

Detection and Removal of Malwares

Monnappa/Nagareshwar



www.SecurityXploded.com

Disclaimer

The Content, Demonstration, Source Code and Programs presented here is "AS IS" without any warranty or conditions of any kind. Also the views/ideas/knowledge expressed here are solely of the trainer's only and nothing to do with the company or the organization in which the trainer is currently working.

However in no circumstances neither the Trainer nor SecurityXploded is responsible for any damage or loss caused due to use or misuse of the information presented here.

Acknowledgement

- Special thanks to **Null** community for their extended support and co-operation.
- Special thanks to **ThoughtWorks** for the beautiful venue.
- Thanks to all the trainers who have devoted their precious time and countless hours to make it happen.

Advanced Malware Analysis Training

This presentation is part of our **Advanced Malware Analysis** Training program. Currently it is delivered only during our local meets for FREE of cost.



For complete details of this course, visit our [Security Training page](#).

Who Are We?

Nagareshwar

- Founder of SecurityXploded
- Reversing, Malware Analysis, Crypto, Secure Coding
- Twitter: @tnagareshwar

Monnappa

- Info Security Investigator @ Cisco
- Member of SecurityXploded (SX)
- Reverse Engineering, Malware Analysis, Memory Forensics
- Twitter: @monnappa22

Part I

The Trailer

(by Nagareshwar)

Contents of Part 1

- What is Virus/Malware/Worm
- Symptoms of Infection
- Agent in Action
- Last Resort
- Anti-Malware Tips

What is Virus/Malware/Worm ?

- **Malware:** Software written for malicious purposes
 - destroy data, steal money, annoy users
- **Virus:** Malware which requires human intervention to spread
 - require user to click on the exe, open a document or visit a website
- **Worm:** Malware which can spread automatically
 - automatically infect other systems in the network
 - spreads through plug & play devices

Symptoms of Infection

- **Unusual Behaviour in Applications**
- **System Slowdown**
- **(Suddenly) Laptop Getting Heated Heavily**
- **Password Change/Reset Emails for your Bank or Online Accounts**
- **Surprise Financial Transactions on your Credit Cards 😊**

Agent in Action

- **Full Anti-virus Scan (manual)**
 - detect known malwares if any
- **Rootkit Scan**
 - GMER, SpyDLLRemover (helps in removal of malware DLLs)
- **Scan the Infected or Suspicious file with VirusTotal**
 - Get the name of virus/malware family
 - Use VirusTotal Scanner Tool for quick scan
- **Check with AV sites like McAfee, Symantec for the detected Malware**
 - to understand infection details or for any removal steps

Agent in Action (contd)

- **BHO Scan (System Slowdown)**
 - Run SpyBHOREmover and disable unusable BHOs

- **Delete Locked/Hidden/Protected Malware Files**
 - Use GMER to delete Hidden Files/Registry Keys
 - Boot with BackTrack, mount your drives and delete the files/registry keys

- **Change Passwords of Bank & other important accounts**
 - Facebook, Google, Twitter, PayPal etc.

Rootkit Scan using GMER

GMER 1.0.15.14827

Rootkit/Malware >>>

Type	Name	Value
Code	85F96DD8	ZwEnumerateKey
Code	85AE4558	ZwFlushInstructionCache
Code	85B1089E	IoCallDriver
Code	86148B1E	IoCompleteRequest
.text	ntkrnlpa.exe!IoCallDriver	804EEEE8 5 Bytes JMP 85B108A3
.text	ntkrnlpa.exe!IoCompleteRequest	804EEF48 5 Bytes JMP 86148B23
PAGE	ntkrnlpa.exe!ZwFlushInstructionCache	805B51CE 5 Bytes JMP 85AE455C
PAGE	ntkrnlpa.exe!ZwEnumerateKey	80622888 5 Bytes JMP 85F96DDC
.text	D:\WINDOWS\System32\msiexec.exe[1660] msvcr7.dll__p__winver + 21	77C1F2B7 1 Byte [E0]
Module	\systemroot\system32\drivers\UACd.sys [**** hidden ****]	A9B74000-A9B85000 (69632 bytes)
Library	D:\WINDOWS\system32\dll.dll [**** hidden ****] @ D:\WINDOWS\System32\msiexec.exe [1660]	0x10000000
Service	D:\WINDOWS\system32\drivers\UACmdivrtmq.sys [**** hidden ****]	[SYSTEM] UACd.sys
File	D:\Documents and Settings\przemek\Local Settings\Temp\UAC9def.tmp	102400 bytes executable
File	D:\Documents and Settings\przemek\Local Settings\Temp\UAC9e2e.tmp	343040 bytes executable
File	D:\Documents and Settings\przemek\Local Settings\Temp\UACa09f.tmp	131072 bytes executable
File	D:\WINDOWS\system32\drivers\UACmdivrtmq.sys	57344 bytes executable
File	D:\WINDOWS\system32\UACvnmbspvx.dll	31232 bytes executable

System
 Sections
 IAT/EAT
 Devices
 Modules
 Processes
 Threads
 Libraries
 Services
 Registry
 Files


C:\
 D:\
 E:\

ADS
 Show all

Scan
Copy
Save ...

OK Cancel

GMER

 **WARNING !!!**

GMER has found system modification caused by ROOTKIT activity.

OK

Remove Malware DLLs using SpyDLLRemover


The screenshot displays the SpyDLLRemover application window. The title bar reads "SpyDLLRemover". The main header features the product name "SPYDLLREMOVER" in a large, stylized font, with the subtitle "Spyware DLL Analysis and Removal Tool" below it. On the left is a shield icon with a yellow star, and on the right is a shield icon with a green sword. The interface includes a menu bar with "Spy Scanner", "Process Viewer", and "DLL Tracer". Below the menu bar, there are three tabs: "Spy Scanner", "Process Viewer", and "DLL Tracer". The "Process Viewer" tab is active, showing a table of running processes. The "DLL Tracer" tab is also active, showing a table of loaded DLLs. At the bottom, there are buttons for "DLL Info", "Check Drifts", "Remove DLL", "Refresh", "Process Info", "Kill Process", and "Export".

Process Name	PID	Session ID	Threat Infor...	Company	Description	Memory	File Size	Date	File Path
chrome.exe	1580	0		Google Inc.	Google Chrome	24,036 K	955 K	14-09-2010	C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Application\chrome.exe
chrome.exe	3688	0		Google Inc.	Google Chrome	3,036 K	955 K	14-09-2010	C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Application\chrome.exe
cmd.exe	3412	0		Microsoft Corporation	Windows Command Pr...	116 K	379 K	04-08-2004	C:\WINDOWS\system32\cmd.exe
cmd.exe	472	0		Microsoft Corporation	Windows Command Pr...	148 K	379 K	04-08-2004	C:\WINDOWS\system32\cmd.exe
cmd.exe	2980	0		Microsoft Corporation	Windows Command Pr...	152 K	379 K	04-08-2004	C:\WINDOWS\system32\cmd.exe
csrss.exe	640	0		Microsoft Corporation	Client Server Runtime...	884 K	6 K	04-08-2004	C:\WINDOWS\system32\csrss.exe
Dbgview.exe	1392	0		Sysinternals	DebugView	1,232 K	450 K	30-08-2010	C:\Documents and Settings\Administrator\Desktop\Dbgview.exe
explorer.exe	1464	0		Windows Explorer	Windows Explorer	14,256 K	1,008 K	04-08-2004	C:\WINDOWS\explorer.exe
explore.exe	3880	0		Microsoft Corporation	Internet Explorer	29,564 K	91 K	27-06-2010	C:\Program Files\Internet Explorer\IEXPLORE.EXE
lsass.exe	720	0		Microsoft Corporation	LSA Shell (Export Vers...	1,272 K	13 K	04-08-2004	C:\WINDOWS\system32\lsass.exe
msmsgs.exe	1696	0		Microsoft Corporation	Windows Messenger	1,660 K	1,628 K	27-06-2010	C:\Program Files\Messenger\msmsgs.exe
mspaint.exe	3616	0		Microsoft Corporation	Paint	1,684 K	335 K	27-06-2010	C:\WINDOWS\system32\mspaint.exe
notepad.exe	3980	0		Microsoft Corporation	Notepad	376 K	67 K	04-08-2004	C:\WINDOWS\system32\notepad.exe
orbitdm.exe	344	0		Orbitdownloader.com	Orbit Downloader	568 K	1,767 K	01-10-2010	C:\Program Files\Orbitdownloader\orbitdm.exe
regedit.exe	3404	0		Microsoft Corporation	Registry Editor	336 K	143 K	04-08-2004	C:\WINDOWS\regedit.exe
services.exe	708	0		Microsoft Corporation	Services and Contrroll...	2,972 K	105 K	04-08-2004	C:\WINDOWS\system32\services.exe
smss.exe	592	0		Microsoft Corporation	Windows NT Session ...	344 K	49 K	04-08-2004	C:\WINDOWS\system32\smss.exe
spoolsv.exe	1572	0		Microsoft Corporation	Spooler SubSystem App	2,772 K	56 K	04-08-2004	C:\WINDOWS\system32\spoolsv.exe
svchost.exe	3384	0		Microsoft Corporation	Generic Host Process ...	4,072 K	14 K	04-08-2004	C:\WINDOWS\system32\svchost.exe
svchost.exe	3036	0		Microsoft Corporation	Generic Host Process ...	1,496 K	14 K	04-08-2004	C:\WINDOWS\system32\svchost.exe
svchost.exe	1204	0		Microsoft Corporation	Generic Host Process ...	4,056 K	14 K	04-08-2004	C:\WINDOWS\system32\svchost.exe

DLL Name	Company	Description	Comment	Load Count	Load Type	File Size	Version	Date	Base Address	Entry Point	File Path
[Unknown]			Hidden Rootkit DLL	1	Dynamic				0x009d0000	0x009d23aa	
[Unknown]			Hidden Rootkit DLL	1	Dynamic				0x009a0000	0x009a23aa	
[Unknown]			Hidden Rootkit DLL	1	Dynamic				0x01ae0000	0x01ae23aa	
AcGeneral.DLL	Microsoft Corp...	Windows Com...		1	Dynamic	1,809 K	5.1.2...	04-08-2004	0x6f880000	0x6f8a5e1a	C:\WINDOWS\AppPatch\AcGeneral.dll
ADVAPI32.dll	Microsoft Corp...	Advanced Win...		26	Dynamic	602 K	5.1.2...	04-08-2004	0x77dd0000	0x77d470d4	C:\WINDOWS\system32\advapi32.dll
Apphelp.dll	Microsoft Corp...	Application Co...		1	Dynamic	124 K	5.1.2...	04-08-2004	0x77b40000	0x77b41c13	C:\WINDOWS\system32\apphelp.dll
conct32.dll	Microsoft Corp...	Common Contr...		1	Dynamic	597 K	5.82	04-08-2004	0x5d090000	0x5d0932da	C:\WINDOWS\system32\conct32.dll
conct32.dll	Microsoft Corp...	User Experien...		1	Dynamic	1,026 K	6.0	28-06-2010	0x773d0000	0x7734a2b3	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1f9f\conct32.dll
GDI32.dll	Microsoft Corp...	GDI Client DLL		-1	Static	271 K	5.1.2...	04-08-2004	0x77f10000	0x77f163ca	C:\WINDOWS\system32\gdi32.dll
kernel32.dll	Microsoft Corp...	Windows NT B...		-1	Static	960 K	5.1.2...	04-08-2004	0x7c800000	0x7c80b436	C:\WINDOWS\system32\kernel32.dll
MSACM32.dll	Microsoft Corp...	Microsoft ACM...		1	Dynamic	70 K	5.1.2...	04-08-2004	0x77be0000	0x77be1292	C:\WINDOWS\system32\msacm32.dll
msvcrt.dll	Microsoft Corp...	Windows NT C...		-1	Static	335 K	7.0.2...	04-08-2004	0x77c10000	0x77c1f2a1	C:\WINDOWS\system32\msvcrt.dll

VirusTotal Scanner Tool

VirusTotalScanner - www.SecurityXploded.com



VirusTotal Scanner


Desktop Tool to Perform Quick Anti-virus Scan using VirusTotal

www.SecurityXploded.com About


Scan File: C:\Users\Administrator\Desktop\gmer.exe

MDS Hash: ff72056739c31e4cc920bfdff4f9a8e5

SHA256 Hash: ce723717c56b2231ea7843f5408225b07a997b466584d38d278db5e7cf2c2eb0



Community Statistics Documentation FAQ About



SHA256: ce723717c56b2231ea7843f5408225b07a997b466584d38d278db5e7cf2c2eb0

File name: 3jqzq15nl.exe

Detection ratio: 1 / 42

Analysis date: 2012-06-24 13:43:27 UTC (3 hours, 3 minutes ago)

[More details](#)

Antivirus	Result	Update
AhnLab-V3	-	201
AntiVir	-	201

Remove BHOs using SpyBHOREmover

SpyBHOREmover - www.SecurityXploded.com



SpyBHOREmover

Advanced Spy BHO Explorer & Eliminator



www.SecurityXploded.com About

Installed BHO List:

BHO Name	Threat Information	Company	Product	Date	BHO CLSID	BHO File Path
QJSIEStartDetectorImpl...	File does not exist				{E7E6F031-17CE-4C0...	<file not found> c:\program files\java\jre6\lib\qjs_plugin.dll
Vanquish	Check Online (Right click here)		Vanquish DLL	24-08-2010	{D0A17037-7D08-41C...	c:\windows\vanquish.dll
Ocbt Class	No Threats found	Orbitdownloader...	Orbitcbt	21-06-2010	{00012384-9842-4900...	c:\program files (x86)\orbitdownloader\orbitcbt.dll
Adobe PDF Link Helper	No Threats found	Adobe Systems I...	AcroIEHelper...	11-06-2008	{18DF081C-E8AD-428...	c:\program files (x86)\common files\adobe\acrobat\activex\acroiehelpershim...
Groove GFS Browser H...	No Threats found	Microsoft Corpor...	Microsoft Offic...	25-04-2009	{72853161-30C5-4D22...	c:\program files (x86)\microsoft office\office14\grooveex.dll
Windows Live Sign-in H...	No Threats found	Microsoft Corpor...			{464-4C02-4AB...	c:\program files (x86)\common files\microsoft shared\windows live\windowsl...
Office Document Cache...	No Threats found	Microsoft Corpor...			{82F5-0E21-49F9...	c:\program files (x86)\microsoft office\office14\utredir.dll
Java(tm) Plug-In 2 SSV ...	No Threats found	Sun Microsyste...				c:\program files (x86)\java\jre6\bin\jp2ssv.dll

Remove BHO
Check for Threats Online
Show File in Explorer
Jump to Registry
File Properties

VirusTotal
ThreatExpert
ProcessLibrary

Removed BHO List:

BHO Name	Company	Product	Date	BHO CLSID	BHO File Path
RealPlayer Download a...	RealPlayer		22-06-2010	{3049C3E9-B461-4BC5-8870-4C03146...	c:\programdata\real\realplayer\browserrecordplugin\ie\rbrowserrecordplugin.dll
Adobe PDF Conversion ...	Adobe Systems Inco...	Adobe PDF Toolbar ...	11-06-2008	{AE7CD045-E861-484f-8273-0445EE16...	c:\program files (x86)\common files\adobe\acrobat\activex\acroiefavclnt.dll
McAfee SiteAdvisor BHO	McAfee, Inc.	McAfee SiteAdvisor	08-08-2010	{B164E929-A1B6-4A06-B104-2CD0E90...	c:\program files (x86)\mcafee\siteadvisor\mciieplg.dll
Trillian Toolbar	Ask	Toolbar	26-05-2010	{D4027C7F-154A-4066-A1AD-4243D81...	c:\program files (x86)\ask.com\genericask\toolbar.dll
SmartSelect Class	Adobe Systems Inco...	Adobe PDF Toolbar ...	11-06-2008	{F4971EE7-DAAD-4053-9964-66508EE...	c:\program files (x86)\common files\adobe\acrobat\activex\acroiefavclnt.dll

Threat Levels: ■ Dangerous ■ Suspicious ■ Need Analysis ■ Good

Refresh Disable BHO Remove BHO Restore BHO Export Close

Threat Report on Virus



Symantec

Enterprise



United States



Shopping

Products & Solutions

Support & Communities

Security Response

Try & Buy

Security Response / Backdoor:Tidserv

Backdoor.Tidserv

Risk Level 2: Low

Summary

Technical Details

Removal

[Download Removal Tool](#) | [Printer Friendly Page](#) | [Rate This Page](#)

Discovered: September 18, 2008

Updated: November 9, 2012 11:40:02 AM

Also Known As: Backdoor:W32/TDSS [F-Secure], BKDR_TDSS [Trend], Win32/Alureon [Microsoft], Trojan-Dropper.Win32.TDSS [Kaspersky], Packed.Win32.TDSS [Kaspersky],

Type: Trojan

Systems Affected: Windows 2000, Windows NT, Windows Server 2003, Windows Vista, Windows XP

1. Prevention and avoidance

1.1 User behavior and precautions

1.2 Patch operating system and software

1.3 Address blocking

2. Infection method

2.1 Forums and blogs

2.2 Hacked websites

2.3 File sharing, cracks, and warez

2.4 Affiliate schemes

3. Functionality

3.1. System modifications

3.2. Network activity

3.3. Rootkit functionality

4. Additional information

Last Resort

In case of full system or widespread infections,

- **System Restore to 'Right Restore Point'**
 - look at the dates of infected files and it should give you right date to restore from
- **Format and Re-install OS**
 - clean-up other drives if necessary
- **Scan other systems/devices in your Network**
 - Your laptops, office systems or friends system may be infected as well

Anti-Malware Tips

- **Never Trust your AntiVirus for Full Protection**
 - It cannot detect advanced virus especially rootkit oriented ones,
 - Smart virus can disable AV auto protection silently giving you false sense of security
- **Always Scan any EXE with VirusTotal**
 - scan files downloaded from Internet and even files sent by close friends
 - Use **VirusTotal Scanner** for quick scan
- **Disable AutoRun**
 - most malwares use this mechanism spread very effectively
 - prevent getting infected through USB stick and stop it from spreading

Anti-Malware Tips (contd)

- **Keep tab on your Startup programs**
 - Use HijackThis or AutoRuns from SysInternals
- **Monitor Worms coming through Network**
 - Use NetShareMonitor
- **Backup your Critical Files Periodically**
 - One who Laughs last is the one who had the backup :)

Part II

The Real Show

(by Monnappa)

Contents of Part 2

- Detection and Removal
- Persistent Mechanism
- Demo 1
- Demo 2
- Demo 3
- Demo 4

Detection and Removal

- 1) Isolate the system from the rest of the network
- 2) Look for suspicious file, process, network and registry values
- 3) Identify the file generating the suspicious activity
- 4) Isolate the suspicious file
- 5) verify if the file is malicious
- 6) Identify the persistence mechanism
- 7) Break its persistence mechanism
- 8) Delete the malicious files from the system
- 9) monitor for suspicious activities (repeat step 2 to step 8)

Persistent mechanism

Below are some of the persistent mechanism used by malware:

- 1) Run Registry key
- 2) Appinit_DLL's
- 3) WinLogon Notify
- 4) Runs as Service
- 5) Service DLL
- 6) BHO

DEMO 1

Suspicious Network Activity

Packet capture shows suspicious activity from 192.168.1.100

No.	Time	Source	Destination	Protocol	Length	Info
7	0.021159	192.168.1.100	217.20.112.172	HTTP	300	POST /stat1.php HTTP/1.0
8	0.021190	217.20.112.172	192.168.1.100	TCP	54	80 > 1035 [ACK] Seq=1 Ack=247 Win=15544 Len=0
9	0.046572	217.20.112.172	192.168.1.100	TCP	204	[TCP segment of a reassembled PDU]
10	0.049240	217.20.112.172	192.168.1.100	HTTP	312	HTTP/1.1 200 OK (text/html)
11	0.049413	192.168.1.100	217.20.112.172	TCP	54	1035 > 80 [ACK] Seq=247 Ack=410 Win=63832 Len=0
12	0.049535	192.168.1.100	217.20.112.172	TCP	54	1035 > 80 [FIN, ACK] Seq=247 Ack=410 Win=63832 Len=0
13	0.049551	217.20.112.172	192.168.1.100	TCP	54	80 > 1035 [ACK] Seq=410 Ack=248 Win=15544 Len=0
14	0.050424	192.168.1.100	89.149.243.223	TCP	62	1036 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
15	0.066539	89.149.243.223	192.168.1.100	TCP	62	80 > 1036 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
16	0.066786	192.168.1.100	89.149.243.223	TCP	54	1036 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17	0.067044	192.168.1.100	89.149.243.223	HTTP	466	POST /stat1.php HTTP/1.0
18	0.067075	89.149.243.223	192.168.1.100	TCP	54	80 > 1036 [ACK] Seq=1 Ack=413 Win=15544 Len=0

Frame 4: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: 00:0c:29:87:a7:71 (00:0c:29:87:a7:71), Dst: 70:71:bc:dc:6b:de (70:71:bc:dc:6b:de)
Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 217.20.112.172 (217.20.112.172)
Transmission Control Protocol, Src Port: 1035 (1035), Dst Port: 80 (80), Seq: 0, Len: 0

26	0.103410	192.168.1.100	4.2.2.2	DNS	68	Standard query A axabw.ru
27	0.103418	192.168.1.100	4.2.2.2	DNS	68	Standard query A axabw.ru
28	1.104681	192.168.1.100	4.2.2.2	DNS	68	Standard query A axabw.ru
29	1.104695	192.168.1.100	4.2.2.2	DNS	68	Standard query A axabw.ru
30	1.560062	192.168.1.100	4.2.2.2	DNS	87	Standard query PTR 223.243.149.89.in-addr.arpa
31	1.560071	192.168.1.100	4.2.2.2	DNS	87	Standard query PTR 223.243.149.89.in-addr.arpa
32	2.105360	192.168.1.100	4.2.2.2	DNS	68	Standard query A axabw.ru
33	2.105375	192.168.1.100	4.2.2.2	DNS	68	Standard query A axabw.ru

Follow TCP Stream

Stream Content

```
POST /stat1.php HTTP/1.0
Host: 89.149.243.223
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1)
Accept-Encoding: gzip,deflate
Content-Length: 246
```

Suspicious Process

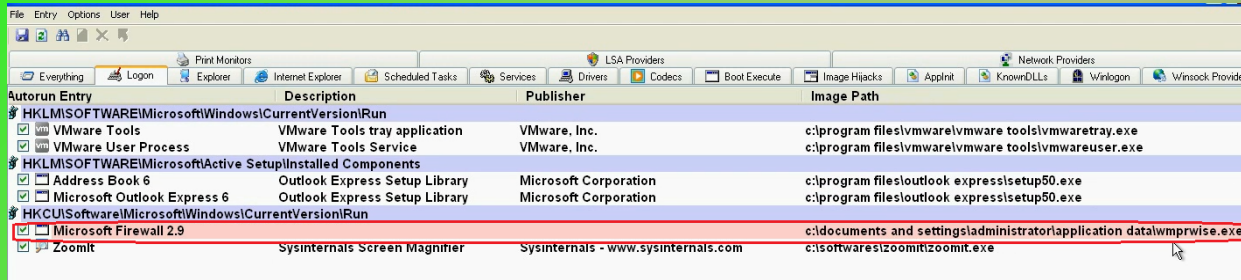
Process explorer shows suspicious process on 192.168.1.100

Process	PID	C...	Private...	Working...	Description	Company Name
System Idle Process	0	52	...	0 K	28 K	
System	4		0 K		236 K	
Interrupts	n/a	5.00	0 K		0 K Hardware Interrupts and DPCs	
smss.exe	584		168 K		388 K Windows NT Session Manager	Microsoft Corporation
csrss.exe	632	1.25	1,444 K		3,136 K Client Server Runtime Process	Microsoft Corporation
winlogon.exe	656		6,780 K		4,196 K Windows NT Logon Application	Microsoft Corporation
services.exe	700	1.25	1,584 K		3,264 K Services and Controller app	Microsoft Corporation
vmacthlp.exe	868		576 K		2,396 K VMware Activation Helper	VMware, Inc.
svchost.exe	880		2,948 K		4,644 K Generic Host Process for Win32 Services	Microsoft Corporation
wmiprvse.exe	1268		2,344 K		4,696 K WMI	Microsoft Corporation
svchost.exe	964		1,664 K		4,084 K Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1052		14,400 K		20,236 K Generic Host Process for Win32 Services	Microsoft Corporation
wuaucrt.exe	1652		6,436 K		6,568 K Automatic Updates	Microsoft Corporation
svchost.exe	1104		1,256 K		3,488 K Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1144		1,724 K		4,616 K Generic Host Process for Win32 Services	Microsoft Corporation
spoolsv.exe	1392		3,760 K		5,516 K Spooler SubSystem App	Microsoft Corporation
vmtoolsd.exe	484		6,452 K		8,644 K VMware Tools Core Service	VMware, Inc.
VMUpgradeHelper.exe	900		996 K		3,904 K VMware virtual hardware upgrade helper applic...	VMware, Inc.
alg.exe	1888		1,100 K		3,460 K Application Layer Gateway Service	Microsoft Corporation
lsass.exe	712	1.25	3,604 K		1,256 K LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1900	2.50	9,144 K		15,012 K Windows Explorer	Microsoft Corporation
VMwareTray.exe	180		1,984 K		4,684 K VMware Tools tray application	VMware, Inc.
VMwareUser.exe	200		3,236 K		8,096 K VMware Tools Service	VMware, Inc.
ZoomIt.exe	228		748 K		2,636 K Sysinternals Screen Magnifier	Sysinternals - www.sysinternals.co...
Tcpview.exe	544		3,540 K		1,168 K TCP/UDP endpoint viewer	Sysinternals - www.sysinternals.co...
procexp.exe	192	36	7,000 K		8,112 K Sysinternals Process Explorer	Sysinternals - www.sysinternals.co...
WMPRWISE.EXE	1832		936 K		2,562 K	

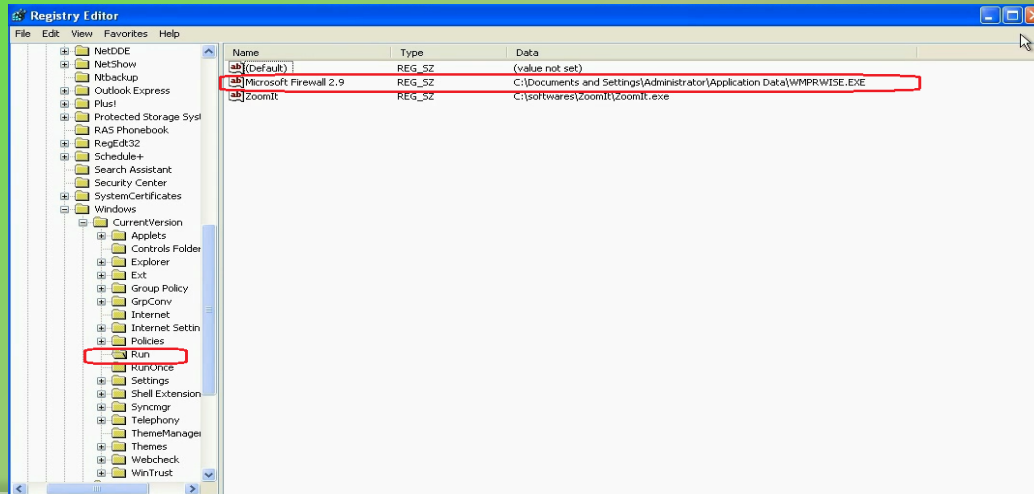
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING
System	4	TCP	192.168.1.100	139	0.0.0.0	0	LISTENING
System	4	UDP	192.168.1.100	137	*	*	
System	4	UDP	0.0.0.0	445	*	*	
System	4	UDP	192.168.1.100	138	*	*	
WMPRWISE.EXE	1832	TCP	192.168.1.100	1036	89.149.243.223	80	LAST_ACK

Persistence Mechanism

Registers the malicious executable in the “Run” registry key, to survive reboot



Autotask Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> VMware Tools	VMware Tools tray application	VMware, Inc.	c:\program files\vmware\vmware tools\vmwaretray.exe
<input checked="" type="checkbox"/> VMware User Process	VMware Tools Service	VMware, Inc.	c:\program files\vmware\vmware tools\vmwareuser.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
<input checked="" type="checkbox"/> Address Book 6	Outlook Express Setup Library	Microsoft Corporation	c:\program files\outlook express\setup50.exe
<input checked="" type="checkbox"/> Microsoft Outlook Express 6	Outlook Express Setup Library	Microsoft Corporation	c:\program files\outlook express\setup50.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> Microsoft Firewall 2.9	Sysinternals Screen Magnifier	Sysinternals - www.sysinternals.com	c:\documents and settings\administrator\application data\wmpwise.exe
<input checked="" type="checkbox"/> Zoomit			c:\softwares\zoomit\zoomit.exe



Name	Type	Data
(Default)	REG_SZ	(value not set)
Microsoft Firewall 2.9	REG_SZ	C:\documents and settings\administrator\application data\WMPWISE.EXE
Zoomit	REG_SZ	C:\softwares\zoomit\zoomit.exe

VirusTotal Results

Suspicious file was confirmed to be malicious



Ikarus	Backdoor.Win32.Azbreg	20121008
Jiangmin	-	20121007
K7AntiVirus	-	20121008
Kaspersky	Trojan-Dropper.Win32.Dapato.bswq	20121008
Kingsoft	Win32.Malware.Generic.a.(kcloud)	20121008
McAfee	PWS-Zbot.gen.amx	20121008
McAfee-GW-Edition	PWS-Zbot.gen.amx	20121008
Microsoft	Trojan:Win32/Nedsym.G	20121008
Norman	W32/Troj_Generic.EPGYA	20121008
nProtect	Trojan.Generic.KD.747453	20121008
Panda	Trj/CI.A	20121008
Rising	-	20121007
Sophos	Troj/Zbot-CRY	20121008
SUPERAntiSpyware	-	20121005
Symantec	Trojan.Gen	20121008

Breaking the Persistence

Deleting the registry value removes the persistence mechanism used by the malware

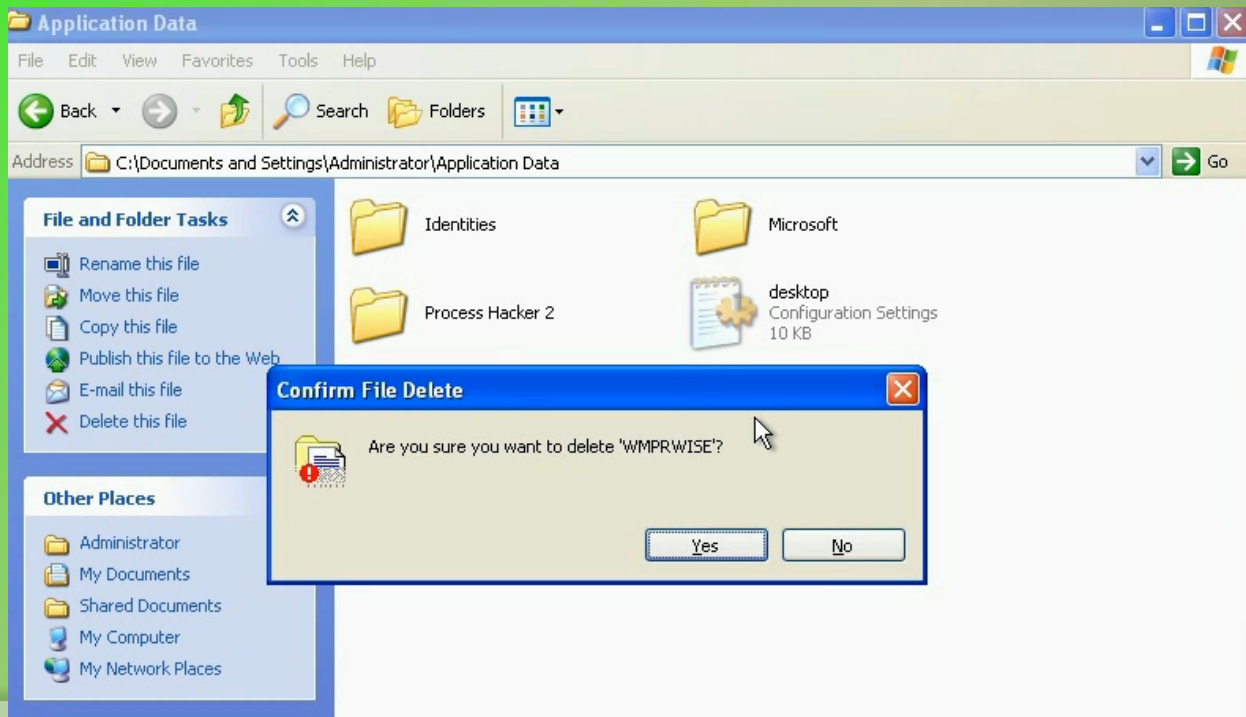
The screenshot shows the Autoruns utility window. The list of startup items is as follows:

Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> VMware Tools	VMware Tools tray application	VMware, Inc.	c:\program files\vmware\vmware tools\vmwaretray.exe
<input checked="" type="checkbox"/> VMware User Process	VMware Tools Service	VMware, Inc.	c:\program files\vmware\vmware tools\vmwareuser.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
<input checked="" type="checkbox"/> Address Book 6	Outlook Express Setup Library	Microsoft Corporation	c:\program files\outlook express\setup50.exe
<input checked="" type="checkbox"/> Microsoft Outlook Express 6	Outlook Express Setup Library	Microsoft Corporation	c:\program files\outlook express\setup50.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> Microsoft Firewall 2.9	Sysinternals Screen Magnifier	Sysinternals - www.sysinternals.com	c:\documents and settings\administrator\application data\wmpwise.exe
<input checked="" type="checkbox"/> ZoomIt	Sysinternals Screen Magnifier	Sysinternals - www.sysinternals.com	c:\software\zoomit\zoomit.exe

A dialog box titled "Autoruns" is displayed, asking: "Are you sure you want to delete autorun of Microsoft Firewall 2.9?". The dialog has "Yes" and "No" buttons.

Removal

Deleting the malicious file to remove the malware from the system



DEMO 2

Suspicious Network Activity

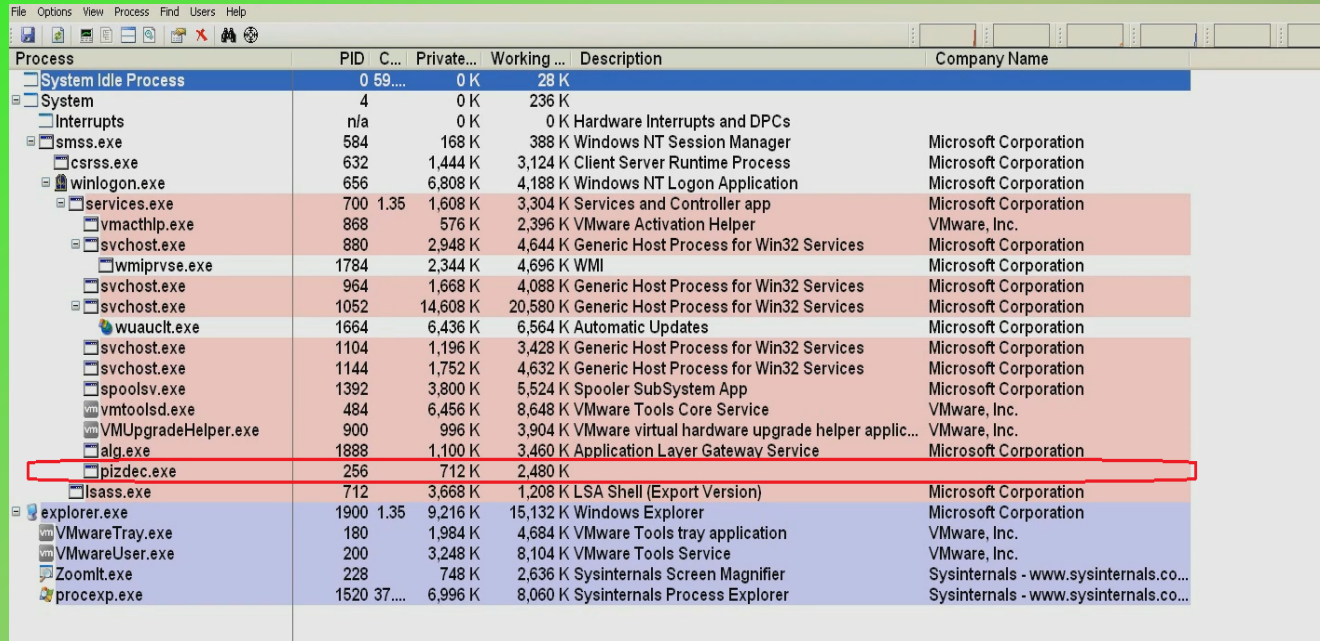
Packet capture shows suspicious activity from 192.168.1.100

8	7.964052	192.168.1.100	89.28.41.81	TCP	62	1035 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
9	7.974392	89.28.41.81	192.168.1.100	TCP	62	80 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
10	7.974618	192.168.1.100	89.28.41.81	TCP	54	1035 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	7.976120	192.168.1.100	89.28.41.81	HTTP	303	POST /login/ HTTP/1.0 (application/x-www-form-urlencoded)
12	7.976147	89.28.41.81	192.168.1.100	TCP	54	80 > 1035 [ACK] Seq=1 Ack=250 Win=15544 Len=0
13	8.001536	89.28.41.81	192.168.1.100	TCP	204	[TCP segment of a reassembled PDU]
14	8.004385	89.28.41.81	192.168.1.100	HTTP	312	HTTP/1.1 200 OK (text/html)
15	8.004536	192.168.1.100	89.28.41.81	TCP	54	1035 > 80 [ACK] Seq=250 Ack=410 Win=63832 Len=0
16	8.004941	192.168.1.100	89.28.41.81	TCP	54	1035 > 80 [FIN, ACK] Seq=250 Ack=410 Win=63832 Len=0
17	8.004964	89.28.41.81	192.168.1.100	TCP	54	80 > 1035 [ACK] Seq=410 Ack=251 Win=15544 Len=0

```
Follow TCP Stream
Stream Content
POST /login/ HTTP/1.0
Host: 89.28.41.81
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US)
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
```


Suspicious Process

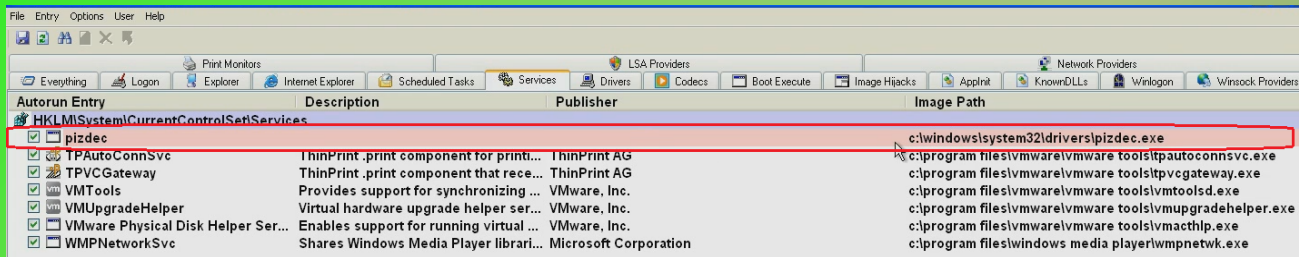
Process explorer shows suspicious process on 192.168.1.100



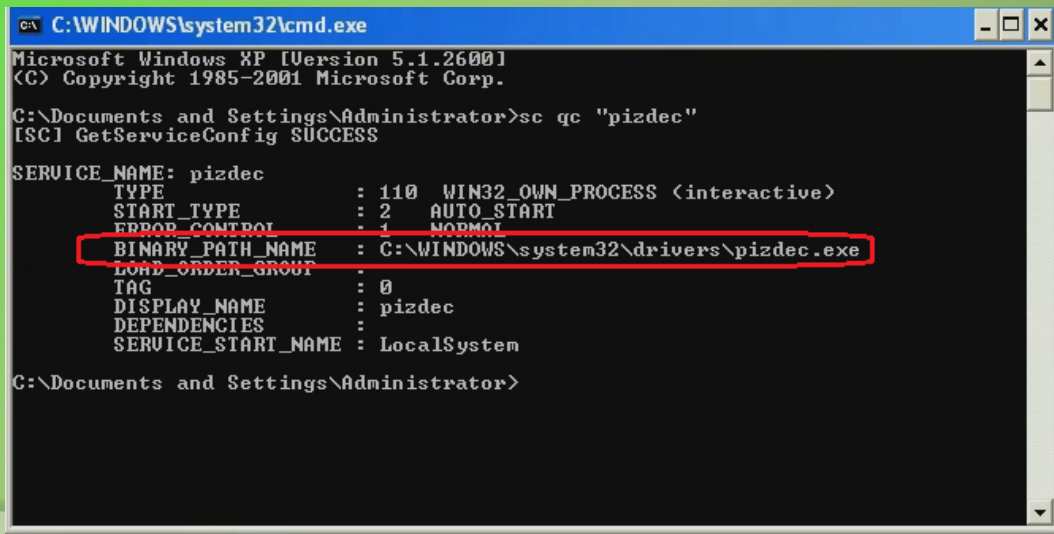
Process	PID	C...	Private...	Working ...	Description	Company Name
System Idle Process	0	59....	0 K	28 K		
System	4		0 K	236 K		
Interrupts	n/a		0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	584		168 K	388 K	Windows NT Session Manager	Microsoft Corporation
csrss.exe	632		1,444 K	3,124 K	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	656		6,808 K	4,188 K	Windows NT Logon Application	Microsoft Corporation
services.exe	700	1.35	1,608 K	3,304 K	Services and Controller app	Microsoft Corporation
vmacthlp.exe	868		576 K	2,396 K	VMware Activation Helper	VMware, Inc.
svchost.exe	880		2,948 K	4,644 K	Generic Host Process for Win32 Services	Microsoft Corporation
wmiiprvse.exe	1784		2,344 K	4,696 K	WMI	Microsoft Corporation
svchost.exe	964		1,668 K	4,088 K	Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1052		14,608 K	20,580 K	Generic Host Process for Win32 Services	Microsoft Corporation
wuauclt.exe	1664		6,436 K	6,564 K	Automatic Updates	Microsoft Corporation
svchost.exe	1104		1,196 K	3,428 K	Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1144		1,752 K	4,632 K	Generic Host Process for Win32 Services	Microsoft Corporation
spoolsv.exe	1392		3,800 K	5,524 K	Spooler SubSystem App	Microsoft Corporation
vmtoolsd.exe	484		6,456 K	8,648 K	VMware Tools Core Service	VMware, Inc.
VMUpgradeHelper.exe	900		996 K	3,904 K	VMware virtual hardware upgrade helper applic...	VMware, Inc.
alg.exe	1888		1,100 K	3,460 K	Application Layer Gateway Service	Microsoft Corporation
plzdec.exe	256		712 K	2,480 K		
lsass.exe	712		3,668 K	1,208 K	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1900	1.35	9,216 K	15,132 K	Windows Explorer	Microsoft Corporation
VMwareTray.exe	180		1,984 K	4,684 K	VMware Tools tray application	VMware, Inc.
VMwareUser.exe	200		3,248 K	8,104 K	VMware Tools Service	VMware, Inc.
ZoomIt.exe	228		748 K	2,636 K	Sysinternals Screen Magnifier	Sysinternals - www.sysinternals.co...
procexp.exe	1520	37....	6,996 K	8,060 K	Sysinternals Process Explorer	Sysinternals - www.sysinternals.co...

Persistence Mechanism

Malware runs as service which is set to auto-start



Autorun Entry	Description	Publisher	Image Path
<input checked="" type="checkbox"/> pizdec			c:\windows\system32\drivers\pizdec.exe
<input checked="" type="checkbox"/> TPAutoConnSvc	ThinPrint .print component for print...	ThinPrint AG	c:\program files\vmware\vmware tools\tpautoconnsvc.exe
<input checked="" type="checkbox"/> TPVCGateway	ThinPrint .print component that rece...	ThinPrint AG	c:\program files\vmware\vmware tools\tpvcgateway.exe
<input checked="" type="checkbox"/> VMTools	Provides support for synchronizing ...	VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe
<input checked="" type="checkbox"/> VMUpgradeHelper	Virtual hardware upgrade helper ser...	VMware, Inc.	c:\program files\vmware\vmware tools\vmupgradehelper.exe
<input checked="" type="checkbox"/> VMware Physical Disk Helper Ser...	Enables support for running virtual ...	VMware, Inc.	c:\program files\vmware\vmware tools\vmacthlp.exe
<input checked="" type="checkbox"/> WMPNetworkSvc	Shares Windows Media Player librari...	Microsoft Corporation	c:\program files\windows media player\wmpnetwk.exe



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

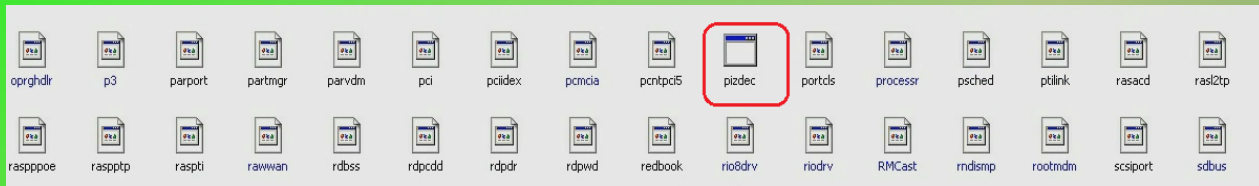
C:\Documents and Settings\Administrator>sc qc "pizdec"
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: pizdec
        TYPE               : 110        WIN32_OWN_PROCESS (interactive)
        START_TYPE          : 2         AUTO_START
        ERROR_CONTROL       : 1         NORMAL
        BINARY_PATH_NAME    : C:\WINDOWS\system32\drivers\pizdec.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME       : pizdec
        DEPENDENCIES        :
        SERVICE_START_NAME : LocalSystem

C:\Documents and Settings\Administrator>
```

VirusTotal Results

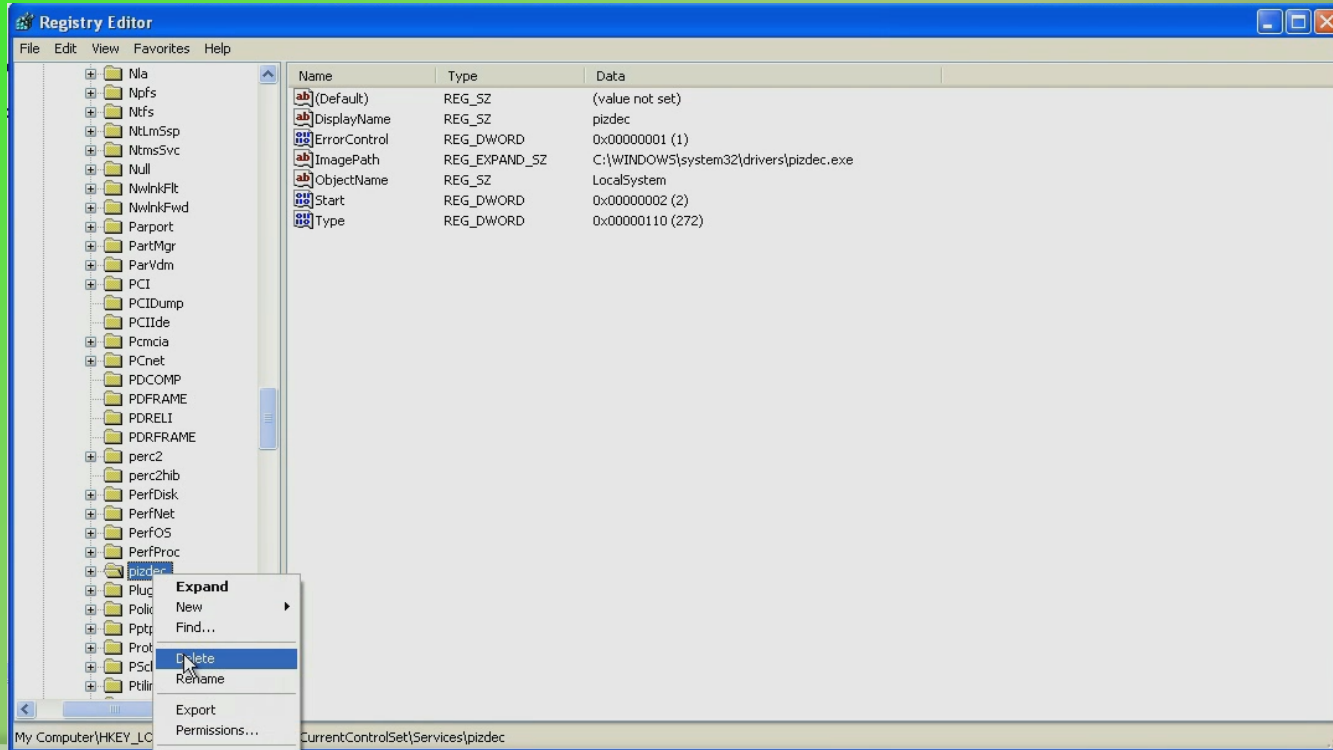
Suspicious file was confirmed to be malicious



Antivirus	Result	Update
Agnitum	Worm.Zwr!NoeqxUze2H8	20121114
AhnLab-V3	Backdoor/Win32.Skill	20121115
AntiVir	TR/ATRAPS.Gen	20121115
Antiy-AVL	Trojan/Win32.Scar.gen	20121115
Avast	Win32:Downloader-JED [Trj]	20121115
AVG	Delf.AHXI	20121115
BitDefender	Gen:Variant.Zusy.Elzob.7405	20121115
ByteHero	-	20121107
CAT-QuickHeal	Trojan.Dishigy.a	20121115

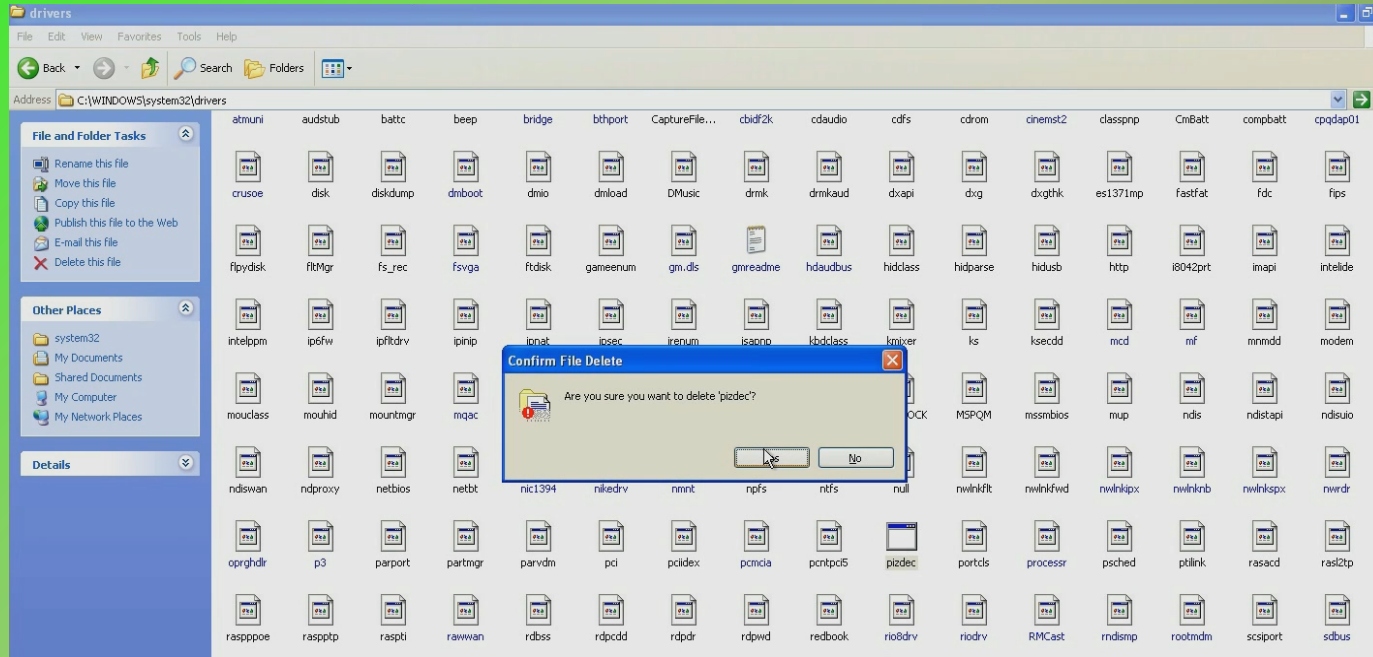
Breaking the Persistence

Deleting the registry value removes the persistence mechanism used by the malware



Removal

Deleting the malicious file to remove the malware from the system



DEMO 3

Suspicious Network Activity

Packet capture shows suspicious activity from 192.168.1.100

No.	Time	Source	Destination	Protocol	Length	Info
61	19.885083	192.168.1.100	192.168.1.2	TCP	54	1026 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
62	19.885262	192.168.1.100	192.168.1.2	HTTP	296	POST /cgi-bin/0wpq4.cgi HTTP/1.1
63	19.885278	192.168.1.2	192.168.1.100	TCP	54	80 > 1026 [ACK] Seq=1 Ack=243 Win=15544 Len=0
65	19.898126	192.168.1.100	192.168.1.2	TCP	62	1029 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
66	19.898278	192.168.1.2	192.168.1.100	TCP	62	80 > 1029 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
67	19.898349	192.168.1.100	192.168.1.2	TCP	54	1029 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
68	19.898498	192.168.1.100	192.168.1.2	HTTP	134	GET /zb/Timesvc.dll HTTP/1.0
69	19.898514	192.168.1.2	192.168.1.100	TCP	54	80 > 1029 [ACK] Seq=1 Ack=81 Win=14600 Len=0
71	19.904547	192.168.1.2	192.168.1.100	TCP	204	[TCP segment of a reassembled PDU]
72	19.907594	192.168.1.2	192.168.1.100	HTTP	312	HTTP/1.1 200 OK (text/html)
73	19.907771	192.168.1.100	192.168.1.2	TCP	54	1026 > 80 [ACK] Seq=243 Ack=410 Win=63832 Len=0
74	19.907777	192.168.1.100	192.168.1.2	TCP	54	[TCP Dup ACK 73#1] 1026 > 80 [ACK] Seq=243 Ack=410 Win=63832 Len=0

Frame 59: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: 00:0c:29:87:a7:71 (00:0c:29:87:a7:71), Dst: 70:71:bc:dc:6b:de (70:71:bc:dc:6b:de)
Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.2 (192.168.1.2)
Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: 80 (80), Seq: 0, Len: 0

```
Stream Content
GET /zb/Timesvc.dll HTTP/1.0
Host: www.macfeeresponse.org
Pragma: no-cache

HTTP/1.1 200 OK
Server: INetSim HTTP Server
Connection: Close
Content-Length: 258
Content-Type: text/html
Date: Wed, 12 Dec 2012 16:03:47 GMT
```

```
Stream Content
POST /cgi-bin/0wpq4.cgi HTTP/1.1
Host: www.yellowpaperofindia.com
Content-Length: 133
Pragma: no-cache
```

Suspicious Process

Below screenshot shows svchost.exe (pid 1052) making connections on port 80

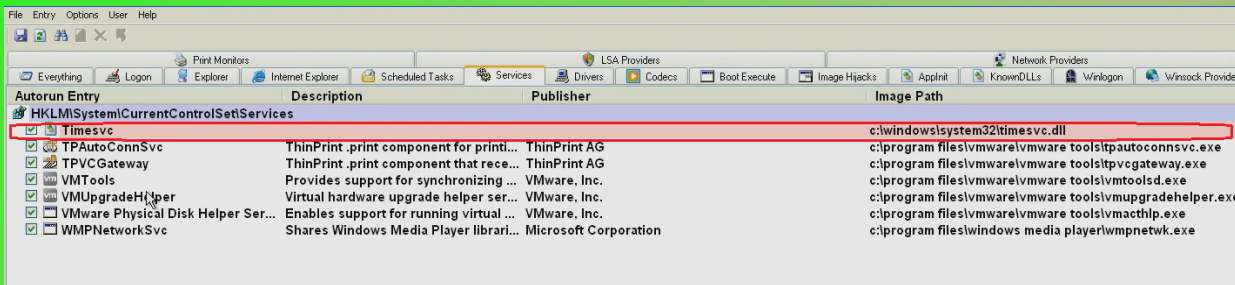
Pr...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Pac...	Sent B...
alg.exe	1852	TCP	127.0.0.1	1031	0.0.0.0	0	LISTENING		
lsass.exe	712	UDP	0.0.0.0	500	*	*			
lsass.exe	712	UDP	0.0.0.0	4500	*	*			
svchost.exe	964	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING		
svchost.exe	1052	UDP	192.168.1.100	123	*	*			
svchost.exe	1052	UDP	127.0.0.1	123	*	*			
svchost.exe	1052	TCP	192.168.1.100	1029	192.168.1.2	80	LAST_ACK	1	
svchost.exe	1052	TCP	192.168.1.100	1026	192.168.1.2	80	LAST_ACK	1	
svchost.exe	1176	UDP	192.168.1.100	1900	*	*			
svchost.exe	1108	UDP	0.0.0.0	51073	*	*		1	
svchost.exe	1176	UDP	127.0.0.1	1900	*	*			
svchost.exe	1052	UDP	127.0.0.1	1028	*	*		1	
svchost.exe	1052	TCP	192.168.1.100	1030	192.168.1.2	80	SYN_SENT		
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING		
System	4	TCP	192.168.1.100	139	0.0.0.0	0	LISTENING		
System	4	UDP	192.168.1.100	137	*	*			
System	4	UDP	0.0.0.0	445	*	*			
System	4	UDP	192.168.1.100	138	*	*		1	

Endpoints: 18 Established: 0 Listening: 4 Time Wait: 0 Close Wait: 0

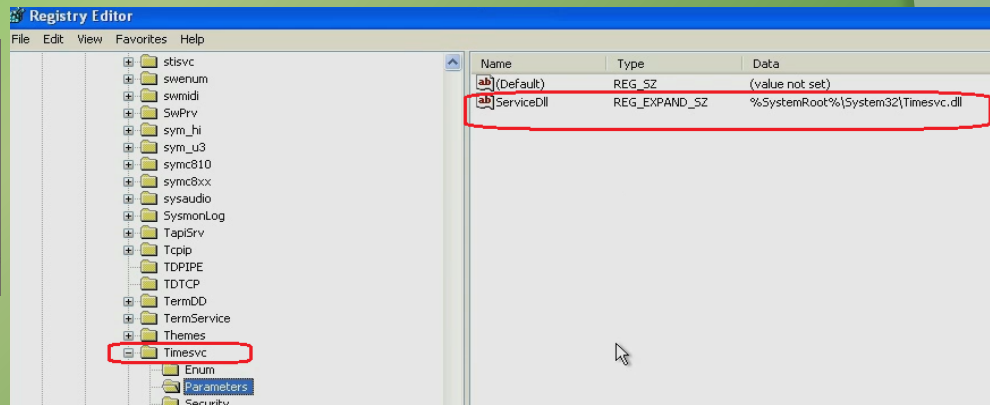
start TCPView - Sysintern... 9:33 PM

Persistence Mechanism

Malware installs a service DLL under the “netsvcs” svchost group

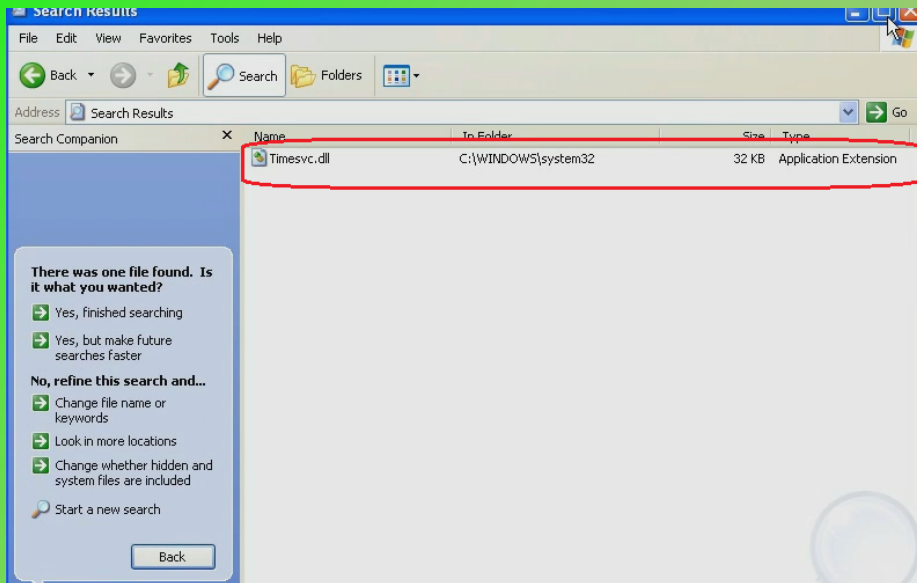


```
C:\Documents and Settings\Administrator>sc qc "timesvc"  
[SC] GetServiceConfig SUCCESS  
  
SERVICE_NAME: timesvc  
        TYPE               : 120  WIN32_SHARE_PROCESS (interactive)  
        START_NAME           : 2     AUTO_START  
        ERROR_CONTROL        : 1     NORMAL  
        BINARY_PATH_NAME     : C:\WINDOWS\system32\svchost.exe -k netsvcs  
        LOAD_ORDER_GROUP    :  
        TAG                  : 0  
        DISPLAY_NAME        : Windows Time Service Management Instrumentation  
        DEPENDENCIES         :  
        SERVICE_START_NAME  : LocalSystem
```



VirusTotal Results

Suspicious file was confirmed to be malicious

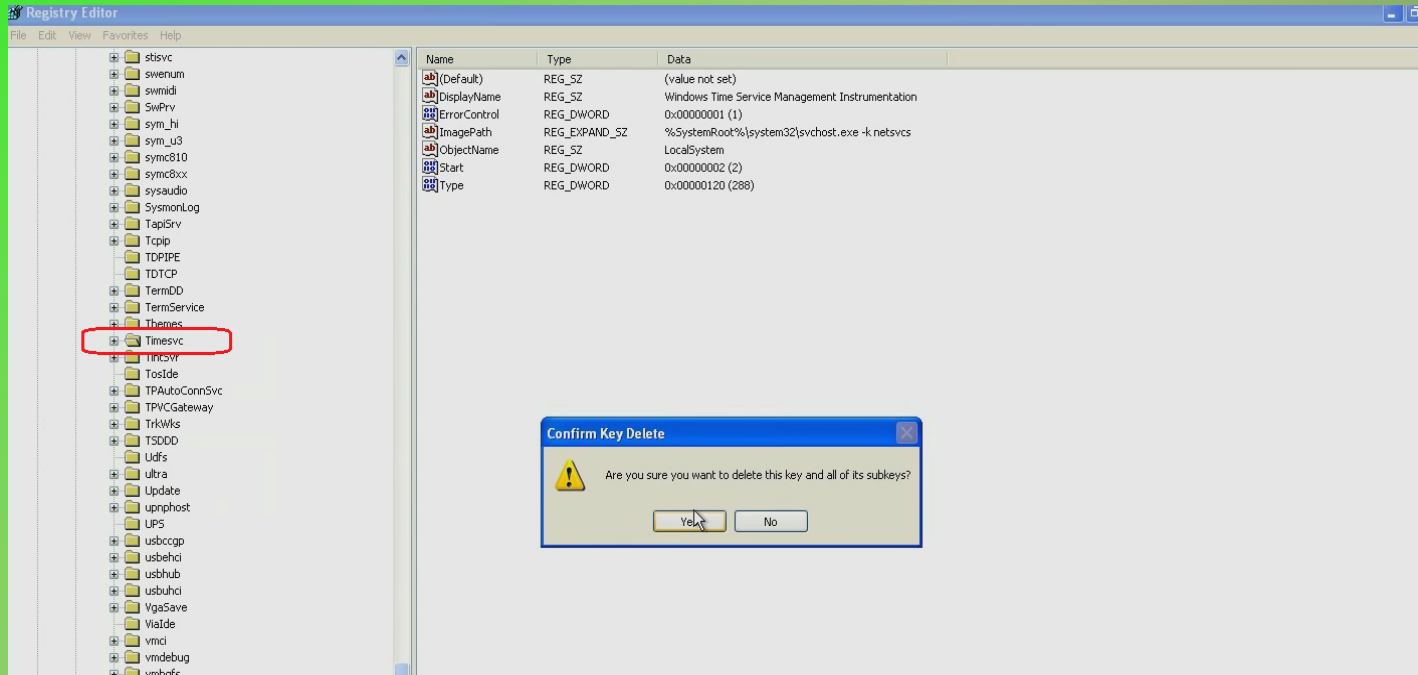


A screenshot of the VirusTotal search results page for the file Timesvc.dll. The page shows a list of scanning engines and their results. The results are as follows:

Engine	Result	Time
eSafe	-	20121115
ESET-NOD32	a variant of Win32/TrojanDownloader.Agent.NVS	20121116
F-Prot	W32/Backdoor2.CDOC	20121116
F-Secure	Trojan.Agent.AJKV	20121116
Fortinet	W32/Agent.ADPV/tr	20121116
GData	Trojan.Agent.AJKV	20121116
Ikarus	Trojan-Dropper.Agent	20121116
Jiangmin	Backdoor/Agent.bqjp	20121116
K7AntiVirus	Backdoor	20121115
Kaspersky	Backdoor.Win32.Agent.odf	20121116
Kingsoft	Win32.Hack.PcClient.Lal.(kcloud)	20121112
McAfee	Enfal	20121116
McAfee-GW-Edition	Enfal	20121116
Microsoft	TrojanDownloader.Win32/Snagit.A.dll	20121116

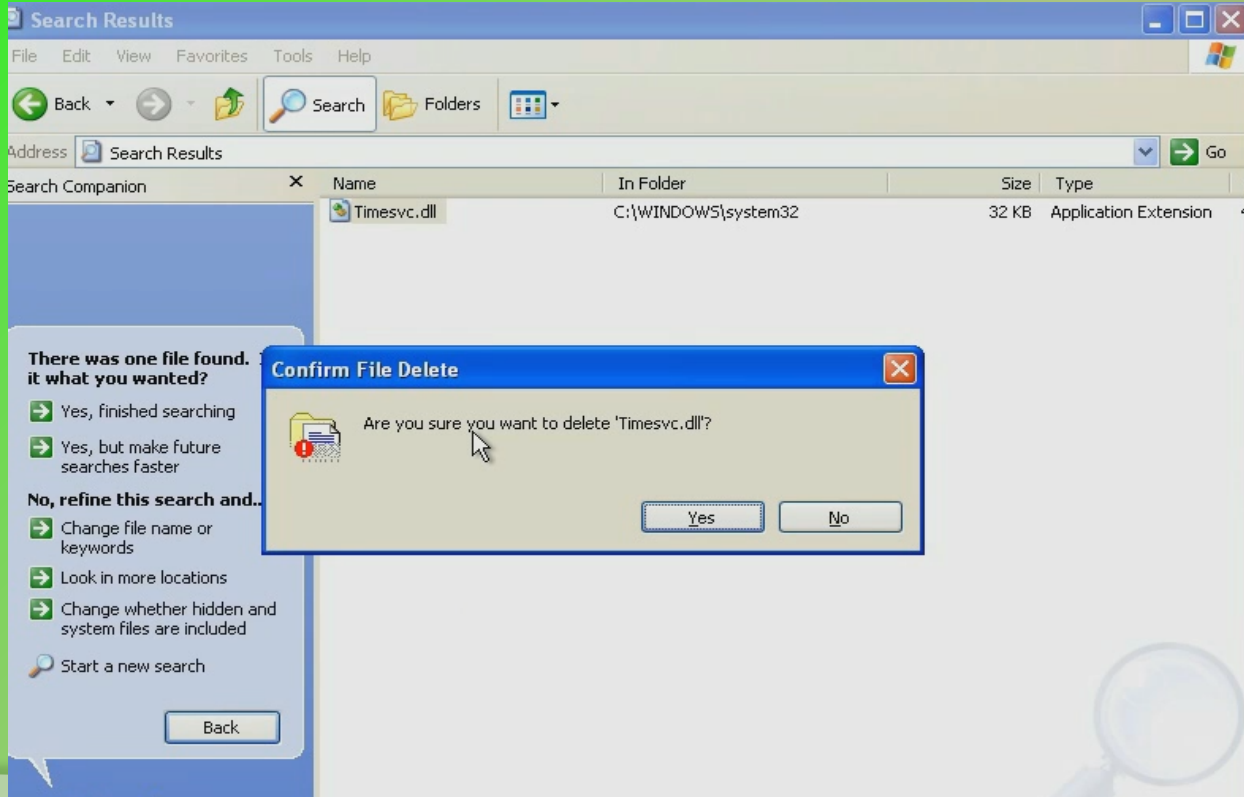
Breaking the Persistence

Deleting the registry key removes the persistence mechanism used by the malware



Removal

Deleting the malicious file to remove the malware from the system



DEMO 4

Suspicious Network Activity

Packet capture shows suspicious activity from 192.168.1.100

6	1.673664	192.168.1.100	4.2.2.2	DNS	74 Standard query A scfzf.xicp.net
7	1.702733	4.2.2.2	192.168.1.100	DNS	90 Standard query response A 192.168.1.2
8	1.708565	192.168.1.100	192.168.1.2	TCP	62 mxrlogin > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
9	1.715264	192.168.1.2	192.168.1.100	TCP	62 http > mxrlogin [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
10	1.721027	192.168.1.100	192.168.1.2	TCP	54 mxrlogin > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	1.721632	192.168.1.100	192.168.1.2	HTTP	101 POST / HTTP/1.1
12	1.721649	192.168.1.2	192.168.1.100	TCP	54 http > mxrlogin [ACK] Seq=1 Ack=128 Win=14600 Len=0
13	1.742372	192.168.1.2	192.168.1.100	TCP	204 [TCP segment of a reassembled PDU]
14	1.742917	MurataMa 50:89:0c	Vmware 87:a7:71	ARP	60 192.168.1.2 is at 04:46:65:50:89:0c
15	1.745258	192.168.1.2	192.168.1.100	HTTP	312 HTTP/1.1 200 OK (text/html)
16	1.745382	192.168.1.100	192.168.1.2	TCP	54 mxrlogin > http [ACK] Seq=128 Ack=410 Win=63832 Len=0

Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Vmware 87:a7:71 (00:0c:29:87:a7:71), Dst: Pegatron dc:6b:de (70:71:bc:dc:6b:de)
Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 4.2.2.2 (4.2.2.2)
User Datagram Protocol, Src Port: 56316 (56316), Dst Port: domain (53)
Domain Name System (query)

Follow TCP Stream

Stream Content

```
POST / HTTP/1.1
Host: scfzf.xicp.net
Content-Length: 0
Connection: Keep-Alive
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: INetSim HTTP Server
Connection: Close
Content-Length: 258
Content-Type: text/html
Date: Mon, 10 Dec 2012 16:52:03 GMT
```

Suspicious Process Activity

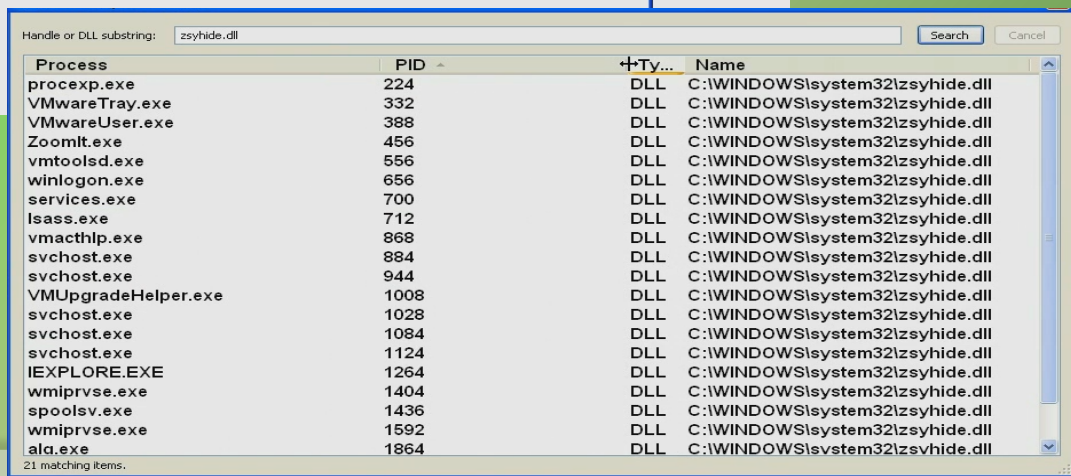
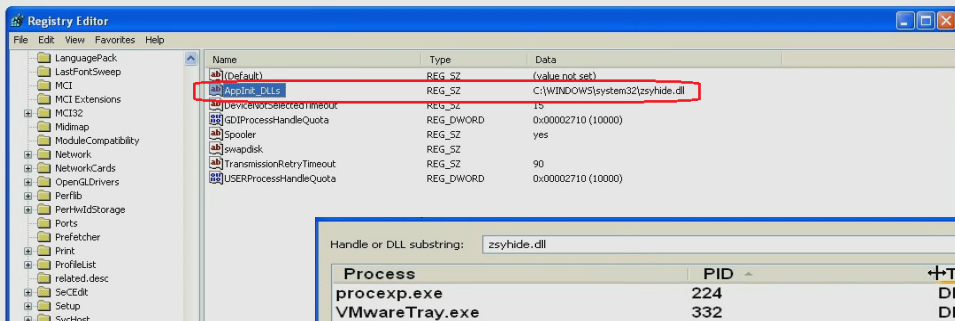
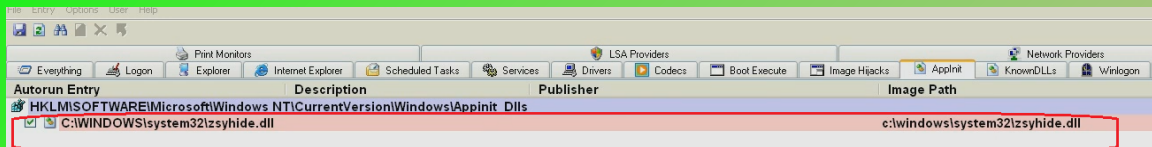
Shows iexplore.exe making connections on port 80 (even though iexplore.exe was not run manually)

Pr...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Pac...	Sen
alox.exe	1888	TCP	127.0.0.1	4028	0.0.0.0	0	LISTENING		
IEXPLORE.EXE	408	TCP	192.168.1.100	1226	192.168.1.2	80	ESTABLISHED		
lsass.exe	712	UDP	0.0.0.0	500	*	*			
lsass.exe	712	UDP	0.0.0.0	4500	*	*			
svchost.exe	964	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING		
svchost.exe	1052	UDP	192.168.1.100	123	*	*			
svchost.exe	1052	UDP	127.0.0.1	1033	*	*			
svchost.exe	1144	UDP	192.168.1.100	1900	*	*			
svchost.exe	1052	UDP	127.0.0.1	123	*	*			
svchost.exe	1144	UDP	127.0.0.1	1900	*	*			
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING		
System	4	TCP	192.168.1.100	139	0.0.0.0	0	LISTENING		
System	4	UDP	192.168.1.100	137	*	*			
System	4	UDP	0.0.0.0	445	*	*			
System	4	UDP	192.168.1.100	138	*	*			

Process	PID	C...	Private...	Working ...	Description	Company Name
System Idle Process	0	10...	0 K	28 K		
System	4		0 K	236 K		
System	n/a	< 0...	0 K		0 K Hardware Interrupts and DPCs	
smss.exe	584		168 K	388 K	Windows NT Session Manager	Microsoft Corporation
csrss.exe	632		1,448 K	3,136 K	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	656		6,972 K	4,704 K	Windows NT Logon Application	Microsoft Corporation
services.exe	700		1,608 K	3,284 K	Services and Controller app	Microsoft Corporation
vmacthlp.exe	868		576 K	2,396 K	VMware Activation Helper	VMware, Inc.
svchost.exe	880		2,948 K	4,644 K	Generic Host Process for Win32 Services	Microsoft Corporation
wmiprvse.exe	1132		2,368 K	4,764 K	WMI	Microsoft Corporation
svchost.exe	964		1,672 K	4,092 K	Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1052		15,640 K	22,356 K	Generic Host Process for Win32 Services	Microsoft Corporation
wuauclt.exe	1664		6,436 K	6,564 K	Automatic Updates	Microsoft Corporation
svchost.exe	1104		1,252 K	3,480 K	Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1144		1,724 K	4,616 K	Generic Host Process for Win32 Services	Microsoft Corporation
spoolsv.exe	1392		3,796 K	5,520 K	Spooler SubSystem App	Microsoft Corporation
vmtoolsd.exe	484		6,456 K	8,640 K	VMware Tools Core Service	VMware, Inc.
VMUpgradeHelper.exe	900		996 K	3,904 K	VMware virtual hardware upgrade helper applic...	VMware, Inc.
alg.exe	1888		1,100 K	3,460 K	Application Layer Gateway Service	Microsoft Corporation
lsass.exe	712		3,636 K	1,440 K	LSA Shell (Export Version)	Microsoft Corporation
IEXPLORE.EXE	128		1,588 K	4,100 K	Internet Explorer	Microsoft Corporation
explorer.exe	1900		9,088 K	15,060 K	Windows Explorer	Microsoft Corporation
VMwareTray.exe	180		1,984 K	4,684 K	VMware Tools tray application	VMware, Inc.
VMwareUser.exe	200		3,236 K	8,096 K	VMware Tools Service	VMware, Inc.
ZoomIt.exe	228		748 K	2,636 K	Sysinternals Screen Magnifier	Sysinternals - www.sysinternals.co...
Tcpview.exe	448		3,512 K	1,172 K	TCPIUDP endpoint viewer	Sysinternals - www.sysinternals.co...
procexp.exe	1196		7,692 K	9,728 K	Sysinternals Process Explorer	Sysinternals - www.sysinternals.co...

Persistence Mechanism

Malware installs Appinit DLL which loads the DLL into all the process which loads user32.dll



Persistence Mechanism (contd)

Malware hooks to the winlogon event

The screenshot shows the Windows Registry Editor with the following path selected: `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\zsydll`. The right pane displays the registry values for this path:

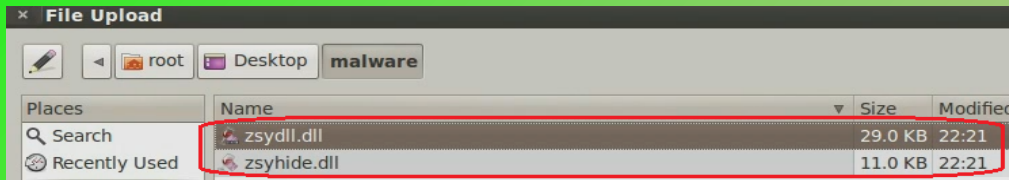
Name	Type	Data
(Default)	REG_SZ	(value not set)
Asynchronous	REG_DWORD	0x00000001 (1)
DllName	REG_SZ	C:\WINDOWS\system32\zsydll.dll
Impersonate	REG_DWORD	0x00000000 (0)
Shutdown	REG_SZ	DoShutdown
Startup	REG_SZ	DoStartup

The screenshot shows the Process Explorer Search window with the search criteria set to `zsydll.dll`. The results table is as follows:

Process	PID	Type	Name
winlogon.exe	656	DLL	C:\WINDOWS\system32\zsydll.dll
IEEXPLORE.EXE	18...	DLL	C:\WINDOWS\system32\zsydll.dll

VirusTotal Results

Suspicious files were confirmed to be malicious



Detection ratio: 40 / 44

Analysis date: 2012-11-29 18:47:19 UTC (1 week, 3 days ago)

[More details](#)

Analysis [Comments](#) [Votes](#) [Additional information](#)

Antivirus	Result
Agnitum	Backdoor.Gusil6ABTWo5ogJ4
AhnLab-V3	Win-Trojan/Ginwui.11264
AntiVir	BDS/Ginwui.A
Antiy-AVL	Backdoor/Win32.Ginwui.gen
Avast	Win32:Trojan-gen
AVG	BackDoor.Generic2.XAU
BitDefender	Backdoor.Ginwui.B

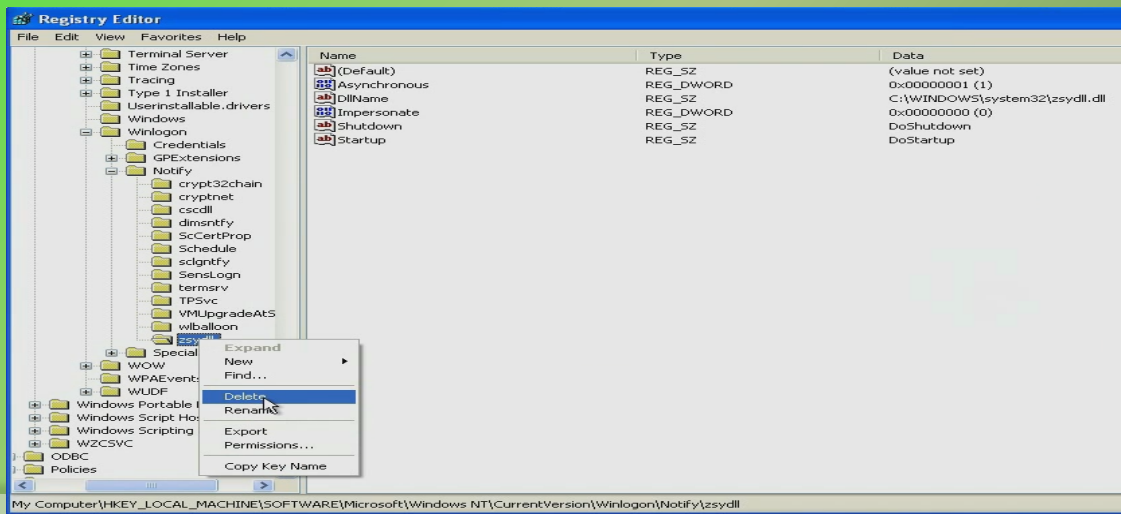
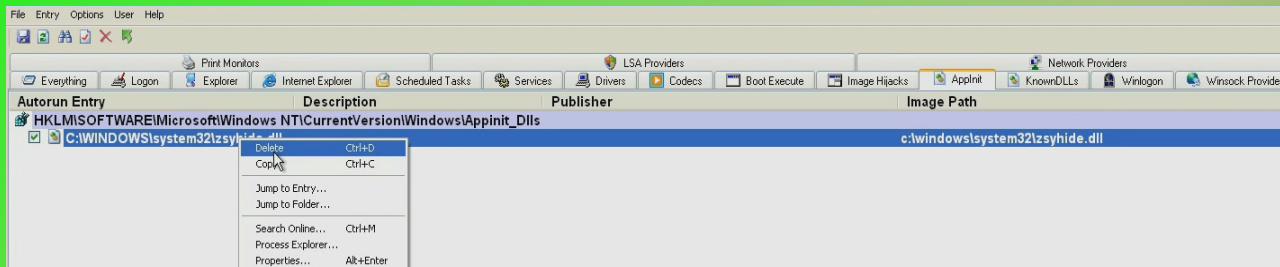
[More details](#)

Analysis [Comments](#) [Votes](#) [Additional information](#)

Antivirus	Result
AntiVir	BDS/Ginwui.A.DLL
Authentium	-
Avast	-
AVG	BackDoor.Generic2.KAT
BitDefender	Backdoor.Ginwui.B
CAT-QuickHeal	-
ClamAV	-
DrWeb	BackDoor.Ginwui
eTrust-InoculateIT	Win32/Ginwui.BIDLL!Trojan
eTrust-Vet	Win32/Ginwui.B
Ewido	Backdoor.Ginwui.a

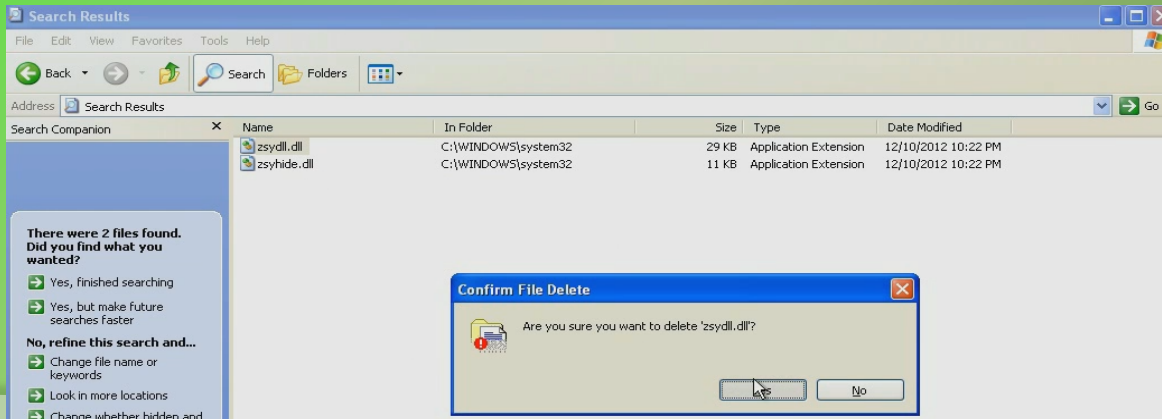
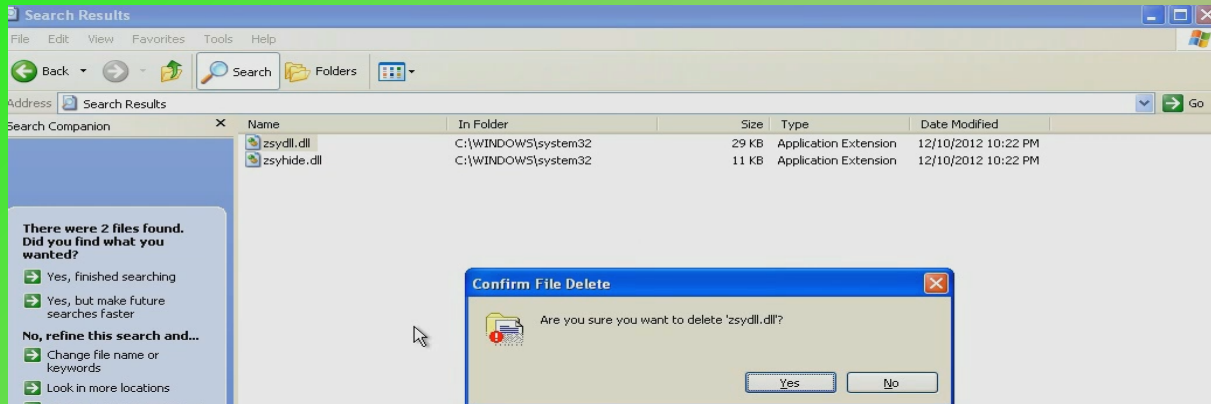
Breaking the Persistence

Deleting the registry key removes the persistence mechanism used by the malware



Removal

Deleting both the malicious files to remove the malware from the system



Reference

[Complete Reference Guide for Advanced Malware Analysis Training](#)
[Include links for all the Demos & Tools]

Thank You !



www.SecurityXploded.com