CIS 2011 vs. NIS 2011 vs. unknown malware

November 2, 2010

Summary: In the comparative test focused mainly on ability to prevent system infection Comodo Internet Security 2011 received 97 points and Norton Internet Security received 42 points out of 100 total points.

Introduction

Our task was to make a comparison of how are Comodo Internet Security 2011 (CIS) and Norton Internet Security 2011 (NIS) effective against unknown malware. We were asked to find 20 malware samples detected neither by CIS's anti-virus engine, nor by the anti-virus engine of NIS. Both CIS and NIS implement security features that should protect users from malicious attacks performed by locally executed malware even if it is not yet included in their anti-virus databases. The primary evaluation criterion of the products' efficiency in fighting unknown malware was whether or not the malware was able to infect the system so that it persisted in the system after the reboot. Secondary criteria were whether the system was damaged or some important changes to the system settings were made by the actions of malware, and whether any information leaked from the tested machine to a malicious server on the Internet.

This report is delivered with the archive of all the used malware samples. The archive is protected with password "infected".

Methodology

The research was done on virtual machines running 32-bit Windows 7 Professional. Internet Explorer 8, Windows Live Messenger 2009, Windows Live Mail 2009, and Total Commander 7.55a were installed on all testing machines. User accounts on eBay, PayPal, Windows Live, and FTPWT were created for this research. Internet Explorer was set to remember username and password for eBay account, Windows Live Messenger was set to automatically log in to the network when the system starts, Windows Live Mail was set to remember username and password for both email servers (POP3 and SMTP), and Total Commander was set to remember the complete login information for FTP access on FTPWT. The Windows User Account Control was disabled on all testing machines.

Fully updated Comodo Internet Security PREMIUM 2011 5.0.162636.1135 and Norton Internet Security 2011 18.1.0.37 were used for this research. These versions were the latest stable releases of the tested products available when the research started.

The whole process started with collecting of the malware samples. We collected more than a thousand of malware samples in order to find 20 samples not detected by anti-virus engines of the tested products. The samples were not run in this phase, they were scanned as raw files. Having the set of unknown malware ready for the tests, we had to make sure that during the testing process no new virus signatures affect our testing. This is why we had to disable anti-virus updates of both CIS and NIS and also to turn of their cloud-based detection technologies – this means that the samples and/or their characteristics were not submitted for analysis on the updated Internet servers of the products' vendors. The used malware samples were not detected by anti-virus engines when the testing process started. They may be detected now, however.

Configuration of CIS

In order to get the best from CIS, we have changed its configuration profile to COMODO – Proactive Security. In order to prevent issues with new virus signatures, Automatic updates were disabled on several places in the CIS's configuration. Also Automatically scan unrecognized files in the cloud option of Defense+'s Execution Control Settings was disabled. All other settings were set to their default values including the configuration of CIS's Sandbox functionality, which is enabled by default. This particular setting, which was a part of the task's assignment, heavily reduces the number of alerts that CIS displays due to a number of automatic rules implemented in the sandbox.

Configuration of NIS

In order to get best from NIS, we had to enable Advanced Events Monitoring feature. This is possible after turning off the Automatic Program Control in the Advanced Settings of NIS's Smart Firewall. In this configuration NIS is able to block more malicious attacks. In order to prevent issues with new virus signatures, Insight Protection, SONAR Protection, and Automatic Live Update were turned off. All other settings were set to their default values.

Testing procedure

All malware samples were run on three machines – the unprotected machine without any security product installed, the machine with CIS installed, and the machine with NIS installed. Every malware had its own set of these machines and hence it was not possible for any machine to be influenced by more than one malware. The following procedure was performed with every malware machine:

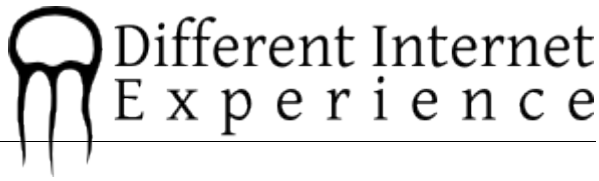
1) The machine was switched on.
2) The system started and the user logged in. Windows Live Messenger automatically started.
3) Internet Explorer was started manually.
4) The malware sample was copied to the machine and started by Windows Explorer.
5) The user browsed the Internet with the Internet Explorer during which he logged in PayPal and eBay accounts.
6) The user checked for the emails in its Windows Live email accounts.
7) The user logged out and in again in Windows Live Messenger.
8) The FTP account on FTPWT was accessed using Total Commander.
9) After a short pause the machine was rebooted and steps 2) – 8) were repeated once again. The machine was then switched off.

In case of an alert from the operating system or the security software the action in question was always blocked regardless the accuracy of its description.

Getting the results

There were four output channels from every machine – file system modifications, registry modifications, network traffic and the human tester's observations. The file system modifications were obtained from snapshots of hard disks of the unprotected machine, on which no malware was executed, and the testing machine, which hard drive state was saved just after completing the testing procedure. The registry modifications were obtained from snapshots of registry hive files of the unprotected machine and the testing machine. The hive files were extracted from the hard drive snapshots. The network traffic was obtained from a network sniffer that was started prior every testing procedure to capture the packets originated from the tested machine. The human tester's observations provided additional information and supported the other outputs.

Based on the data collected from the mentioned outputs on the machines without security products installed, we have determined key signs of each malware infection. Then using the data from the other machines we have evaluated how were CIS and NIS effective against each malware.



Each sample was also submitted to Virustotal service, report links are included in the results.

Scoring

For each malware sample, the security product's ability to protect the system against persistent infection was rewarded with 3 points. If the product prevented damaging the system and changing important system settings, it received 1 point. Finally, the product received 1 point if no information leaked from the tested machine to a malicious Internet server. The number of malware samples was 20 and hence the maximum number of points that a product could receive was 100.

Detailed results

Malware Sample.01

VirusTotal report: 1288268993

Unprotected machine results

File system modifications

None.

Registry modifications

- Malware registered itself under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.
- Malware changed Internet Explorer's Post Platform part of User Agent.

Network traffic

- Malware attempted to connect to Internet server mssql.sqlsrvblade.kinghost.net on port 1039/TCP.

Additional information

None.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to access the protected COM interface Shell.Explorer.2.
- Malware crashed.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

None.

Registry modifications

- Malware registered itself under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.
- Malware changed Internet Explorer's Post Platform part of User Agent.

Network traffic

None.

Additional information

- NIS alerted about malware's attempt to access the Internet.

Score

2 points:

- Malware was started after the reboot.
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

Malware Sample.02

VirusTotal report: 1288271800

Unprotected machine results

File system modifications

- Malware deleted its own executable.
- Malware created ".info" file in the temporary directory. This file contained a brief system information.
- Malware modified the system HOSTS file in order to redirect Internet traffic to various domains, including www.americanexpress.com.br and www.santander.com.br, to a phishing server.

Registry modifications

None.

Network traffic

- Malware attempted to send ".info" file contents to web server nowinf.sitebr.net.

Additional information

None.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about malware's access to the Internet.
- Malware reported file access error.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

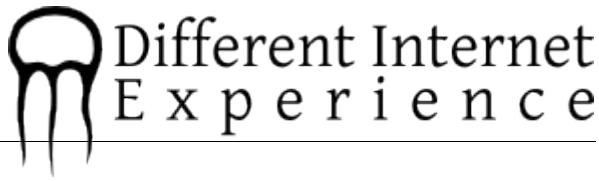
NIS results

File system modifications

- BAT script intended to delete the malware's executable and itself was created in the malware's working directory.
- Malware created ".info" file in the temporary directory. This file contained a brief system information.
- Malware modified the system HOSTS file in order to redirect Internet traffic to various domains, including www.americanexpress.com.br and www.santander.com.br, to a phishing server.

Registry modifications

None.



Network traffic

None.

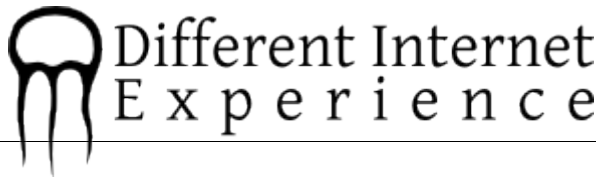
Additional information

- NIS alerted about malware's attempt to access the Internet.
- NIS alerted about malware's attempt to execute the self-erasing BAT script.

Score

2 points:

- System HOSTS file was changed, user's traffic was redirected to malicious server.
- No important system settings were changed. (1 point)
- No information leaked. (1 point)



Malware Sample.03

VirusTotal report: 1288276079

Unprotected machine results

File system modifications

- Malware created new file in the user's profile directory – "winlogon.exe".
- Malware modified the system HOSTS file in order to redirect Internet traffic to various domains, including bn.com.pe, to a phishing server, and it redirected many domains of security companies, including ahnlab.com, comodo.com, f-secure.com, kaspersky.com, mcafee.com, microsoft.com, to its own server.

Registry modifications

- Malware registered the new "winlogon.exe" under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.
- Malware changed various URLs in Internet Explorer's configuration such as its StartPage, DefaultPage, LocalPage.
- Malware changed various system settings in order to disable system restore and UAC notifications.
- In order to prevent various security products from running, malware changed debugger settings for many executable names such as "avp.exe", "bullguard.exe", "drweb32.exe".

Network traffic

- Malware communicated heavily with cheaps1.info web server.
- Network traffic related to the changed Internet Explorer's start page was captured.

Additional information

- Prior the first reboot applications in the system including Internet Explorer and Total Commander crashed randomly.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

None.

Score

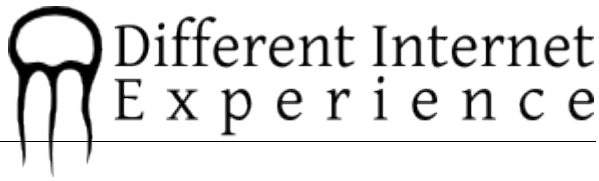
5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

- Malware created new file in the user's profile directory – "winlogon.exe".
- Malware modified the system HOSTS file in order to redirect Internet traffic to various domains, including



bn.com.pe, to a phishing server, and it redirected many domains of security companies, including ahnlab.com, comodo.com, f-secure.com, kaspersky.com, mcafee.com, microsoft.com, to its own server.

Registry modifications

- Malware registered the new "winlogon.exe" under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.
- Malware changed various URLs in Internet Explorer's configuration such as its StartPage, DefaultPage, LocalPage.
- Malware changed various system settings in order to disable system restore and UAC notifications.
- In order to prevent various security products from running, malware changed debugger settings for many executable names such as "avp.exe", "bullguard.exe", "drweb32.exe".

Network traffic

- Network traffic related to the changed Internet Explorer's start page was captured.

Additional information

- NIS alerted about malware's attempt to access the Internet.
- NIS alerted about malware's attempt to access the Internet using a newly created system process "svchost.exe".
- Prior the first reboot applications in the system including Internet Explorer and Total Commander crashed randomly.

Score

1 point:

- Malware was started after the reboot. System HOSTS file was changed, user's traffic was redirected to malicious server.
- Malware changed important URLs in Internet Explorer's settings. Malware changed settings related to UAC and installed itself as a debugger for various executable names.
- No information leaked. (1 point)

Malware Sample.04

VirusTotal report: 1288278555

Unprotected machine results

File system modifications

- Malware copied its executable to Windows directory as “win2.exe”.

Registry modifications

- Malware registered “win2.exe” under “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.

Network traffic

- Malware attempted to connect to web server ccanlitv.com.

Additional information

None.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

None.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

- Malware copied its executable to Windows directory as “win2.exe”.

Registry modifications

- Malware registered “win2.exe” under “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.

Network traffic

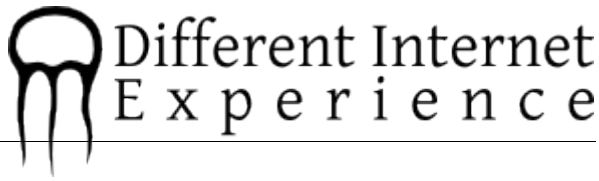
None.

Additional information

- NIS alerted about malware's attempt to access the Internet.

Score

2 points:



- Malware was started after the reboot.
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

Malware Sample.05

VirusTotal report: 1288279328

Unprotected machine results

File system modifications

- Malware created new files in Windows directory – e.g. "GettingStarrted.exe", "psisdeecd.dll".
- Malware registered new Task Scheduler jobs, for which "At1.job" and "At2.job" files were created in "Windows\Tasks" and "At1" and "At2" files in "Windows\System32\Tasks" directory.
- Malware deleted its own executable.

Registry modifications

- Malware registered "psisdeecd.dll" as Browser Helper Object.
- Registry entries related to the new Task Scheduler jobs were created.

Network traffic

None.

Additional information

- The first job was created in order to run malware repeatedly. The second job was created in order to run a BAT script that deleted the original malware executable and itself.

CIS results

File system modifications

- Malware registered new Task Scheduler job, for which "At1.job" file was created in "Windows\Tasks" and "At1" file in "Windows\System32\Tasks" directory.

Registry modifications

- Registry entries related to the new Task Scheduler job were created.

Network traffic

None.

Additional information

- The created job was the one which role was to delete the original executable. The second job was not created.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

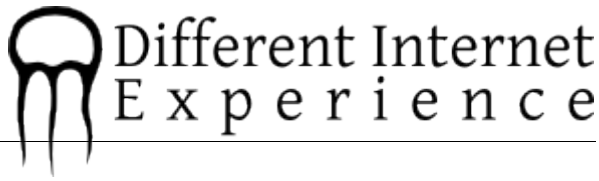
- Malware created new files in Windows directory – e.g. "cipherr.exe", "DevicePPairing.dll".

Registry modifications

- Malware registered "DevicePPairing.dll" as Browser Helper Object.

Network traffic

None.



Additional information

- NIS alerted about malware's attempt to execute the system “at” command.
- NIS alerted about Internet Explorer's attempt to access the Internet using the unrecognized module “DevicePPairing.dll”.

Score

2 points:

- Malware DLL was installed in the system as Browser Helper Object.
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

Malware Sample.06

VirusTotal report: 1288279356

Unprotected machine results

File system modifications

- Malware copied its executable to the user's application data folder as “hotfix.exe”.
- BAT script intended to delete the malware's executable was created in the user's application data folder.
- Malware deleted its own executable.

Registry modifications

- Malware registered “hotfix.exe” in “Shell” value under “HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon” in order to persist in the system.
- Malware disabled various Internet Explorer's warnings such as WarnonBadCertRecving, WarnOnPost, WarnOnPostRedirect.

Network traffic

- Malware sent a single request to web server on address 85.234.191.174.

Additional information

- Malware displayed a fake Microsoft Security Essentials Alert in order to manipulate the user to install additional malware.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to access the protected COM interface Shell.Explorer.2.
- Malware crashed.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

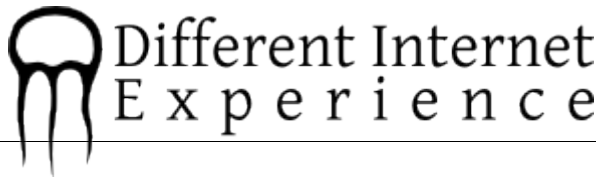
NIS results

File system modifications

- Malware copied its executable to the user's application data folder as “hotfix.exe”.
- BAT script intended to delete the malware's executable was created in the user's application data folder.

Registry modifications

- Malware registered “hotfix.exe” in “Shell” value under “HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon” in order to persist in the system.
- Malware disabled various Internet Explorer's warnings such as WarnonBadCertRecving, WarnOnPost,



WarnOnPostRedirect.

Network traffic

None.

Additional information

- Malware displayed a fake Microsoft Security Essentials Alert in order to manipulate the user to install additional malware.
- NIS alerted about malware's attempt to access the Internet.
- NIS alerted about malware's attempt to execute the self-erasing BAT script.
- NIS alerted about malware's attempt to perform keylogging activity.
- NIS alerted about malware's attempt to inject code in its own process.

Score

1 point:

- Malware was started after the reboot.
- Malware disabled various Internet Explorer's warnings.
- No information leaked. (1 point)

Malware Sample.07

VirusTotal report: 1288279375

Unprotected machine results

File system modifications

- Malware created "cleansweep.exe" directory in the system drive's root directory and created new files in this directory – "cleansweep.exe", "config.bin".

Registry modifications

- Malware registered "cleansweep.exe" under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.
- Malware disabled various Internet Explorer's warnings such as WarnonBadCertRecving, WarnOnPost, WarnOnPostRedirect and changed other settings of Internet Explorer in order to decrease its security.

Network traffic

- Malware sent information about the system and user to web server on address 204.12.237.196 and bubblegum2010.com.
- Malware downloaded files from web server on address 204.12.237.196.

Additional information

None.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

None.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- NIS alerted about malware's attempt to inject code into Windows Explorer.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

Malware Sample.08

VirusTotal report: 1288279402

Unprotected machine results

File system modifications

- Malware infected system file “wininit.exe” in the system directory and “explorer.exe” file in the Windows directory in order to persist in the system.
- Malware created “Server” directory under the user's Documents folder and stored couple of its files in it.

Registry modifications

- Malware set registry value “FirstRun” under “HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\sr\Parameters”. Same value was set under “HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\sr\Parameters”.

Network traffic

- Malware sent information about the system to web server nanocloudcontroller.com.

Additional information

None.

CIS results

File system modifications

- Malware created “Server” directory under the user's Documents folder and stored couple of its files in it.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to gain unlimited access to the computer.
- CIS alerted about malware's attempt to access Windows Print Spooler Service interface.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

- Malware infected system file “wininit.exe” in the system directory in order to persist in the system.
- “explorer.exe” file in the Windows directory was deleted.
- Malware created “Server” directory under the user's Documents folder and stored couple of its files in it.

Registry modifications

None.

Network traffic

None.

Additional information

- NIS displayed information about blocked security risks identified as “Trojan.Gen” and “Suspicious.Mystic”.
- NIS displayed information about removed security risk identified as “Suspicious.Mystic”.

Score

1 point:

- Infected “wininit.exe” started after the reboot.
- “explorer.exe” was deleted.
- No information leaked. (1 point)

Malware Sample.09

VirusTotal report: 1288279438

Unprotected machine results

File system modifications

- Malware copied its executable to Windows directory as “nvsvc32.exe”.

Registry modifications

- Malware registered “nvsvc32.exe” under “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.
- Malware registered “nvsvc32.exe” under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.
- Malware registered “nvsvc32.exe” under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.
- Malware added “nvsvc32.exe” to the list of authorized applications of Windows firewall.
- Malware changed Internet Explorer's start page to “http://redirecturls.info”.

Network traffic

- Malware communicated with various web servers.
- Network traffic related to the changed Internet Explorer's start page was captured.

Additional information

None.

CIS results

File system modifications

- Malware copied its executable to the Public folder as “nvsvc32.exe”.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to access the Internet.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

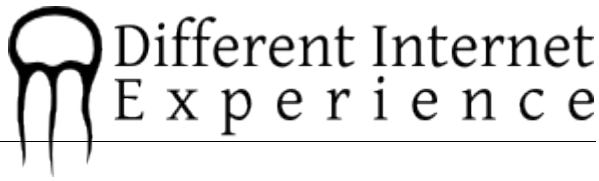
NIS results

File system modifications

- Malware copied its executable to Windows directory as “nvsvc32.exe”.

Registry modifications

- Malware registered “nvsvc32.exe” under “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.
- Malware registered “nvsvc32.exe” under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\



CurrentVersion\Run" in order to persist in the system.

- Malware registered "nvsvc32.exe" under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.
- Malware added "nvsvc32.exe" to the list of authorized applications of Windows firewall.
- Malware changed Internet Explorer's start page to "http://redirecturls.info".

Network traffic

- Network traffic related to the changed Internet Explorer's start page was captured.

Additional information

- NIS alerted about malware's attempt to access the Internet.

Score

1 point:

- Malware was started after the reboot.
- Malware changed Internet Explorer's start page.
- No information leaked. (1 point)

Malware Sample.10

VirusTotal report: 1288279467

Unprotected machine results

File system modifications

- Malware created new files in the user's local application data directory – e.g. "lsasss32.exe", "winload.inf", copy of its main executable.
- Malware created "fuckingList" file under the user's profile directory. This file contained Windows Live account user name.

Registry modifications

- Malware stored its settings under "HKEY_LOCAL_MACHINE\Software\Licenses".
- Malware registered "lsasss32.exe" under "HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run" in order to persist in the system.

Network traffic

- Malware downloaded an executable file from web server dc222.4shared.com.
- Malware communicated with various web servers including mygamelink.com.

Additional information

None.

CIS results

File system modifications

None.

Registry modifications

- Malware stored its settings under "HKEY_LOCAL_MACHINE\Software\Licenses".

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to access the protected COM interface of system process "svchost.exe".

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

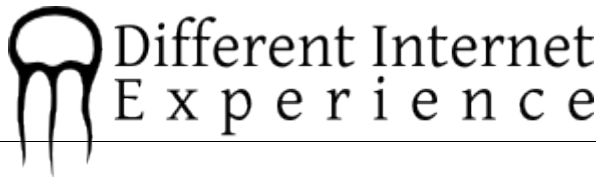
None.

Registry modifications

None.

Network traffic

None.



Additional information

- NIS alerted about malware's attempt to inject code in its own process.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

Malware Sample.11

VirusTotal report: 1288341181

Unprotected machine results

File system modifications

- Malware created new file in the user's local application data directory – "Dend1der.dll".

Registry modifications

- Malware stored its settings under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Rqixaripecilu".
- Malware registered system program "rundll32.exe" with a full path to "Dend1der.dll" as an argument under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.

Network traffic

- Malware resolved domain name "0000782240.4413c3da.01.CB2C6193464E46669575B4663078CEF7.n.empty.1355.empty.6_1._t_i.3000.explorer_exe.168.rc2.a4h9uploading.com".
- Malware attempted to communicate with web server 151907da1028.aginder.net.

Additional information

None.

CIS results

File system modifications

- Malware created new file in the user's local application data directory – "TPHMWm.dll".

Registry modifications

- Malware stored its settings under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Rqixaripecilu".

Network traffic

- Malware resolved domain name "0001292640.4413c3da.02.2A00E2BD908B4601B66B50BA026992F3.n.empty.1355.empty.6_1._t_i.3000.explorer_exe.168.rc2.a4h9uploading.com".

Additional information

- CIS alerted about malware's attempt to install global hook handled by "TPHMWm.dll".

Score

4 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- DNS query carrying data about the system was sent to Internet server.

NIS results

File system modifications

- Malware created new file in the user's local application data directory – "KBHEatL.dll".

Registry modifications

- Malware stored its settings under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Rqixaripecilu".
- Malware registered system program "rundll32.exe" with a full path to "KBHEatL.dll" as an argument under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.

Network traffic

None.

Additional information

- NIS alerted about malware's attempt to access the Internet.
- NIS alerted about Windows Explorer's, Internet Explorer's, Windows Live Messenger's, and Total Commander's attempt to access the Internet using unrecognized module "KBHEatL.dll". Blocking these attempts caused that the infected applications were no longer able to access the Internet.

Score

1 point:

- Malware was started after the reboot.
- Malware infected processes in the system with its DLL.
- No information leaked. (1 point)

Malware Sample.12

VirusTotal report: 1288341195

Unprotected machine results

File system modifications

- Malware created new file in the user's local application data directory – "91792.exe".
- Malware created link to "91792.exe" called "Security Tool.lnk" in the user's start menu folder.
- Malware deleted its own executable.

Registry modifications

- Malware registered "91792.exe" under "HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce" in order to persist in the system.

Network traffic

- Malware communicated with web server casualpayments.com.

Additional information

- Malware displayed GUI of fake security software called "SecurityTool", which performed a fake scan that found number of infections in the computer.
- Malware displayed various alerts in order to make the user believe the computer is heavily infected and make them buy and activate the fake security software.
- Malware blocked starting non-critical applications on the computer including Total Commander claiming the applications are infected.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

None.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

- BAT script intended to delete the malware's executable and itself was created in the user's temporary directory.
- Malware created new file in the user's local application data directory – "796956132.exe".
- Malware created link to "796956132.exe" called "Security Tool.lnk" in the user's start menu folder.

Registry modifications

- Malware registered "796956132.exe" under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce" in order to persist in the system.

Network traffic

None.

Additional information

- NIS alerted about malware's attempt to execute the self-erasing BAT script.
- After the reboot the malware GUI was frozen due to NIS's alert that was displayed under the GUI window.
- Malware blocked starting non-critical applications on the computer including Total Commander claiming the applications are infected.

Score

1 point:

- Malware was started after the reboot.
- Malware blocked starting applications.
- No information leaked. (1 point)

Malware Sample.13

VirusTotal report: 1288341192

Unprotected machine results

File system modifications

- Malware created new directory in the user's local application data directory – "Bitrix Security". This directory contained various files including "nlqocq.dll".
- Malware deleted its own executable.

Registry modifications

- Malware registered system program "rundll32.exe" with a full path to "nlqocq.dll" as an argument under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.
- Malware disabled pop-up blocker, phishing filter and ActiveX warnings in Internet Explorer's settings.
- Malware stored its settings under "HKEY_CURRENT_USER\Software\Microsoft\Essentials".

Network traffic

- Malware communicated with web server ronderboook.com.

Additional information

None.

CIS results

File system modifications

- Malware created new directory in the user's local application data directory – "Bitrix Security". This directory contained various files including "nlqocq.dll".

Registry modifications

- Malware stored its settings under "HKEY_CURRENT_USER\Software\Microsoft\Essentials".
- Malware disabled pop-up blocker, phishing filter and ActiveX warnings in Internet Explorer's settings.

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to access protected COM interface.

Score

4 points:

- No infection persisted in the system. (3 points)
- Malware changed Internet Explorer's settings and decreased its security.
- No information leaked. (1 point)

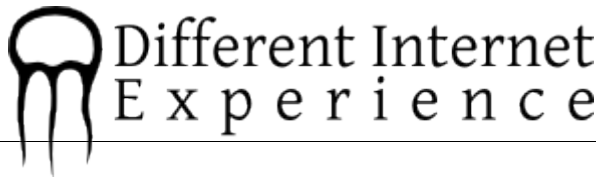
NIS results

File system modifications

- Malware created new directory in the user's local application data directory – "Bitrix Security". This directory contained various files including "nlqocq.dll".

Registry modifications

- Malware registered system program "rundll32.exe" with a full path to "nlqocq.dll" as an argument under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.



- Malware disabled pop-up blocker, phishing filter and ActiveX warnings in Internet Explorer's settings.
- Malware stored its settings under “HKEY_CURRENT_USER\Software\Microsoft\Essentials”.

Network traffic

None.

Additional information

- NIS alerted about malware's attempt to execute “cmd.exe” in order to delete its own executable.
- NIS alerted about Internet Explorer's, Windows Live Messenger's, and Total Commander's attempt to access the Internet using unrecognized module “nlqocq.dll”. Blocking these attempts caused that the infected applications were no longer able to access the Internet.

Score

1 point:

- Malware was started after the reboot.
- Malware infected processes in the system with its DLL. Malware changed Internet Explorer's settings and decreased its security.
- No information leaked. (1 point)

Malware Sample.14

VirusTotal report: 1288348444

Unprotected machine results

File system modifications

- Malware deleted its own executable.
- Malware created "dwm.exe" in the user's temporary directory.
- Malware created new files under the user's application directory – "shell.exe", "stor.cfg", "svchost.exe".

Registry modifications

- Malware registered the new "svchost.exe" under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.
- Malware added the new "shell.exe" to "Shell" value under "HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" in order to persist in the system.
- Malware registered the new "dwm.exe" to "Load" value under "HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows" in order to persist in the system.
- Malware changed the settings of Internet Explorer in order to make it use proxy on localhost's port 50370.

Network traffic

- Malware sent information about the system to web server protectyourpc-11.com.
- Malware communicated with various Chinese web servers – e.g. qudeteyuj.cn.

Additional information

None.

CIS results

File system modifications

- Malware created new files under the user's application directory – "stor.cfg", "svchost.exe".

Registry modifications

- Malware changed the settings of Internet Explorer in order to make it use proxy on localhost's port 50370.

Network traffic

None.

Additional information

- Internet Explorer was not able to access the Internet.
- CIS alerted about malware's attempt to access the Internet.

Score

4 points:

- No infection persisted in the system. (3 points)
- Internet Explorer was not able to access the Internet.
- No information leaked. (1 point)

NIS results

File system modifications

- Malware created new files under the user's application directory – "stor.cfg", "svchost.exe".

Registry modifications

- Malware registered the new "svchost.exe" under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.

- Malware changed the settings of Internet Explorer in order to make it use proxy on localhost's port 50370.

Network traffic

None.

Additional information

- Internet Explorer was not able to access the Internet.
- NIS alerted about malware's attempt to access the Internet.

Score

1 points

- Malware was started after the reboot.
- Internet Explorer was not able to access the Internet.
- No information leaked. (1 point)

Malware Sample.15

VirusTotal report: 1288348449

Unprotected machine results

File system modifications

- Malware deleted its own executable.
- Malware created two INI files in ProgramData directory.
- Malware created "rasadhlp.dll" in the Internet Explorer's installation directory in order to persist in the system and infect Internet Explorer when it is started.

Registry modifications

None.

Network traffic

- Malware communicated with web server newprojectbrain.com.

Additional information

None.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about "TrojWare.Win32.TrojanDownloader.Murlo" in a newly created HTM file in the user's temporary directory.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

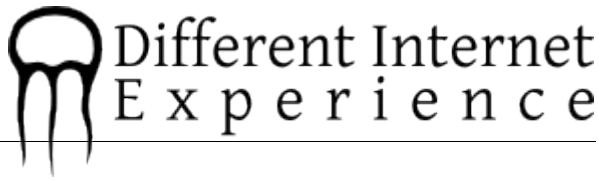
None.

Registry modifications

None.

Network traffic

None.



Additional information

- NIS alerted about blocked security risk “Trojan.Gen”.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

Malware Sample.16

VirusTotal report: 1288350227

Unprotected machine results

File system modifications

- Malware created “oldbin.exe” in the Windows directory.
- Malware created “eraseme_44600.exe” in the user's temporary directory.

Registry modifications

- Malware registered “oldbin.exe” under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run” and under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.
- Malware created new “Allow” rules in Windows firewall settings for “oldbin.exe” and added its binaries on the Windows firewall list of authorized applications.

Network traffic

- Malware communicated with web server nice.niceshot.in.
- Malware downloaded executable file from iphoneate.in.

Additional information

None.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to execute shellcode as a result of possible buffer overflow attack.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

- Malware created “oldbin.exe” in the Windows directory.

Registry modifications

- Malware registered “oldbin.exe” under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run” and under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.

- Malware created new “Allow” rules in Windows firewall settings for “oldbin.exe” and added its binaries on the Windows firewall list of authorized applications.

Network traffic

None.

Additional information

- NIS alerted about malware's attempt to access the Internet.

Score

2 points:

- Malware was started after the reboot.
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

Malware Sample.17

VirusTotal report: 1288354153

Unprotected machine results

File system modifications

- Malware created new files in "Windows\Help" directory – "Mesada.dll", "Mesada.hlp".

Registry modifications

- Malware registered itself under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run" in order to persist in the system.

Network traffic

- Malware attempted to send information about the system to web server angkorbooking.com.

Additional information

None.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- Malware reported access denied to "Windows\Help\Mesada.dll".

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

- Malware created new files in "Windows\Help" directory – "Mesada.dll".

Registry modifications

None.

Network traffic

None.

Additional information

- NIS alerted about malware's attempt to inject code into process "charmap.exe".

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

Malware Sample.18

VirusTotal report: 1288355860

Unprotected machine results

File system modifications

- Malware deleted its own executable.
- Malware created new files in the system directory – “netsf.inf”, “passthru.sys”, “sigtabd.exe”, “tdn.exe”, ...

Registry modifications

- Malware registered “tdn.exe” under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run” in order to persist in the system.
- Malware set Driver Signing policy to disabled.

Network traffic

- Malware communicated with UDP server os1122.com.

Additional information

- The operating system alerted about installation of unsigned driver. Malware's attempt to disable Driver Signing policy in registry does not work on Windows 7.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to access the Internet.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

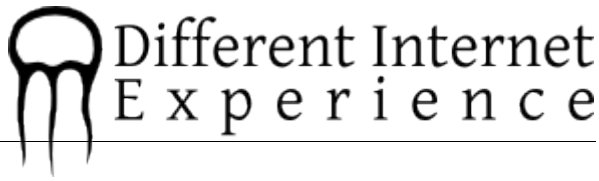
- Malware deleted its own executable.
- Malware created new files in the system directory – “netsf.inf”, “passthru.sys”, “sigtabd.exe”, “tdn.exe”, …

Registry modifications

- Malware registered “tdn.exe” under “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run” in order to persist in the system.
- Malware set Driver Signing policy to disabled.

Network traffic

None.



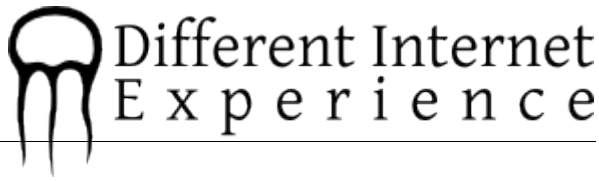
Additional information

- NIS alerted about malware's attempt to access the Internet.
- The operating system alerted about installation of unsigned driver. Malware's attempt to disable Driver Signing policy in registry does not work on Windows 7.

Score

2 points:

- Malware was started after the reboot.
- No important system settings were changed. (1 point)
- No information leaked. (1 point)



Malware Sample.19

VirusTotal report: 1288355869

Unprotected machine results

File system modifications

- Malware created number of executables in the user's temporary directory.
- Malware created new directory "Roaming" in the user's application data folder and created new files in it – "AntiVirus_Studio_2010.exe", "securitycenter.exe", "securityhelper.exe", "taskmgr.dll".
- Malware created various links to its executables – e.g. in Quick Launch and Start Menu.

Registry modifications

- Malware created new rules for the Windows firewall's filtering engine.
- Malware disabled system services "Windows Firewall", "Security Center" and "Windows Update".
- System service "IKE and AuthIP IPsec Keying Modules" was set to start automatically.
- Malware stored its settings under "HKEY_CURRENT_USER\Software\AntiVirus 2010".
- Malware registered "AntiVirus_Studio_2010.exe", "securitycenter.exe" and "securityhelper.exe" under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" in order to persist in the system.

Network traffic

- Malware performed TXT DNS queries on <number>.httpany.net and received answers.
- Malware communicated with web server httpsolution.eu.
- Malware inserted "/antivirusstudio2010net.com" string into some HTTP requests.

Additional information

- Malware displayed GUI of fake security software called "AntiVirus Studio 2010", which performed a fake scan that found number of infections in the computer.
- Malware displayed fake Security Center Alerts warning about infection and unauthorized connections in the system in order to make the user buy and activate the fake security software.
- Malware displayed fake spyware warnings and fake warnings about finding spam bots on the computer in order to make the user buy and activate the fake security software.
- Malware randomly blocked Internet communication and displayed virus attack alert in the browser.
- Malware randomly covered the desktop with black window and played messy sounds in order to convince the user that the computer is infected.

CIS results

File system modifications

- Malware created number of executables in the user's temporary directory.
- Malware created new directory "Roaming" in the user's application data folder and created new files in it – "AntiVirus_Studio_2010.exe", "securitycenter.exe", "securityhelper.exe".
- Malware created various links to its executables – e.g. in Quick Launch and Start Menu.

Registry modifications

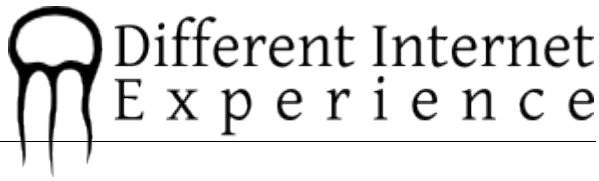
- Malware stored its settings under "HKEY_CURRENT_USER\Software\AntiVirus 2010".

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to gain unlimited access to the computer.



- CIS alerted about malware's attempt to access the Internet.
- CIS alerted about malicious item “Win32.PkdKrap.AS” in “taskmgr.dll”.
- CIS alerted about malware's attempt to access the protected COM interfaces.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

- Malware created “jkfuckfu.exe” in the user's temporary directory.
- Malware created new directory “Roaming” in the user's application data folder and created new files in it – “securityhelper.exe”, “taskmgr.dll”.
- Malware created various links to its executables – e.g. in Quick Launch and Start Menu.

Registry modifications

- Malware disabled system services “Windows Firewall”, “Security Center” and “Windows Update”.
- Malware stored its settings under “HKEY_CURRENT_USER\Software\AntiVirus 2010”.
- Malware registered itself under “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” in order to persist in the system.

Network traffic

None.

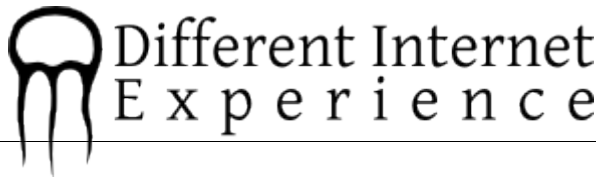
Additional information

- NIS alerted about malware's attempt to access the Internet.
- NIS alerted about Windows Subsystem's attempt to access network using NetBIOS.
- NIS alerted about malware's attempt to run “cmd.exe”.
- NIS alerted about blocked security risk “Trojan.FakeAV!gen32”.
- NIS alerted about malware's attempt to inject code into its own process.

Score

1 point:

- Malware was started after the reboot.
- Malware disabled important system services.
- No information leaked. (1 point)



Malware Sample.20

VirusTotal report: 1288355852

Unprotected machine results

File system modifications

- Malware deleted its own executable.
- Malware created new files in the Windows temporary directory – "1a93e7.sys", "93i79q179.sys".
- Malware modified system driver "compbatt.sys" in the system drivers directory in order to persist in the system.

Registry modifications

- Malware changed name servers to servers in Ukraine.

Network traffic

- Malware communicated with web servers 174.142.51.17 and xeriotz.com.

Additional information

- DNS queries were redirected to malicious servers.

CIS results

File system modifications

None.

Registry modifications

None.

Network traffic

None.

Additional information

- CIS alerted about malware's attempt to access Windows Print Spooler Service interface.

Score

5 points:

- No infection persisted in the system. (3 points)
- No important system settings were changed. (1 point)
- No information leaked. (1 point)

NIS results

File system modifications

None.

Registry modifications

- Malware changed name servers to servers in Ukraine.

Network traffic

None.

Additional information

- NIS alerted about "svchost.exe"'s attempt to access the Internet using unrecognized module "ernel32.dll".
- DNS queries were redirected to malicious servers.

Score

1 point:

- DNS queries were redirected to malicious servers.
- DNS servers were changed.
- No information leaked. (1 point)

Summary of results

The table shown below summarizes the results of CIS's and NIS's performance against 20 malware samples. Successful prevention of persistent malware infection was rewarded with 3 points, success to protect the important system settings and to prevent significant damages of the system was rewarded with 1 point as well as prevention of information leaks.

Malware	Comodo Internet Security			Norton Internet Security		
	Infection	Modification	Data leak	Infection	Modification	Data leak
Sample.01	SUCCESS	SUCCESS	SUCCESS	FAILURE	SUCCESS	SUCCESS
Sample.02	SUCCESS	SUCCESS	SUCCESS	FAILURE	SUCCESS	SUCCESS
Sample.03	SUCCESS	SUCCESS	SUCCESS	FAILURE	FAILURE	SUCCESS
Sample.04	SUCCESS	SUCCESS	SUCCESS	FAILURE	SUCCESS	SUCCESS
Sample.05	SUCCESS	SUCCESS	SUCCESS	FAILURE	SUCCESS	SUCCESS
Sample.06	SUCCESS	SUCCESS	SUCCESS	FAILURE	FAILURE	SUCCESS
Sample.07	SUCCESS	SUCCESS	SUCCESS	SUCCESS	SUCCESS	SUCCESS
Sample.08	SUCCESS	SUCCESS	SUCCESS	FAILURE	FAILURE	SUCCESS
Sample.09	SUCCESS	SUCCESS	SUCCESS	FAILURE	FAILURE	SUCCESS
Sample.10	SUCCESS	SUCCESS	SUCCESS	SUCCESS	SUCCESS	SUCCESS
Sample.11	SUCCESS	SUCCESS	FAILURE	FAILURE	FAILURE	SUCCESS
Sample.12	SUCCESS	SUCCESS	SUCCESS	FAILURE	FAILURE	SUCCESS
Sample.13	SUCCESS	FAILURE	SUCCESS	FAILURE	FAILURE	SUCCESS
Sample.14	SUCCESS	FAILURE	SUCCESS	FAILURE	FAILURE	SUCCESS
Sample.15	SUCCESS	SUCCESS	SUCCESS	SUCCESS	SUCCESS	SUCCESS
Sample.16	SUCCESS	SUCCESS	SUCCESS	FAILURE	SUCCESS	SUCCESS
Sample.17	SUCCESS	SUCCESS	SUCCESS	SUCCESS	SUCCESS	SUCCESS
Sample.18	SUCCESS	SUCCESS	SUCCESS	FAILURE	SUCCESS	SUCCESS
Sample.19	SUCCESS	SUCCESS	SUCCESS	FAILURE	FAILURE	SUCCESS
Sample.20	SUCCESS	SUCCESS	SUCCESS	FAILURE	FAILURE	SUCCESS
Score	60	18	19	12	10	20
Total score	**97**			**42**		

CIS perfectly succeeded to prevent persistent malware infection of the system. CIS failed twice to prevent modifications of important system settings and once to prevent information leak to the Internet. NIS was successful to prevent the infection of the system only in case of 4 samples. It also failed in half of the cases to prevent malicious modifications of important system settings or damaging the system in other way. NIS succeeded to block all malware attempts to leak information to the Internet. In some cases, however, this required blocking access of legitimate applications.

Anti-virus detection of samples

For the purpose of this research anti-virus engine updates and features of the tested products that were in touch with the latest virus signatures were switched off. The reasons have been discussed earlier in this document. However, it might be interesting to know whether today's virus signatures are able to detect the used malware samples.

The malware samples used in this research were collected 1 month before creating this report. All the samples were submitted to VirusTotal service just after that. After the research was finished, we have enabled all previously disabled features of CIS and NIS including automatic updates and we have performed updates in order to get the latest signatures. Then we have tried to copy all the used malware samples to both CIS and NIS machines and run them.

In case of CIS, no sample was copied to the target machine because of CIS's anti-virus detection. In case of NIS, Malware Sample.03, Malware Sample.09 and Malware Sample.18 were not blocked during the copying. Then we were able to run these samples on the NIS machine. Malware Sample.03 and Malware Sample.18 were recognized as malicious shortly after they were run and they were removed from the computer. Malware Sample.09 was not blocked and infected the computer.

At first, all 20 malware samples were undetected by CIS and NIS anti-virus engines. After one month CIS's anti-virus engine detected and blocked all 20 samples, while NIS was able to block 19 of them.

About Different Internet Experience

DIFINEX is most known for its project www.matousec.com, which is focused on Windows desktop security industry. DIFINEX's mission is to improve security of end-users. This is achieved through its own security related projects and research and also through a number of services DIFINEX offers to software vendors including computer related security consulting and research, testing and analyses of security products, analyses of computer viruses, worms, spyware and other malware, analyses of Internet and computer threats and vulnerabilities in security software, programming of security products especially analytical and penetration testing tools.

DIFINEX's research lab is recognized as an independent software testing subject. Since 2006, consumers all around the world have considered the results presented by our lab when they choose the security software for their desktops.