Fighting malware on your own

Vitaliy Kamlyuk
Senior Virus Analyst
Kaspersky Lab
Vitaly.Kamluk@kaspersky.com
Why fight malware on your own?

5 reasons:
1. Touch 100% of protection yourself
2. Be prepared for attacks
3. Maintain confidentiality
4. Restore system here and now
5. Time matters
What is available in Windows XP?

- **System tools:**
  - Explorer, Task manager, Regedit, SigVerif,…
  - Console utils: netstat, tasklist, reg, expand,…
  - Interpreters: Batch, JS/VBS
  - Text editors: notepad, wordpad, edit, edlin,…
  - Binary editing tool: debug
  - Symbolic debugger: ntsd
  - OLE repository
Email-Worm.Win32.Warezov

- Detected on 15\textsuperscript{th} August, 2006
- 430 modifications (~25000 of files)
- All application data is encrypted
- Code mutates very often (server-side polymorphic engine)
- Downloads additional modules from the Internet
- Hides its modules from Task Manager
Warezov: Infecting the system
Warezov: Installing KAV 6.0
Warezov: What really happened?
Warezov: Inspecting the system
Warezov: Resistance to manual removal

welcome
Analysis

1. Malware restores registry values when the application terminates (seems to be when malicious dll is unloaded).

2. There is a set of processes running/closing from time to time. So the routine is called several times.

3. The value is restored only if it doesn’t exist.

4. Looks like the malware uses one of the following functions: strstr/wcsstr/CString::Find, strtok or its own substring find routine.

We can hack the malware removal resistance mechanism!
Warezov: Hacking the resistance to manual removal
Trojan.Win32.Agent.ach

- Detected on 12th December, 2006
- Made in Japan
- Silently removes itself after being run
- Suspends running destructive functionality until the following Friday, and after that:
  - Disables pressing Ctrl-Alt-Delete
  - Disables running any executable file from shell
  - Disables system shutdown/reboot
  - If you try hard-reboot, it disables loading the system in any available mode
Agent.ach: Infecting the system
Agent.ach: Infection symptoms
Hard reset result - time matters!
Agent.ach: Inspecting the system
Agent.ach: Removing the malware
Agent.ach: Control check
Detected on 10\textsuperscript{th} December, 2006

The virus infects executable files located on a hard disk partition which is selected at random

Injects own DLL into every process that has visible window

Injected DLL makes screenshots of active windows on the victim machine, encrypts them, and publishes them on a website
Saburex: Getting the code
defcon 15, august 3-5, 2007, las vegas, nv, usa
Saburex: Analysis

Source File

- **Src PE Header**
- **Src Sections**

Infected File

- **Virus PE Header**
- **Virus Section**
- **Compressed chunk of src file**
- **Compressed virus module**

Cured File

- **Src PE Header**
- **Src Sections**

Compression and decompression processes are indicated with arrows and 'compress' and 'decompress' labels.
Simple PE Structure
Saburex: Applying the tool
System evolution

1. MS DOS
2. Windows NT
3. Windows 9x/ME
4. Windows 2000
5. Windows XP
6. Windows Vista
Microsoft.NET in the wild
Sniffing malware communication

Methods:
- Analysis of Windows network monitor
- Catching DNS requests (server emulation)
- Catching HTTP request (server emulation)
- Implementing IP packet filter
Packet Filtering Explained
DefCon 15, August 3-5, 2007, Las Vegas, NV, USA

Backdoor.Win32.IRCBot.ach
Advanced techniques

- Viewing PE header
- Ways of terminating a process
- Dumping loaded executable image
- Extracting string data from binary images
How to view PE header of target PE file in Windows:

1. Run: ntsd <path to target PE file>
2. Locate image base of the loaded module
3. !dh <image base>

```plaintext
File Type: EXECUTABLE IMAGE
FILE HEADER VALUES
  14C machine (i386)
  3 number of sections
3B7D8410 time date stamp Sat Aug 18 00:52:32 2001
  0 file pointer to symbol table
  0 number of symbols
  0 size of optional header
  10F characteristics
    Relocations stripped
    Executable
    Line numbers stripped
    Symbols stripped
    32 bit word machine

OPTIONAL HEADER VALUES
  10B magic #
  7.00 linker version
  12800 size of code
  9600 size of initialized data
  0 size of uninitialized data
  12475 address of entry point
  1000 base of code
  ----- new -----  
 01000000 image base
  1000 section alignment
  200 file alignment
  2 subsystem (Windows GUI)
  5.01 operating system version
  5.01 image version
  4.00 subsystem version
  1F000 size of image
  400 size of headers
  2317D checksum
  00040000 size of stack reserve
```
Ways of terminating a process

- Task manager
- `tasklist + taskkill console apps` (starting from WinXP Pro)
- WMI (starting from WinXP) using:
  - Windows Scripting Host
  - WbemTest Application
- `ntsd` (starting from NT4)
- Own pskill-like utility with PID received from:
  - Qprocess
  - Msinfo32
  - Performance monitor
  - etc.
Kill Process: tasklist + taskkill
Kill Process: WMI + WSH
Kill Process: WMI+WbemTest
Kill Process: ntsd
Kill Process: Own tool in machine code

User code for pskill.exe:

f 1600 1700 90
e 1600 ff,15,04,10,40,00 ,68,00,15,40,00 ,83,c0,04 ,50
e 1610 ff,15,20,10,40,00 ,83,c0,04 ,6a,0a ,6a,00 ,ff,30
e 1620 ff,15,30,10,40,00 ,8B,D8 ,ff,15,08,10,40,00, 3b,c3
e 1630 74,3E ,53 ,6a,00 ,6a,01 ,ff,15,0c,10,40,00 ,6a,00 ,50
e 1640 ff,15,10,10,40,00 ,eb,38
e 1670 33,c0
e 1680 50 ,ff,15,00,10,40,00

Usage:

Pskill.exe <Target Process Id>

Getting Process Id using:

- Qprocess
- Msinfo32
- Performance monitor
Kill Process: Getting PID
Dumping a process
The idea:

Grab all sequences of bytes from given file that form a string consisting of 3 or more ASCII characters.

JScript implementation:

```javascript
var fso=new ActiveXObject("Scripting.FileSystemObject");
var fi=fso.OpenTextFile(WScript.Arguments(0), 1, 0);
var fo=fso.CreateTextFile(WScript.Arguments(1), 1);
var pdb="";
while(!fi.AtEndOfStream) {
    var db=fi.Read(1);
    if(pdb.length>0) {
        if((db.charCodeAt(0)>=32 && db.charCodeAt(0)<=127)) pdb+=db;
        else {
            if(pdb.length>4) fo.Write(pdb+"\n");
            pdb="";
            continue;
        }
    }
    else if((db.charCodeAt(0)>=32 && db.charCodeAt(0)<=127)) pdb=db;
}
fo.Close();
fi.Close();
```
The page cannot be displayed

The page you are looking for is currently unavailable. The website might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address box, make sure that it is spelled correctly.
- To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
  1. Click the Tools menu, and then click Internet Options.
  2. On the Connections tab, click LAN Settings.
  3. Select Automatically detect settings, and then...
Results:
1. You can touch 100% of protection
2. You are ready for being attacked
3. You can preserve your confidentiality
4. You can restore system here and now
5. You know why time matters
Questions?
Fighting malware on your own

May the force be with you!

Vitaliy Kamlyuk
Senior Virus Analyst
Kaspersky Lab
Vitaly.Kamluk@kaspersky.com