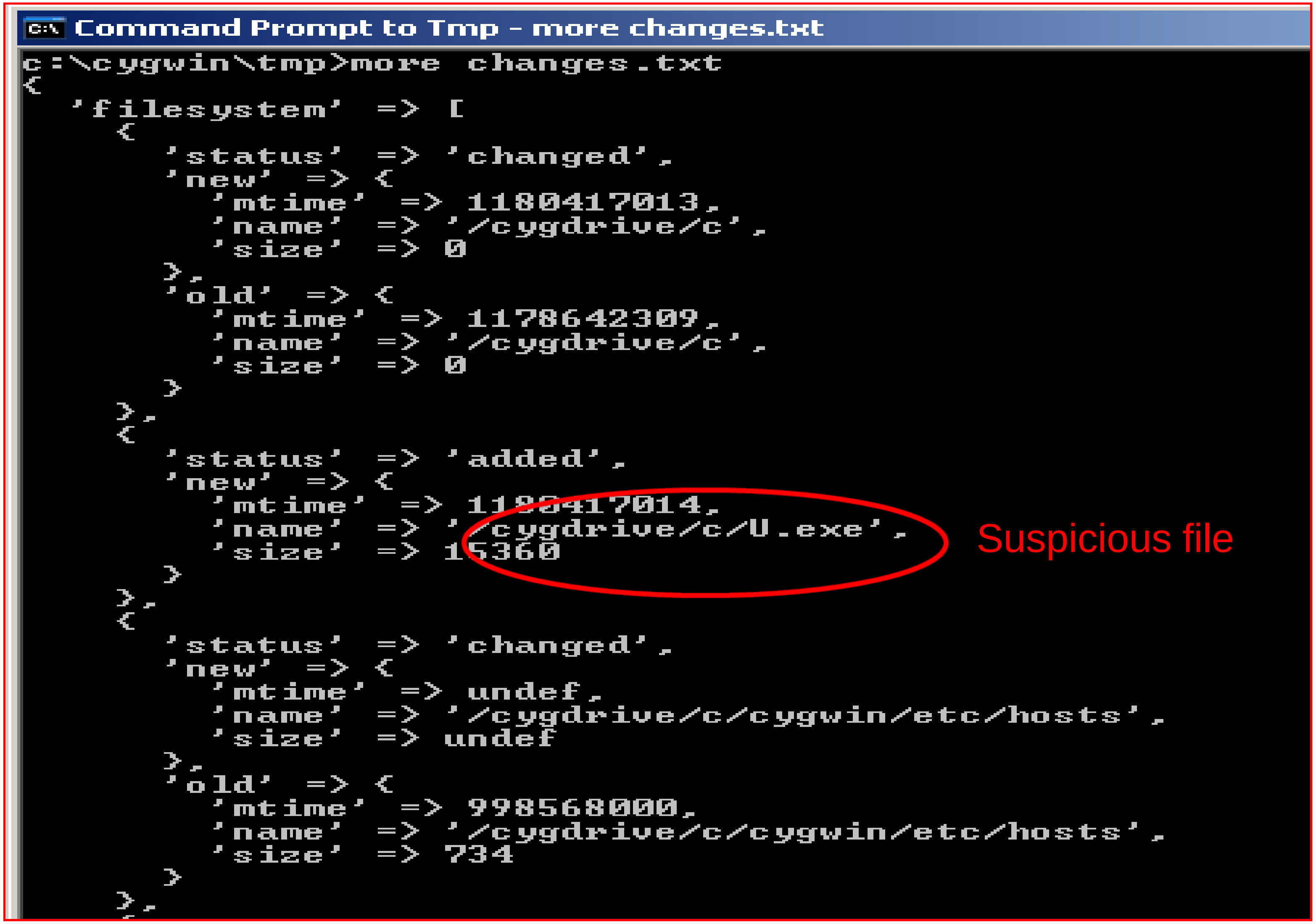
Some Honeyclient Case Examples

<Disclaimer>

Please DO NOT go to any of the sites on the following slides unless you REALLY know what you're doing!!!)

</Disclaimer>

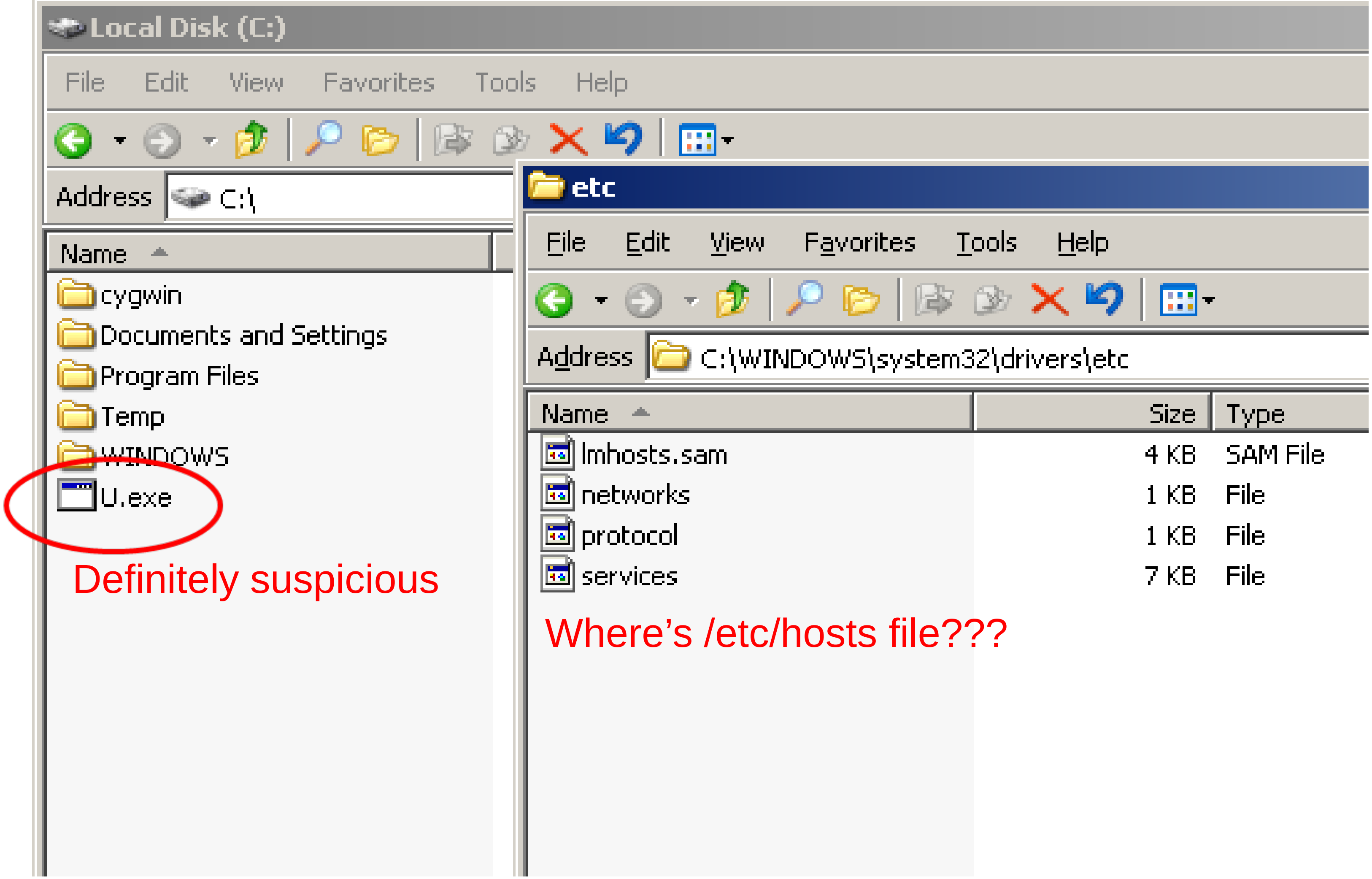
www.world0fwarcraft.net (Changes)



```
c:\cygwin\tmp>more changes.txt
{
  'filesystem' => [
    {
      'status' => 'changed',
      'new'  => {
        'mtime'  => 1180417013,
        'name'  => '/cygdrive/c',
        'size'  => 0
      },
      'old'  => {
        'mtime'  => 1178642309,
        'name'  => '/cygdrive/c',
        'size'  => 0
      }
    },
    {
      'status' => 'added',
      'new'  => {
        'mtime'  => 1180417014,
        'name'  => '/cygdrive/c/U.exe',
        'size'  => 15360
      }
    },
    {
      'status' => 'changed',
      'new'  => {
        'mtime'  => undef,
        'name'  => '/cygdrive/c/cygwin/etc/hosts',
        'size'  => undef
      },
      'old'  => {
        'mtime'  => 998568000,
        'name'  => '/cygdrive/c/cygwin/etc/hosts',
        'size'  => 734
      }
    },
```

Suspicious file

www.world0fwarcraft.net (Changes)


Local Disk (C:)
File Edit View Favorites Tools Help
etc
File Edit View Favorites Tools Help

Address C:\

Name

cygwin
Documents and Settings
Program Files
Temp
WINDOWS
U.exe

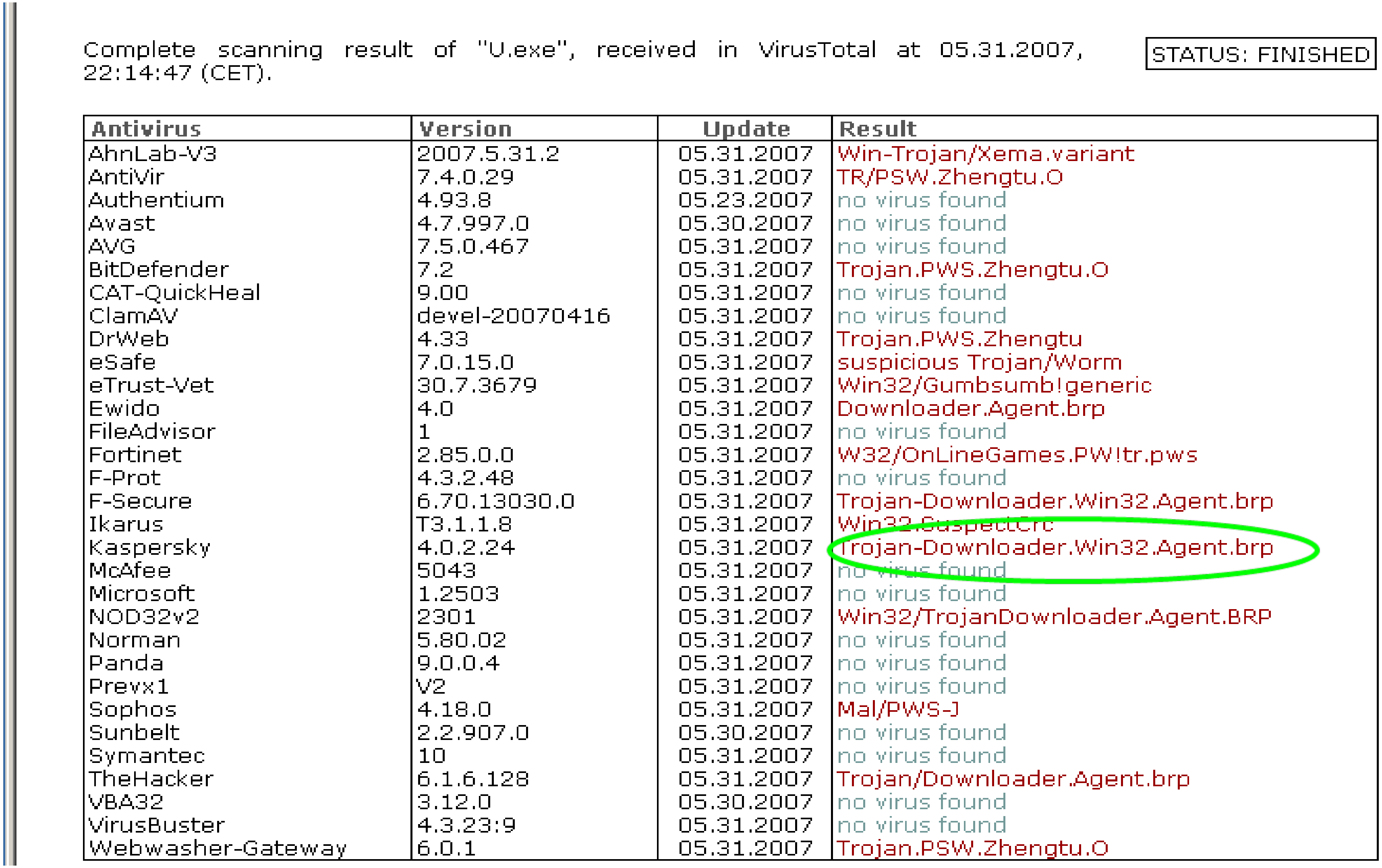
Definitely suspicious

Address C:\WINDOWS\system32\drivers\etc

Name	Size	Type
lmhosts.sam	4 KB	SAM File
networks	1 KB	File
protocol	1 KB	File
services	7 KB	File

Where’s /etc/hosts file???

www.world0fwarcraft.net (Scans)

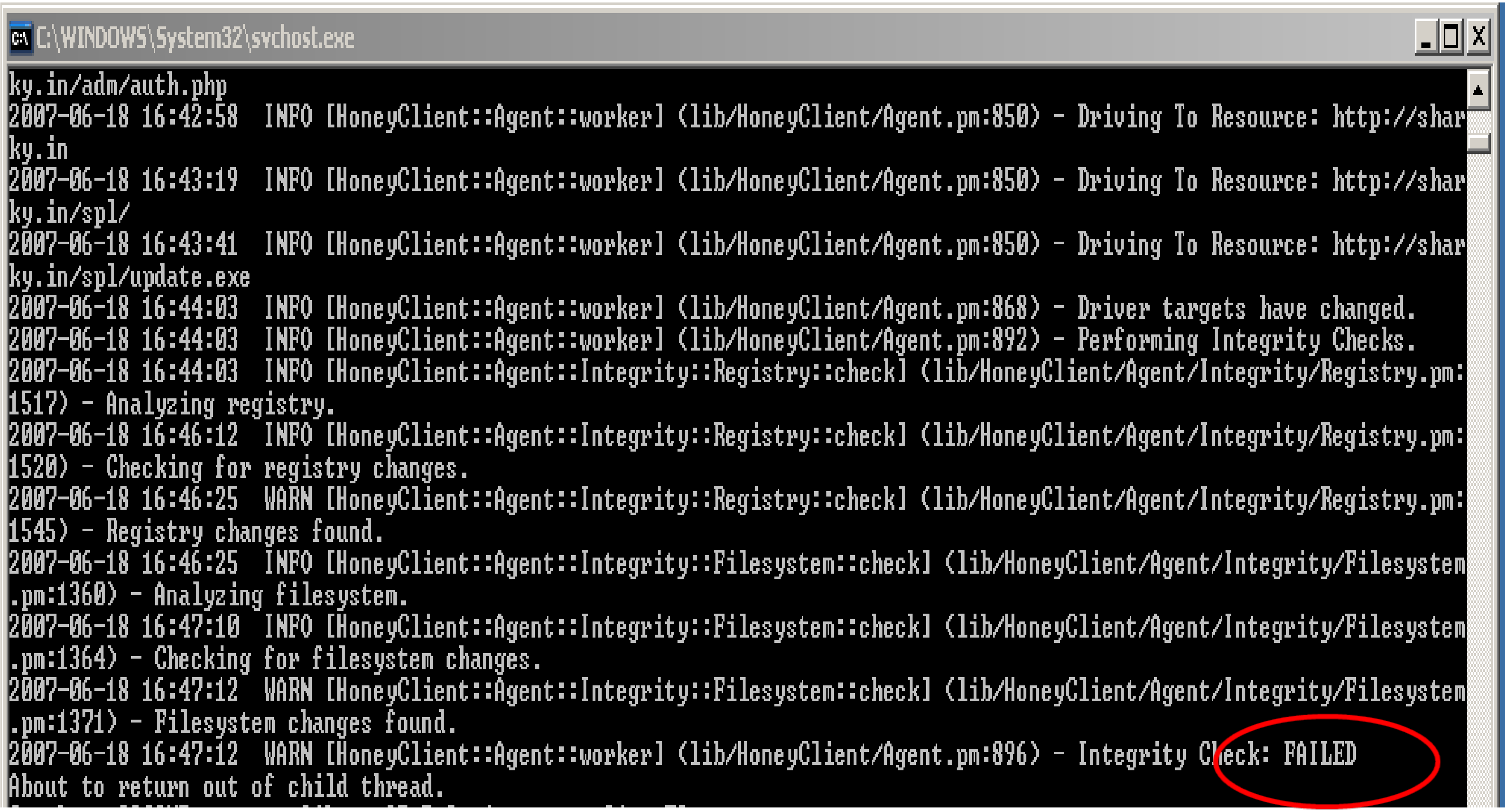


Complete scanning result of "U.exe", received in VirusTotal at 05.31.2007, 22:14:47 (CET).

STATUS: FINISHED

Antivirus	Version	Update	Result
AhnLab-V3	2007.5.31.2	05.31.2007	Win-Trojan/Xema.variant
AntiVir	7.4.0.29	05.31.2007	TR/PSW.Zhengtu.O
Authentium	4.93.8	05.23.2007	no virus found
Avast	4.7.997.0	05.30.2007	no virus found
AVG	7.5.0.467	05.31.2007	no virus found
BitDefender	7.2	05.31.2007	Trojan.PWS.Zhengtu.O
CAT-QuickHeal	9.00	05.31.2007	no virus found
ClamAV	devel-20070416	05.31.2007	no virus found
DrWeb	4.33	05.31.2007	Trojan.PWS.Zhengtu
eSafe	7.0.15.0	05.31.2007	suspicious Trojan/Worm
eTrust-Vet	30.7.3679	05.31.2007	Win32/Gumbsumb!generic
Ewido	4.0	05.31.2007	Downloader.Agent.brp
FileAdvisor	1	05.31.2007	no virus found
Fortinet	2.85.0.0	05.31.2007	W32/OnLineGames.PW!tr.pws
F-Prot	4.3.2.48	05.31.2007	no virus found
F-Secure	6.70.13030.0	05.31.2007	Trojan-Downloader.Win32.Agent.brp
Ikarus	T3.1.1.8	05.31.2007	Win32.SuspectCrc
Kaspersky	4.0.2.24	05.31.2007	Trojan-Downloader.Win32.Agent.brp
McAfee	5043	05.31.2007	no virus found
Microsoft	1.2503	05.31.2007	no virus found
NOD32v2	2301	05.31.2007	Win32/TrojanDownloader.Agent.BRP
Norman	5.80.02	05.31.2007	no virus found
Panda	9.0.0.4	05.31.2007	no virus found
Prevx1	V2	05.31.2007	no virus found
Sophos	4.18.0	05.31.2007	Mal/PWS-J
Sunbelt	2.2.907.0	05.30.2007	no virus found
Symantec	10	05.31.2007	no virus found
TheHacker	6.1.6.128	05.31.2007	Trojan/Downloader.Agent.brp
VBA32	3.12.0	05.30.2007	no virus found
VirusBuster	4.3.23:9	05.31.2007	no virus found
Webwasher-Gateway	6.0.1	05.31.2007	Trojan.PSW.Zhengtu.O

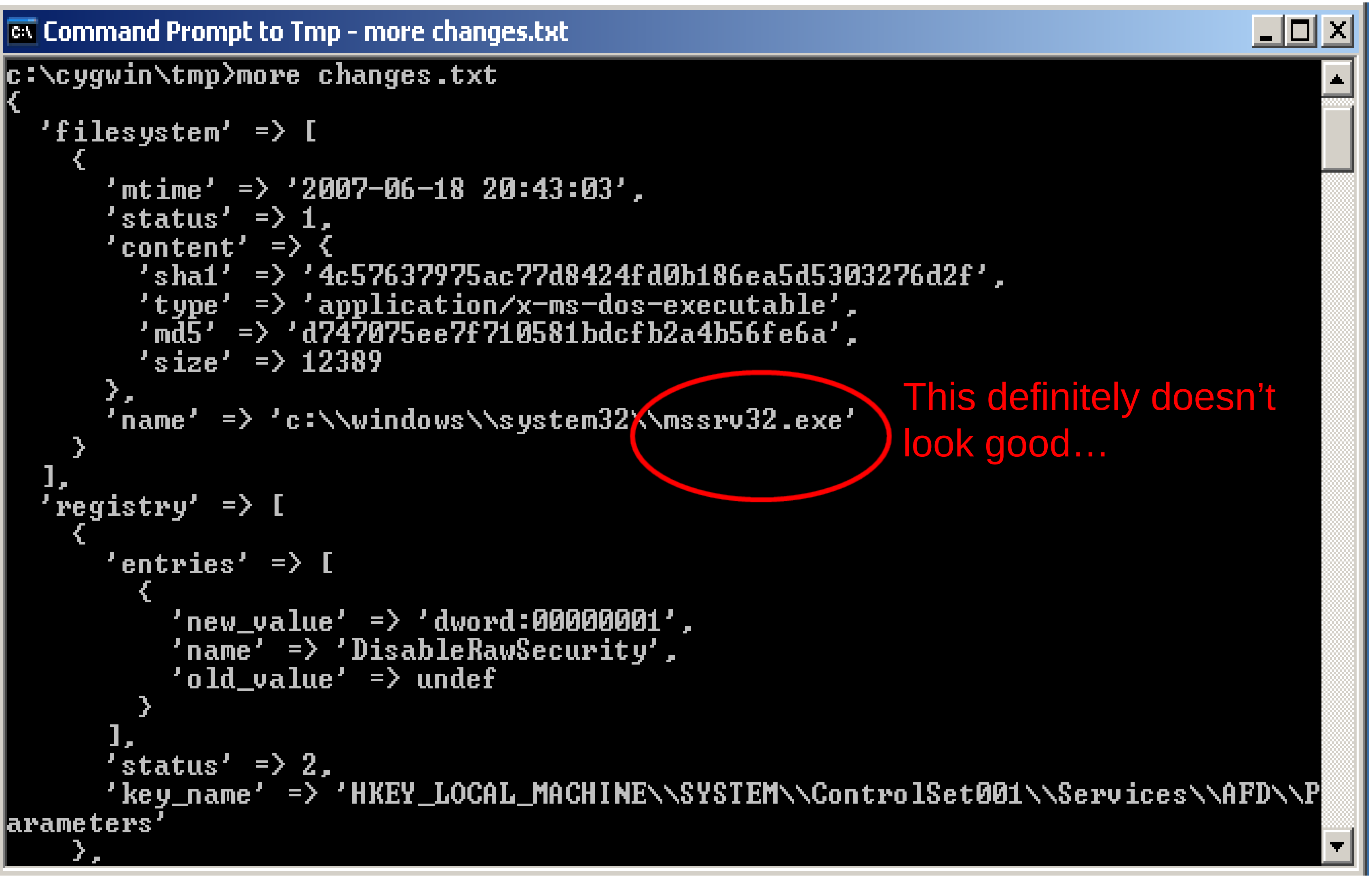
www.sharky.in (Changes)



```
ky.in/adm/auth.php
2007-06-18 16:42:58  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:850) - Driving To Resource: http://shar
ky.in
2007-06-18 16:43:19  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:850) - Driving To Resource: http://shar
ky.in/spl/
2007-06-18 16:43:41  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:850) - Driving To Resource: http://shar
ky.in/spl/update.exe
2007-06-18 16:44:03  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:868) - Driver targets have changed.
2007-06-18 16:44:03  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:892) - Performing Integrity Checks.
2007-06-18 16:44:03  INFO [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1517) - Analyzing registry.
2007-06-18 16:46:12  INFO [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1520) - Checking for registry changes.
2007-06-18 16:46:25  WARN [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1545) - Registry changes found.
2007-06-18 16:46:25  INFO [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1360) - Analyzing filesystem.
2007-06-18 16:47:10  INFO [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1364) - Checking for filesystem changes.
2007-06-18 16:47:12  WARN [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1371) - Filesystem changes found.
2007-06-18 16:47:12  WARN [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:896) - Integrity Check: FAILED
About to return out of child thread.
```

Suspicious behavior, let's check it out further!

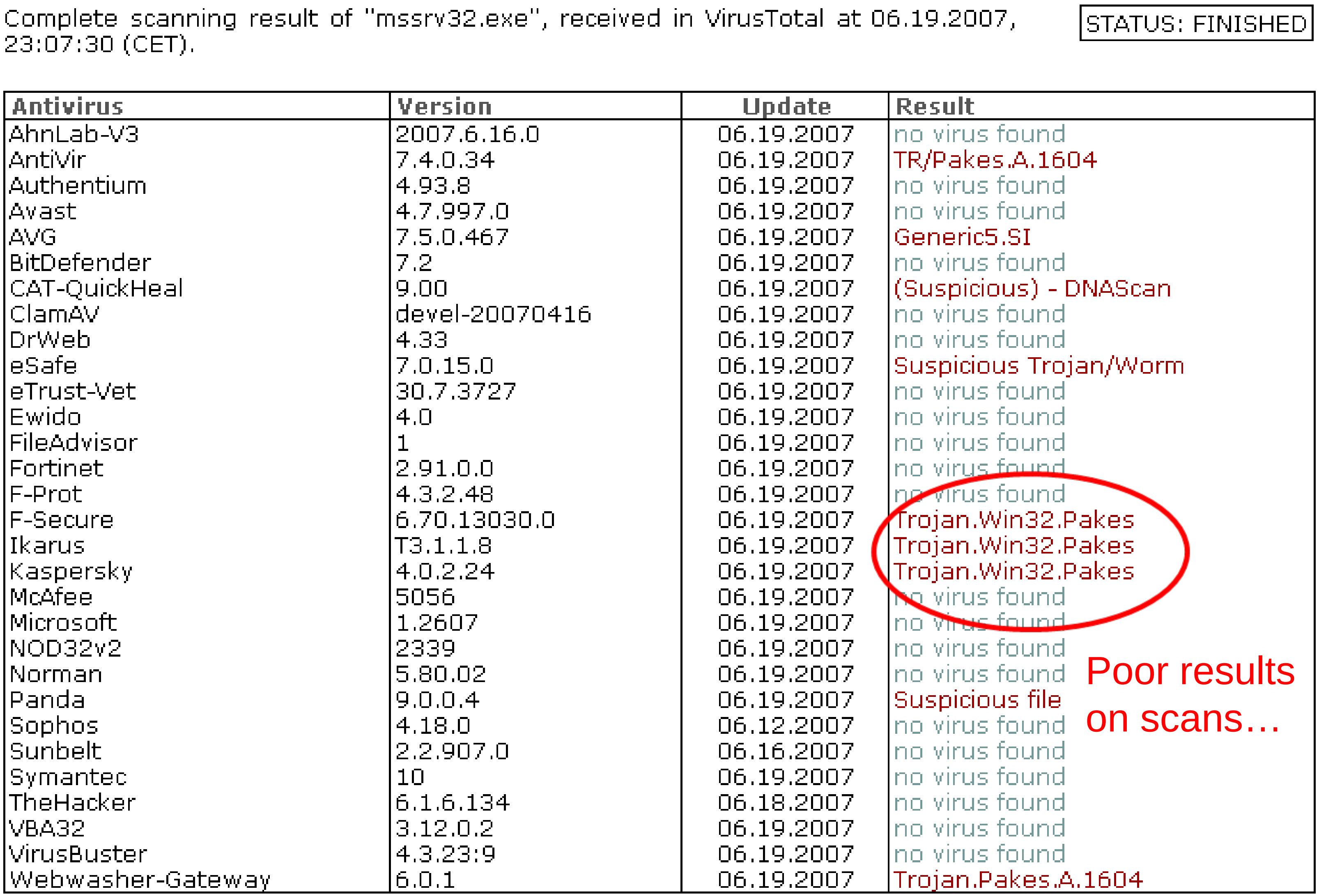
www.sharky.in (Changes)



```
c:\cygwin\tmp>more changes.txt
{
  'filesystem' => [
    {
      'mtime' => '2007-06-18 20:43:03',
      'status' => 1,
      'content' => {
        'sha1' => '4c57637975ac77d8424fd0b186ea5d5303276d2f',
        'type' => 'application/x-ms-dos-executable',
        'md5' => 'd747075ee7f710581bdcfb2a4b56fe6a',
        'size' => 12389
      },
      'name' => 'c:\\windows\\system32\\mssrv32.exe'
    }
  ],
  'registry' => [
    {
      'entries' => [
        {
          'new_value' => 'dword:00000001',
          'name' => 'DisableRawSecurity',
          'old_value' => undef
        }
      ],
      'status' => 2,
      'key_name' => 'HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\AFD\\P
arameters'
    },
```

This definitely doesn't look good…

www.sharky.in (Scan)



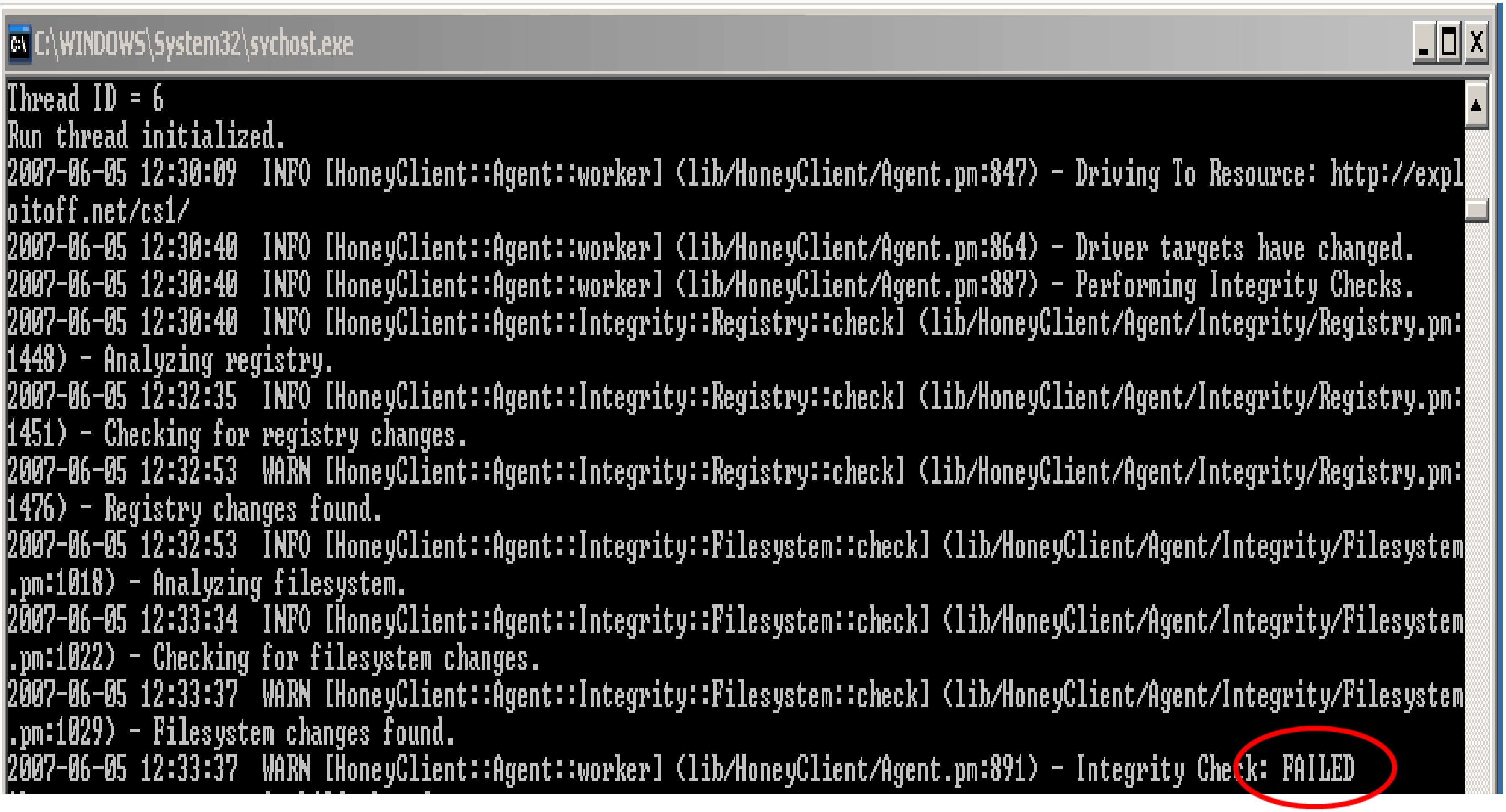
Complete scanning result of "mssrv32.exe", received in VirusTotal at 06.19.2007, 23:07:30 (CET).

STATUS: FINISHED

Antivirus	Version	Update	Result
AhnLab-V3	2007.6.16.0	06.19.2007	no virus found
AntiVir	7.4.0.34	06.19.2007	TR/Pakes.A.1604
Authentium	4.93.8	06.19.2007	no virus found
Avast	4.7.997.0	06.19.2007	no virus found
AVG	7.5.0.467	06.19.2007	Generic5.SI
BitDefender	7.2	06.19.2007	no virus found
CAT-QuickHeal	9.00	06.19.2007	(Suspicious) - DNAScan
ClamAV	devel-20070416	06.19.2007	no virus found
DrWeb	4.33	06.19.2007	no virus found
eSafe	7.0.15.0	06.19.2007	Suspicious Trojan/Worm
eTrust-Vet	30.7.3727	06.19.2007	no virus found
Ewido	4.0	06.19.2007	no virus found
FileAdvisor	1	06.19.2007	no virus found
Fortinet	2.91.0.0	06.19.2007	no virus found
F-Prot	4.3.2.48	06.19.2007	no virus found
F-Secure	6.70.13030.0	06.19.2007	Trojan.Win32.Pakes
Ikarus	T3.1.1.8	06.19.2007	Trojan.Win32.Pakes
Kaspersky	4.0.2.24	06.19.2007	Trojan.Win32.Pakes
McAfee	5056	06.19.2007	no virus found
Microsoft	1.2607	06.19.2007	no virus found
NOD32v2	2339	06.19.2007	no virus found
Norman	5.80.02	06.19.2007	no virus found
Panda	9.0.0.4	06.19.2007	Suspicious file
Sophos	4.18.0	06.12.2007	no virus found
Sunbelt	2.2.907.0	06.16.2007	no virus found
Symantec	10	06.19.2007	no virus found
TheHacker	6.1.6.134	06.18.2007	no virus found
VBA32	3.12.0.2	06.19.2007	no virus found
VirusBuster	4.3.23:9	06.19.2007	no virus found
Webwasher-Gateway	6.0.1	06.19.2007	Trojan.Pakes.A.1604

Poor results on scans…

www.exploitoff.net (Changes)

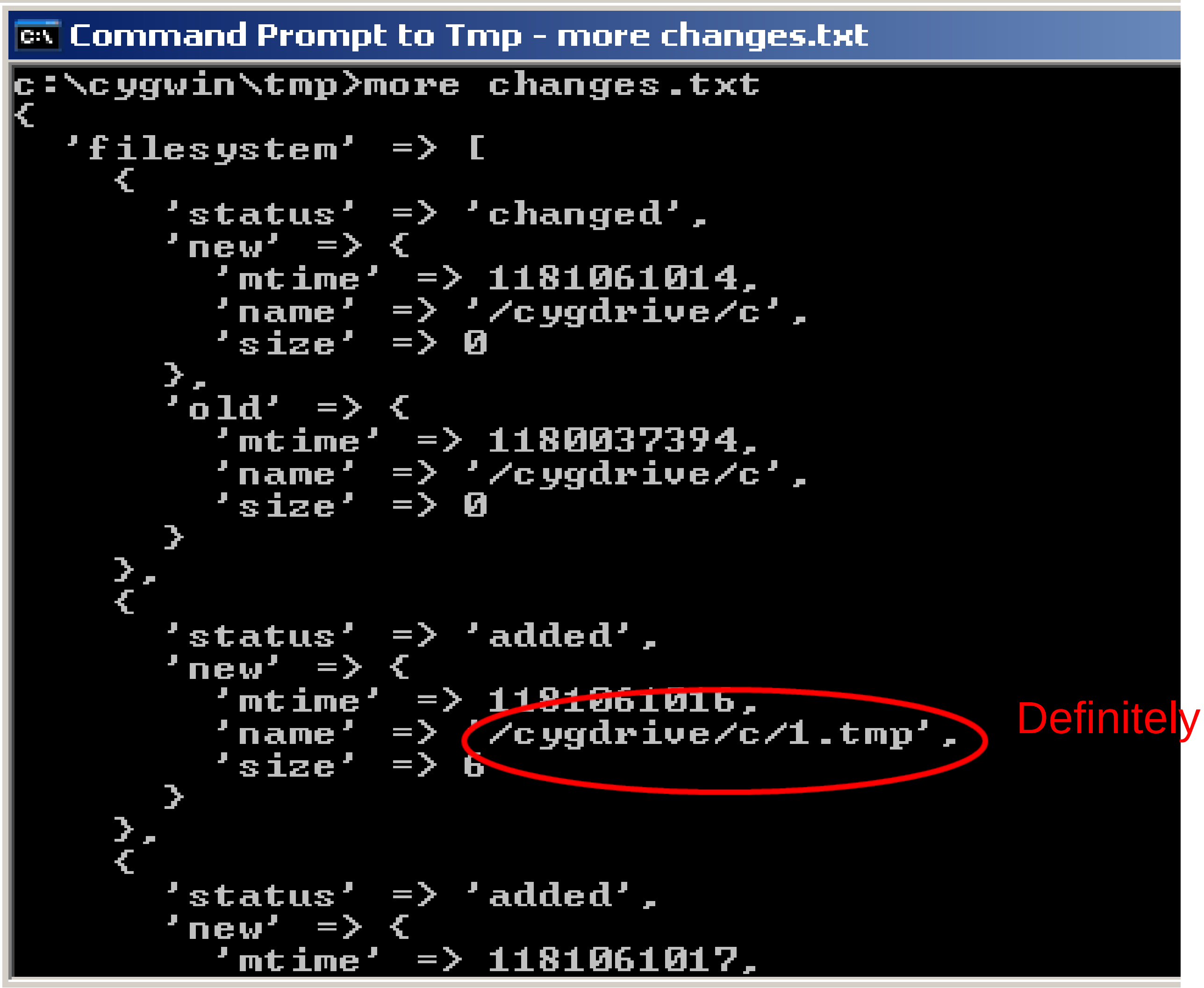


C:\WINDOWS\System32\svchost.exe

```
Thread ID = 6
Run thread initialized.
2007-06-05 12:30:09  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:847) - Driving To Resource: http://expl
oitoff.net/cs1/
2007-06-05 12:30:40  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:864) - Driver targets have changed.
2007-06-05 12:30:40  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:887) - Performing Integrity Checks.
2007-06-05 12:30:40  INFO [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1448) - Analyzing registry.
2007-06-05 12:32:35  INFO [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1451) - Checking for registry changes.
2007-06-05 12:32:53  WARN [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1476) - Registry changes found.
2007-06-05 12:32:53  INFO [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1018) - Analyzing filesystem.
2007-06-05 12:33:34  INFO [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1022) - Checking for filesystem changes.
2007-06-05 12:33:37  WARN [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1029) - Filesystem changes found.
2007-06-05 12:33:37  WARN [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:891) - Integrity Check: FAILED
```

OK. Let's check this out.

www.exploitoff.net (Changes)

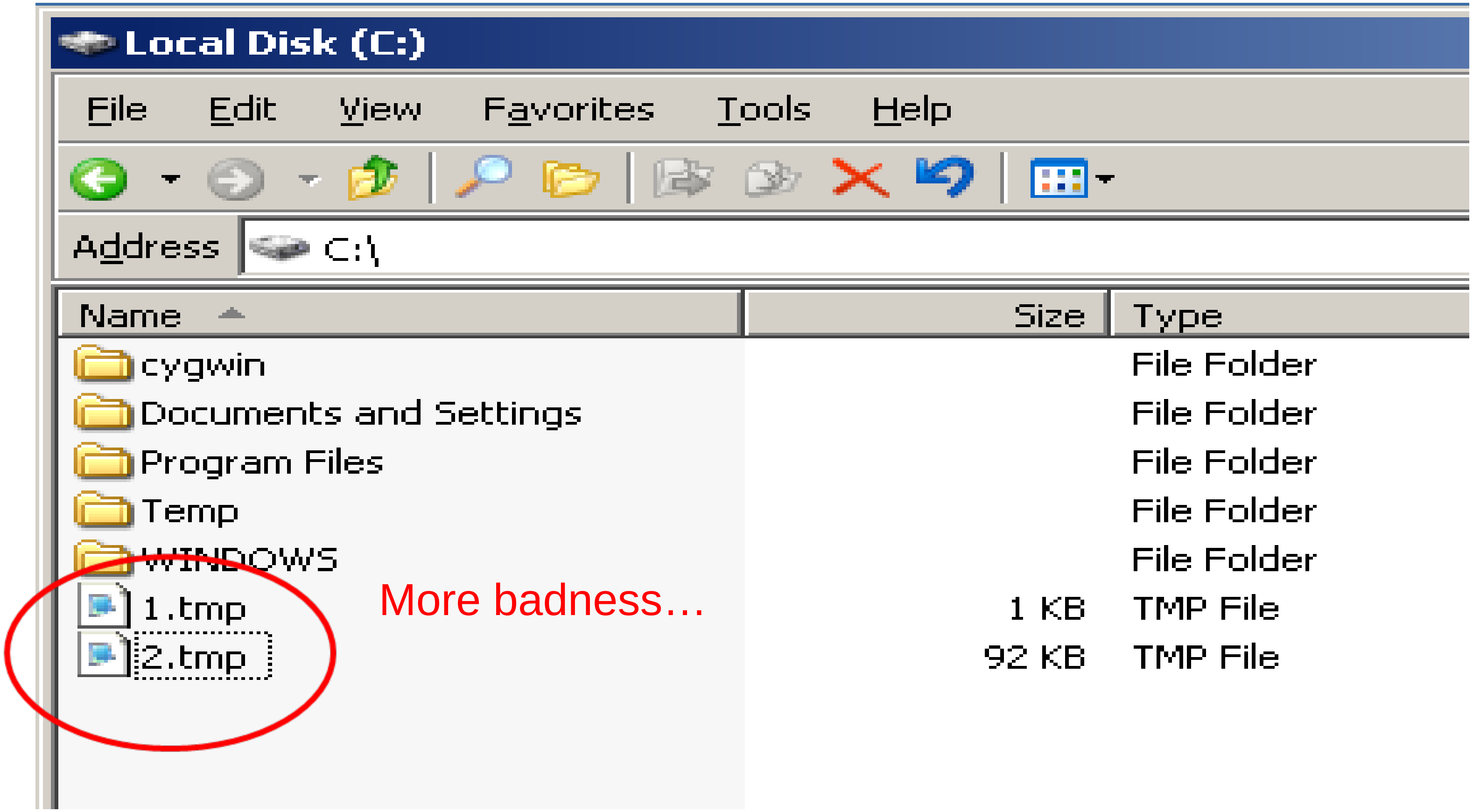


Command Prompt to Tmp - more changes.txt

```
c:\cygwin\tmp>more changes.txt
{
  'filesystem' => [
    {
      'status' => 'changed',
      'new' => {
        'mtime' => 1181061014,
        'name' => '/cygdrive/c',
        'size' => 0
      },
      'old' => {
        'mtime' => 1180037394,
        'name' => '/cygdrive/c',
        'size' => 0
      }
    },
    {
      'status' => 'added',
      'new' => {
        'mtime' => 1181061016,
        'name' => '/cygdrive/c/1.tmp',
        'size' => 6
      }
    },
    {
      'status' => 'added',
      'new' => {
        'mtime' => 1181061017,
```

Definitely not normal…

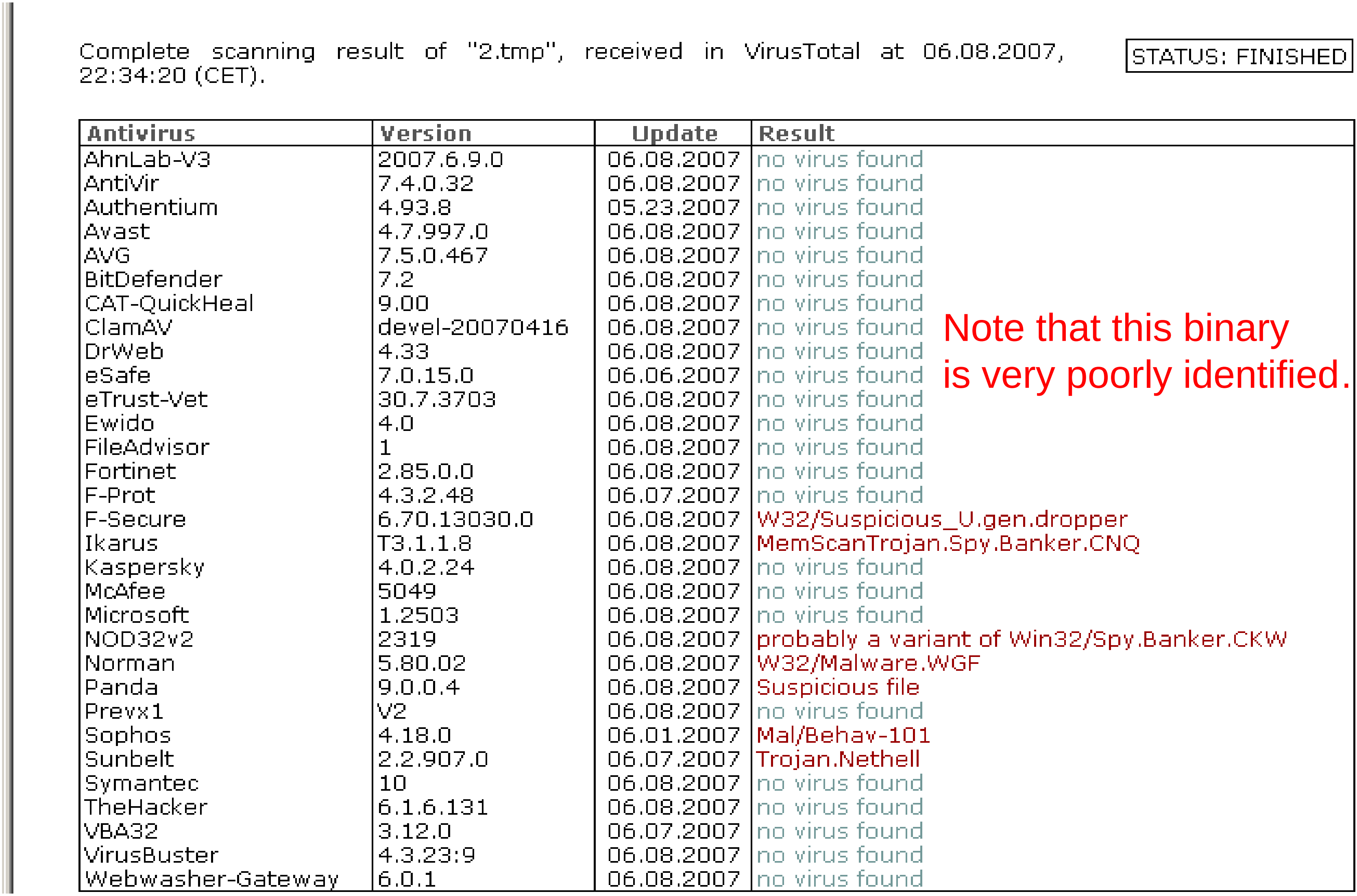
www.exploitoff.net (Changes)



Name	Size	Type
cygwin		File Folder
Documents and Settings		File Folder
Program Files		File Folder
Temp		File Folder
WINDOWS		File Folder
1.tmp	1 KB	TMP File
2.tmp	92 KB	TMP File

More badness…

www.exploitoff.net (Scans)



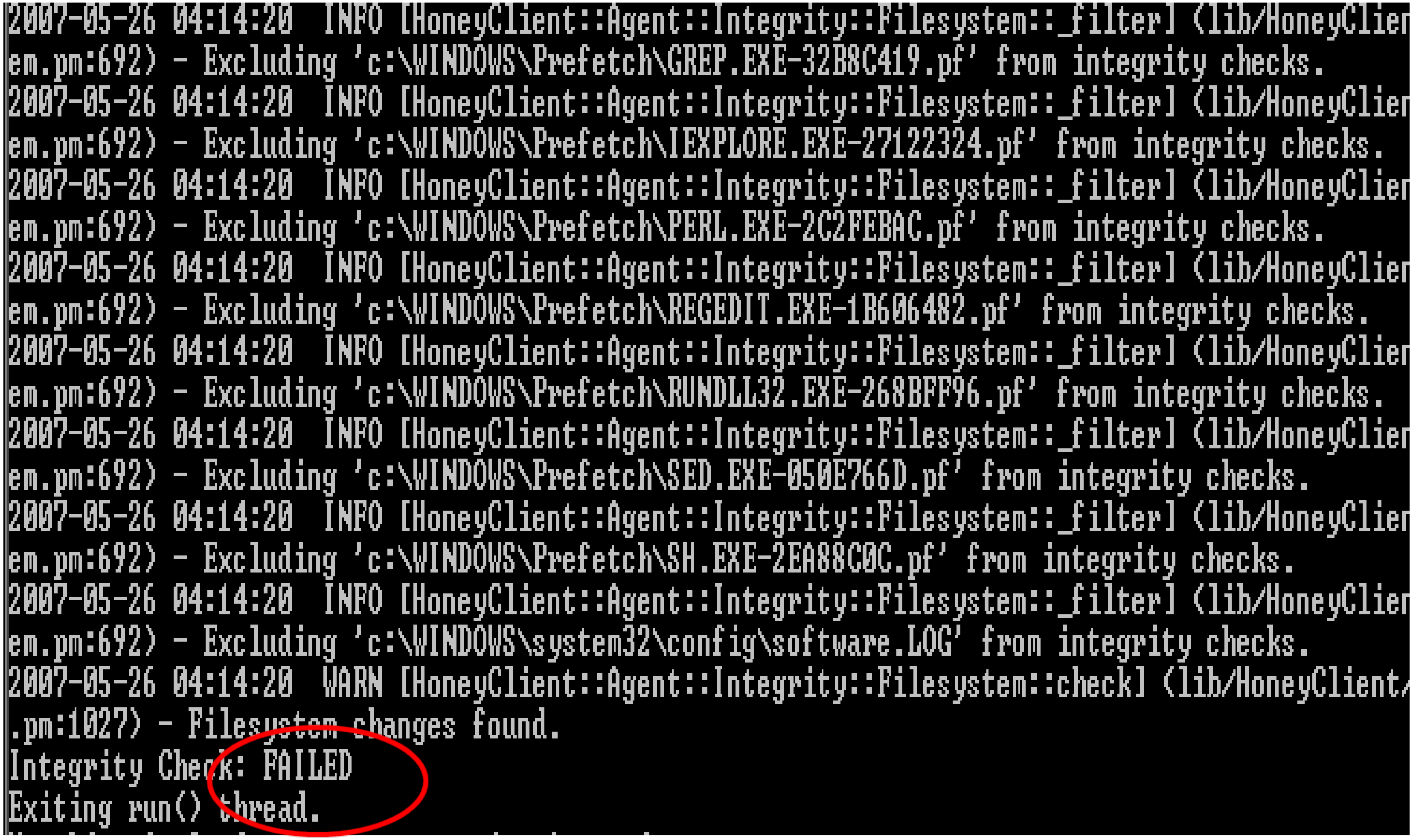
Complete scanning result of "2.tmp", received in VirusTotal at 06.08.2007, 22:34:20 (CET).

STATUS: FINISHED

Antivirus	Version	Update	Result
AhnLab-V3	2007.6.9.0	06.08.2007	no virus found
AntiVir	7.4.0.32	06.08.2007	no virus found
Authentium	4.93.8	05.23.2007	no virus found
Avast	4.7.997.0	06.08.2007	no virus found
AVG	7.5.0.467	06.08.2007	no virus found
BitDefender	7.2	06.08.2007	no virus found
CAT-QuickHeal	9.00	06.08.2007	no virus found
ClamAV	devel-20070416	06.08.2007	no virus found
DrWeb	4.33	06.08.2007	no virus found
eSafe	7.0.15.0	06.06.2007	no virus found
eTrust-Vet	30.7.3703	06.08.2007	no virus found
Ewido	4.0	06.08.2007	no virus found
FileAdvisor	1	06.08.2007	no virus found
Fortinet	2.85.0.0	06.08.2007	no virus found
F-Prot	4.3.2.48	06.07.2007	no virus found
F-Secure	6.70.13030.0	06.08.2007	W32/Suspicious_U.gen.dropper
Ikarus	T3.1.1.8	06.08.2007	MemScanTrojan.Spy.Banker.CNQ
Kaspersky	4.0.2.24	06.08.2007	no virus found
McAfee	5049	06.08.2007	no virus found
Microsoft	1.2503	06.08.2007	no virus found
NOD32v2	2319	06.08.2007	probably a variant of Win32/Spy.Banker.CKW
Norman	5.80.02	06.08.2007	W32/Malware.WGF
Panda	9.0.0.4	06.08.2007	Suspicious file
Prevx1	V2	06.08.2007	no virus found
Sophos	4.18.0	06.01.2007	Mal/Behav-101
Sunbelt	2.2.907.0	06.07.2007	Trojan.Nethell
Symantec	10	06.08.2007	no virus found
TheHacker	6.1.6.131	06.08.2007	no virus found
VBA32	3.12.0	06.07.2007	no virus found
VirusBuster	4.3.23:9	06.08.2007	no virus found
Webwasher-Gateway	6.0.1	06.08.2007	no virus found

Note that this binary is very poorly identified…

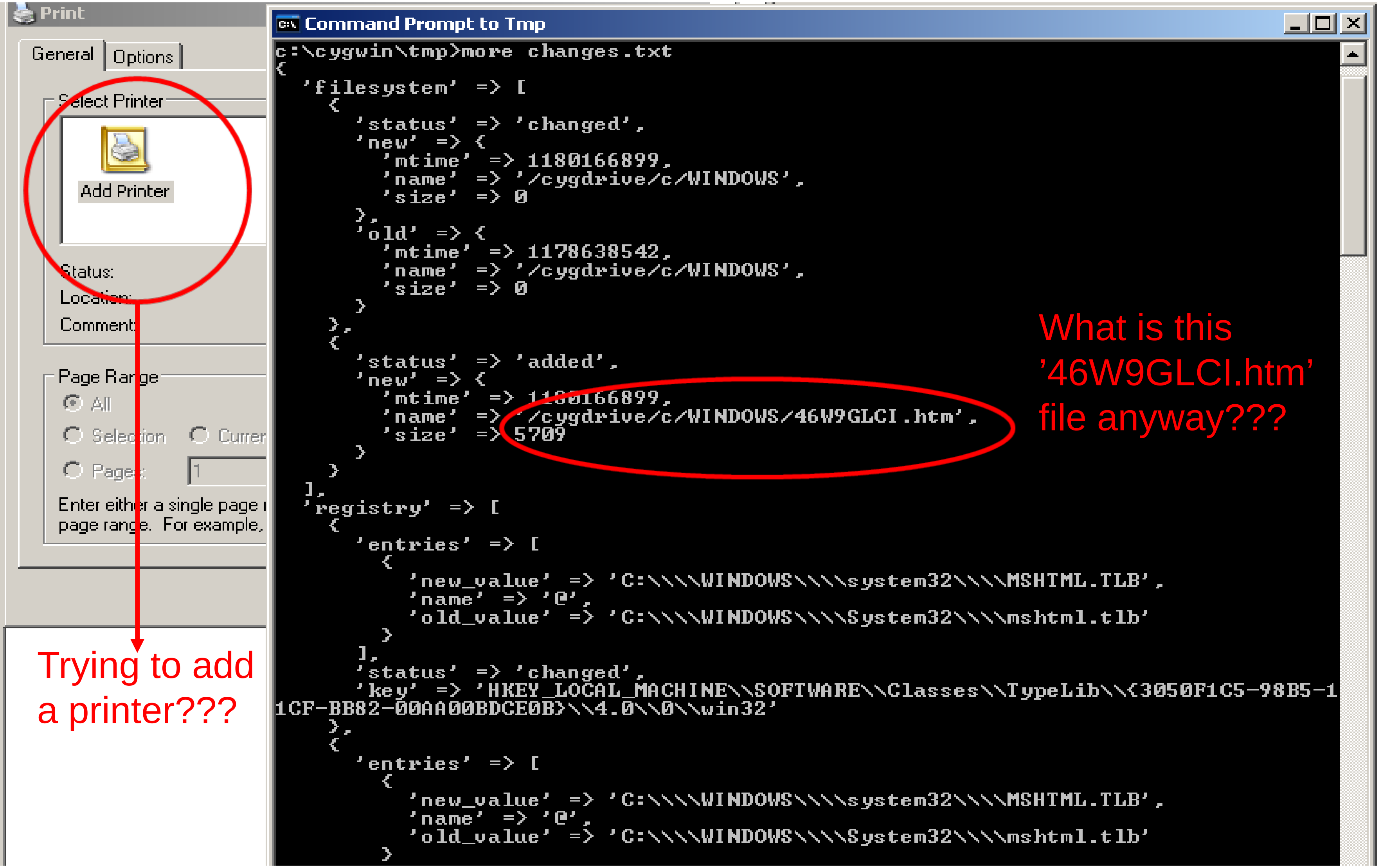
www.haaretz.com (Changes)



```
2007-05-26 04:14:20  INFO [HoneyClient::Agent::Integrity::Filesystem::_filter] (lib/HoneyClien
em.pm:692) - Excluding 'c:\WINDOWS\Prefetch\GREP.EXE-32B8C419.pf' from integrity checks.
2007-05-26 04:14:20  INFO [HoneyClient::Agent::Integrity::Filesystem::_filter] (lib/HoneyClien
em.pm:692) - Excluding 'c:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf' from integrity checks.
2007-05-26 04:14:20  INFO [HoneyClient::Agent::Integrity::Filesystem::_filter] (lib/HoneyClien
em.pm:692) - Excluding 'c:\WINDOWS\Prefetch\PERL.EXE-2C2FEBAC.pf' from integrity checks.
2007-05-26 04:14:20  INFO [HoneyClient::Agent::Integrity::Filesystem::_filter] (lib/HoneyClien
em.pm:692) - Excluding 'c:\WINDOWS\Prefetch\REGEDIT.EXE-1B606482.pf' from integrity checks.
2007-05-26 04:14:20  INFO [HoneyClient::Agent::Integrity::Filesystem::_filter] (lib/HoneyClien
em.pm:692) - Excluding 'c:\WINDOWS\Prefetch\RUNDLL32.EXE-268BFF96.pf' from integrity checks.
2007-05-26 04:14:20  INFO [HoneyClient::Agent::Integrity::Filesystem::_filter] (lib/HoneyClien
em.pm:692) - Excluding 'c:\WINDOWS\Prefetch\SED.EXE-050E766D.pf' from integrity checks.
2007-05-26 04:14:20  INFO [HoneyClient::Agent::Integrity::Filesystem::_filter] (lib/HoneyClien
em.pm:692) - Excluding 'c:\WINDOWS\Prefetch\SH.EXE-2EA88C0C.pf' from integrity checks.
2007-05-26 04:14:20  INFO [HoneyClient::Agent::Integrity::Filesystem::_filter] (lib/HoneyClien
em.pm:692) - Excluding 'c:\WINDOWS\system32\config\software.LOG' from integrity checks.
2007-05-26 04:14:20  WARN [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/
.pm:1027) - Filesystem changes found.
Integrity Check: FAILED
Exiting run() thread.
```

So many bad sites, so little time…

www.haaretz.com (Changes)

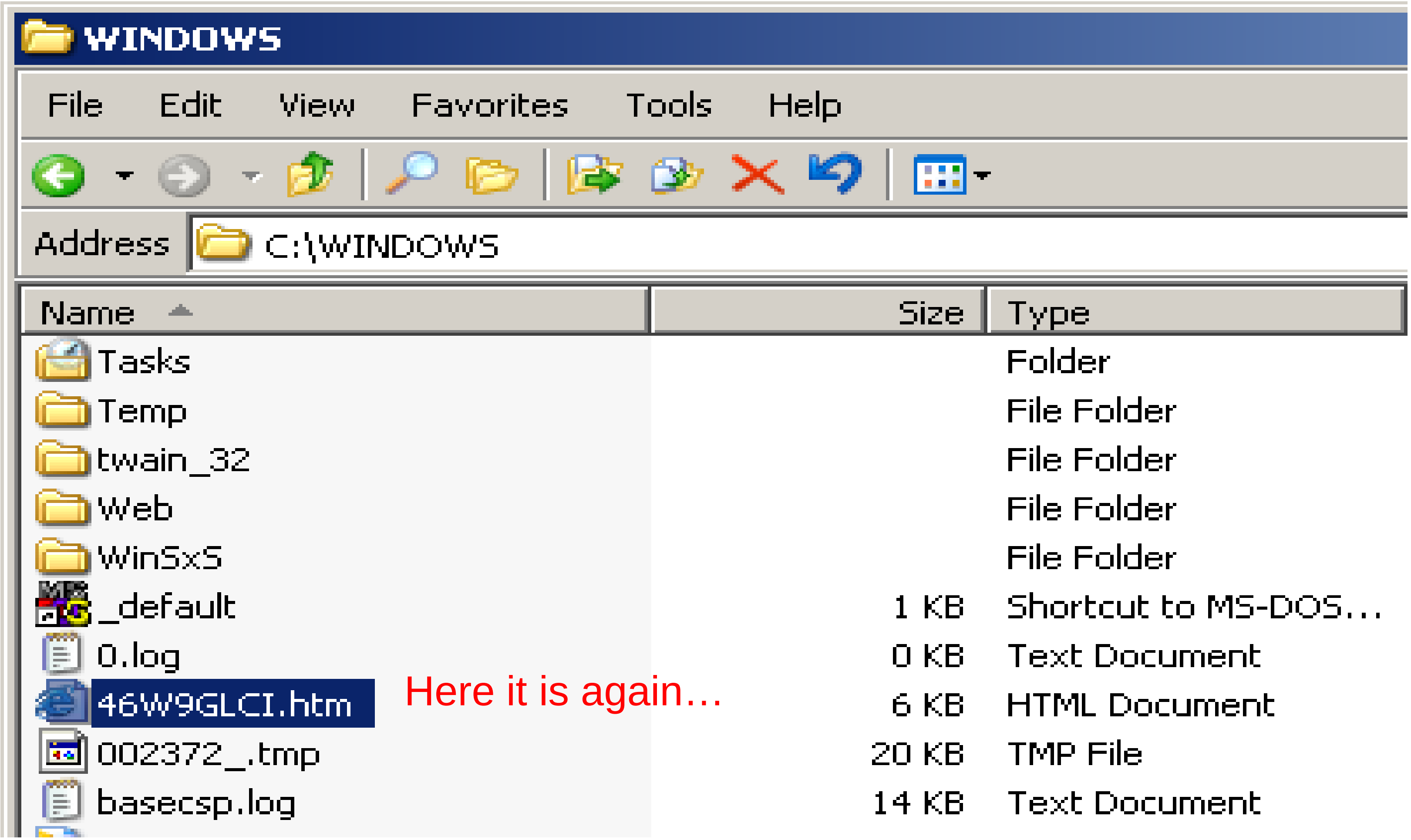


```
c:\cygwin\tmp>more changes.txt
{
  'filesystem' => [
    {
      'status' => 'changed',
      'new' => {
        'mtime' => 1180166899,
        'name' => '/cygdrive/c/WINDOWS',
        'size' => 0
      },
      'old' => {
        'mtime' => 1178638542,
        'name' => '/cygdrive/c/WINDOWS',
        'size' => 0
      }
    },
    {
      'status' => 'added',
      'new' => {
        'mtime' => 1180166899,
        'name' => '/cygdrive/c/WINDOWS/46W9GLCI.htm',
        'size' => 5709
      }
    }
  ],
  'registry' => [
    {
      'entries' => [
        {
          'new_value' => 'C:\\\\WINDOWS\\\\system32\\\\MSHTML.TLB',
          'name' => '@',
          'old_value' => 'C:\\\\WINDOWS\\\\System32\\\\mshtml.tlb'
        }
      ],
      'status' => 'changed',
      'key' => 'HKEY_LOCAL_MACHINE\\SOFTWARE\\Classes\\TypeLib\\{3050F1C5-98B5-1
1CF-BB82-00AA00BDCE0B}\\4.0\\0\\win32'
    },
    {
      'entries' => [
        {
          'new_value' => 'C:\\\\WINDOWS\\\\system32\\\\MSHTML.TLB',
          'name' => '@',
          'old_value' => 'C:\\\\WINDOWS\\\\System32\\\\mshtml.tlb'
        }
```

What is this '46W9GLCI.htm' file anyway???

Trying to add a printer???

www.haaretz.com (Changes)

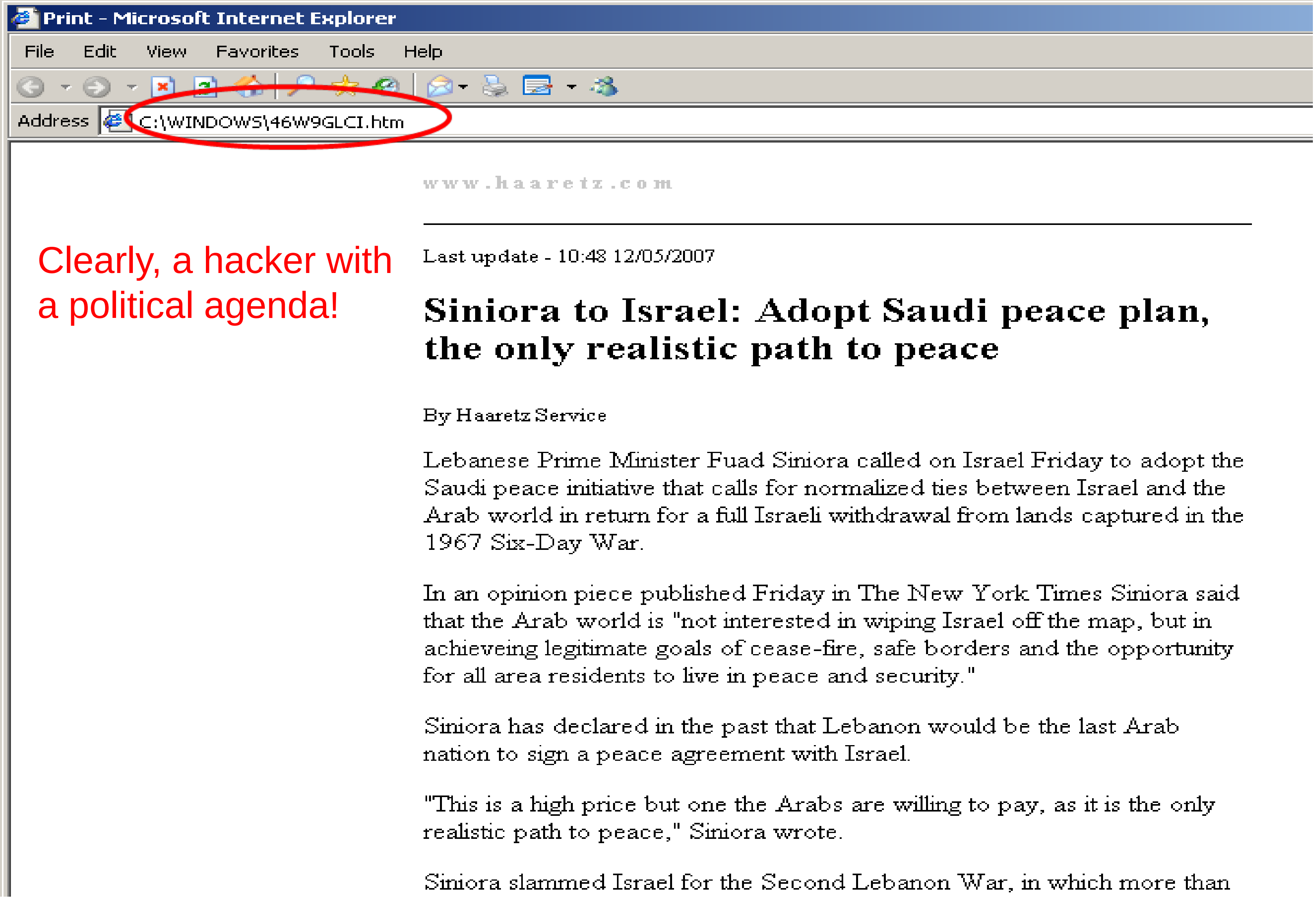


Address C:\WINDOWS

Name	Size	Type
Tasks		Folder
Temp		File Folder
twain_32		File Folder
Web		File Folder
WinSxS		File Folder
_default	1 KB	Shortcut to MS-DOS…
0.log	0 KB	Text Document
46W9GLCI.htm	6 KB	HTML Document
002372_.tmp	20 KB	TMP File
basecsp.log	14 KB	Text Document

Here it is again…

www.haaretz.com



Print - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
C:\WINDOWS\46W9GLCI.htm

www.haaretz.com

Last update - 10:48 12/05/2007

Siniora to Israel: Adopt Saudi peace plan, the only realistic path to peace

By Haaretz Service

Lebanese Prime Minister Fuad Siniora called on Israel Friday to adopt the Saudi peace initiative that calls for normalized ties between Israel and the Arab world in return for a full Israeli withdrawal from lands captured in the 1967 Six-Day War.

In an opinion piece published Friday in The New York Times Siniora said that the Arab world is "not interested in wiping Israel off the map, but in achieveing legitimate goals of cease-fire, safe borders and the opportunity for all area residents to live in peace and security."

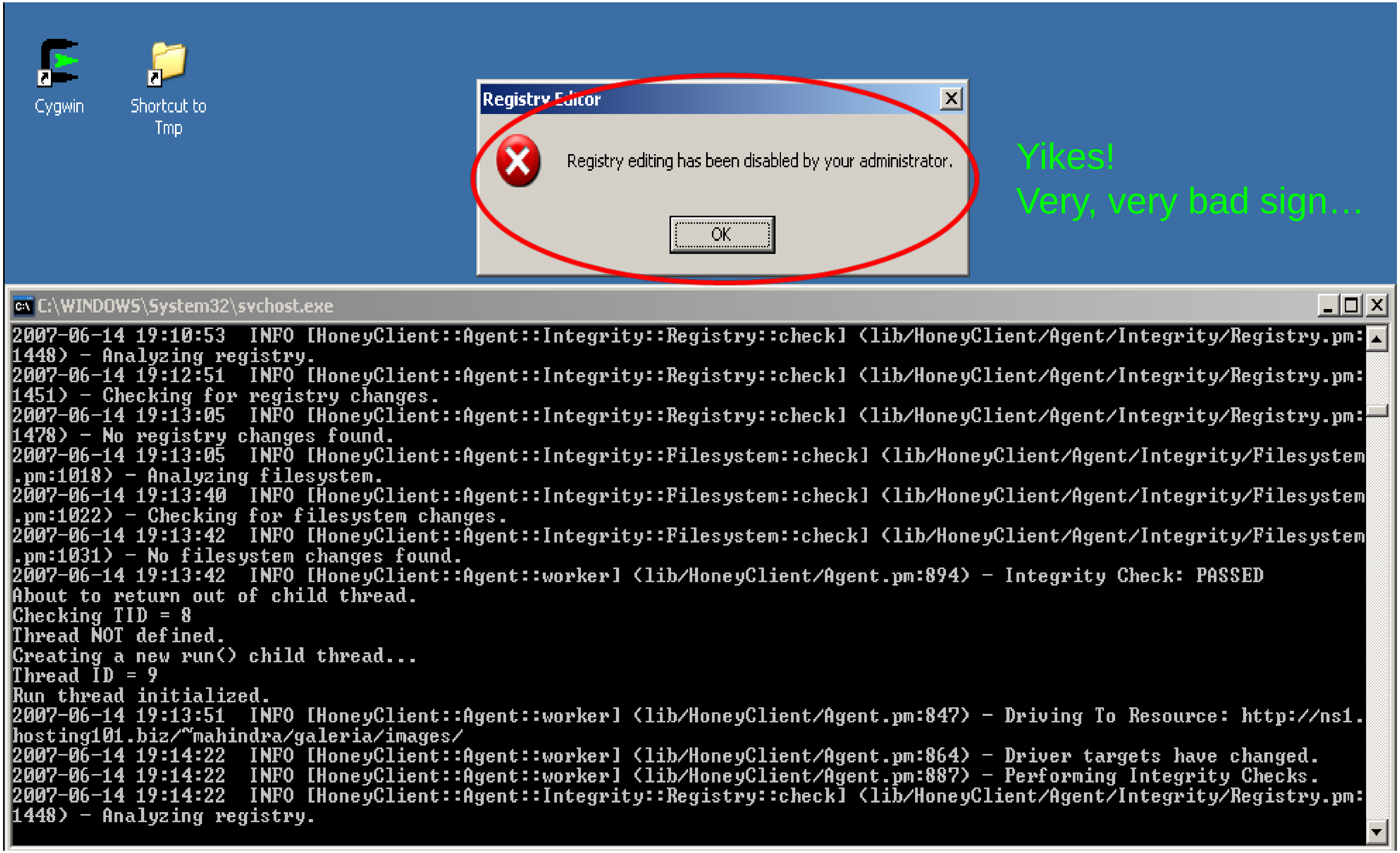
Siniora has declared in the past that Lebanon would be the last Arab nation to sign a peace agreement with Israel.

"This is a high price but one the Arabs are willing to pay, as it is the only realistic path to peace," Siniora wrote.

Siniora slammed Israel for the Second Lebanon War, in which more than

Clearly, a hacker with a political agenda!

ns1.hosting101.biz



Registry editing has been disabled by your administrator.

Yikes!
Very, very bad sign…

```
2007-06-14 19:10:53  INFO [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1448) - Analyzing registry.
2007-06-14 19:12:51  INFO [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1451) - Checking for registry changes.
2007-06-14 19:13:05  INFO [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1478) - No registry changes found.
2007-06-14 19:13:05  INFO [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1018) - Analyzing filesystem.
2007-06-14 19:13:40  INFO [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1022) - Checking for filesystem changes.
2007-06-14 19:13:42  INFO [HoneyClient::Agent::Integrity::Filesystem::check] (lib/HoneyClient/Agent/Integrity/Filesystem
.pm:1031) - No filesystem changes found.
2007-06-14 19:13:42  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:894) - Integrity Check: PASSED
About to return out of child thread.
Checking TID = 8
Thread NOT defined.
Creating a new run() child thread...
Thread ID = 9
Run thread initialized.
2007-06-14 19:13:51  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:847) - Driving To Resource: http://ns1.
hosting101.biz/~mahindra/galeria/images/
2007-06-14 19:14:22  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:864) - Driver targets have changed.
2007-06-14 19:14:22  INFO [HoneyClient::Agent::worker] (lib/HoneyClient/Agent.pm:887) - Performing Integrity Checks.
2007-06-14 19:14:22  INFO [HoneyClient::Agent::Integrity::Registry::check] (lib/HoneyClient/Agent/Integrity/Registry.pm:
1448) - Analyzing registry.
```