# **Deactivate the Rootkit**

Anibal L. Sacco

Alfredo A. Ortega







# **History:**

2004: The BIOS size of 60% of all notebooks suffered an increase of 25Kb

- Fast forward 5 years, 2009:
  - We were trying to install our own BIOS rootkit (Persistent BIOS Infection Talk, CanSecWest / Syscan)
  - Here is a very quick look of that research:





#### **Persistent BIOS Infection:**

We presented a generic technique to modify the BIOS of most common chipsets to insert malicious code in it.

This technique is applicable to any computer that supports installation of BIOS updates that are not digitally signed using cryptographically strong methods.

In the news: "Researchers unveil persistent BIOS attack" securityfocus.com

"Researchers Demo BIOS attack that survives disk wipes" - slashdot.org

"This is BS, it was discovered/created 20 years ago" - KCOp3



# **Persistent BIOS Infection:**

The only caveat is to know where to patch. We chose the 'decompression routine', because its uncompressed and easily findable using pattern matching.





#### **Persistent BIOS Infection:**

We can resume it in three easy steps:

- 1) Dump BIOS firmware using flashrom
- 2) Patch and compensate
- 3) Re-flash



# 'pre' Demo Time

We will show three different demonstrations of malicious code injected on the BIOS:

- Windows code injection (VMWARE)
- OpenBSD file attributes modification
- Real hardware demo



# **Deactivate the Rootkit:**

And... What about notebooks?

When we started to look into notebook BIOSes...

We found that there was something already there!





# What is the rootkit?

Absolute Corp. Computrace, Anti-theft agent

Option ROM Embedded in Phoenix BIOS

Agreements with law enforcement agencies.

Inside notebooks from HP, Dell, Lenovo, Toshiba, Gateway, Asus, Panasonic, and more.

Option ROM header:

00000000 55 aa 2a eb 15 43 6f 6d 70 75 54 72 61 63 65 20 |U.\*..CompuTrace | 00000010 56 38 30 2e 38 36 36 78 1d 00 e9 5c 01 50 43 49 |V80.866x...\.PCI 00000020 52 17 19 34 12 00 00 18 00 00 06 00 00 2a 00 00 |R..4.....\*..



# **Basic Inner workings:**

#### See patent application US 2006/0272020 A1





# **Basic Inner workings:**





# **Problems found:**

- Huge privacy risk (bad/no authentication)
- Anyone could activate it with enough privileges
- Anyone can change the configuration
- Anyone can de-activate it (at least in certain known cases)
- Whitelisted by AV (potentally indetectable)



#### More problems found:

Use of URL instead of IP (hosts redirection)

Configuration block modification: Demo if there is time...

Configuration block XOR 0xB5:																	
000000000	b1	b7	b5	b5	35	ab	b1	b4	b5	f5	b4	aa	b1	b5	b5	b5	5
00000010	b5	a5	bf	41	41	30	49	4e	30	30	30	30	30	95	b1	1f	AA0IN00000
00000020	ee	30	86	a0	b1	8b	b5	35	b5	ac	ae	4a	4a	4a	4a	4a	.05JJJJJ
00000030	4a	נרנרנרנרנרנרנרנר															
00000040	4a	4a	4a	4a	4a	4a	af	b4	35	ae	b3	b5	b5	b5	b5	b5	]]]]]]5
00000050	b5	a8	b7	b5	b5	f3	b3	b5	b5	b5	b5	b5	b5	f2	b3	b5	
00000060	b5	b5	b5	b5	b5	fd	af	00	50	d1	35	71	17	73	65	61	P.5q.sea
00000070	72	63	68	2e	6e	61	6d	65	71	75	65	72	79	2e	63	6f	rch.namequery.co
00000080	6d	bf	b7	b2	a5	b3	b3	ac	35	b4	b4	b5	b5	b2	b3	b5	m5
00000090	b5	b5	b5	b5	4a	98	b4	0d	98	b4	0d	9e	b1	41	54	44	JATD
000000a0	54	81	b7	38	2c	80	b7	39	2c	82	b2	39	2c	39	31	38	T8,9,9,918



# Computrace network dump

📶 dump	-computrace.pcap	p - Wireshark				
<u>Eile E</u> d	lit <u>V</u> iew <u>G</u> o <u>⊂</u> ap	pture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> el	lp			
		🖻 🛃 🗶 😂 占	् 🗢 🔿 7 👱 🛛		2, Q, 00, 🔟   🚟 🗹 🥵 %   🧱	
Eilter:			▼ Expression	<u>⊂</u> lear <u>A</u>	pply	
No. +	Time	Source	Destination	Protocol	Info	
1	5 60,440231	192,168,1,106	200.49.130.32	DNS	Standard query A search namequery.com	
1	6 60.461281	200.49.130.32	192.168.1.106	DNS	Standard query response A 209.53.113.223	
1	7 60.462498	192.168.1.106	209.53.113.223	TCP	dab-sti-c > http [sYN] seq=0 win=16384 Len=0 Mss=1460	
1	.8 60.713433	209.53.113.223	192.168.1.106	TCP	http > dab-sti-c [SYN, ACK] seq=0 Ack=1 win=16384 Len=0 MSS=1380	
	0 60.713730	192.168.1.106	209.53.113.223	ПСР НТТР	DOST / HITP/1 1	
2	1 61.088749	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
2	2 61.094166	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
2	23 61.351083	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
2	24 61.352547	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
	25 63.606194 26 63 780390	209 53 113 223	192 168 1 106		TCP Retransmission POST / HTP/1.1	
2	27 63.780436	192.168.1.106	209.53.113.223	TCP	TCP Dup ACK 25#11 dab-sti-c > http://acki.seg.s71 Ack=303 win=16258 Len=0	
2	8 63.866557	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
2	29 63.870400	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
3	30 64.139773	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
2	31 64.141114	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
3	62 64.474921 83 64 476428	192 168 1 106	200 53 113 223	HITP	POST / HTTP/1.1	
3	34 64.736404	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
3	35 64.737786	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
3	6 65.085654	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
3	37 65.087146	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
	8 66.668545	192.168.1.106 209 52 112 222	209.53.113.223	HITP	TCP Retransmission POST / HTTP/LI	
4	0 67.023603	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
4	1 67.297820	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
4	2 67.299226	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
4	3 67.636110	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
4	4 67.637562	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
4	16 67 801377	192 168 1 106	200 53 113 223	HTTP	POST / HTP/1 1	
4	7 68.250560	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
4	8 68.251961	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
4	9 68.510245	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
	0 68.511703	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
	1 68.867463	209.03.113.223	200 52 112 222	HITP	HITP/I.I 200 OK (JPEG JFIF IMage)	
5	3 69.125921	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JETE image)	
5	4 69.127355	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
5	55 69.734737	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
5	6 69.736033	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
	07 71.043219 08 71 230774	192.108.1.100 209 53 113 222	209.53.113.223	HITP		
5	9 71.233296	192.168.1.106	209.53.113.223	HTTP	Post / HTTP/1.1	
e	50 71.296482	209.53.113.223	192.168.1.106	TCP	[TCP Dup ACK 58#1] http > dab-sti-c [PSH, ACK] seg=3101 ACk=3351 win=65139 Len=0	
6	51 71.506213	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
6	52 71.507745	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
e e	3 /1.834983	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF 1mage)	-
	A ALASHASS	197 TBA I 1116	700 DK 11K 77K	ALLE		



#### **Computrace network dump**

📶 dum	o-computrace.pcap	) - Wireshark				_ [] ]
<u>Eile E</u>	dit ⊻iew <u>G</u> o <u>C</u> ap	oture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> elp				
e ë		🖻 🖬 💥 😂 占   🔍	🗢 🛸 😜 ዥ 👱		. Q. Q. 🖭   🔐 🗵 🥵 %   🔀	
Eilter:			▼ Expression	on <u>⊂</u> lear <u>A</u> pp	ply	
No. +	Time	Source	Destination	Protocol	Info	Ŀ
	15 60.440231	192.168.1.106	200.49.130.32	DNS	Standard guery A search.nameguery.com	
	16 60.461281	200.49.130.32	192.168.1.106	DNS	Standard query response A 209.53.113.223	
	17 60.462498	192.168.1.106	209.53.113.223	TCP	dab-sti-c > http [syN] seq=0 win=16384 Len=0 MSS=1460	
	18 60.713433	209.53.113.223	192.168.1.106	TCP	http > dab-sti-c [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1380	-
	19 60.713494	192.168.1.106	209.53.113.223	TCP	dab-sti-c > http [ACK] seq=1 Ack=1 win=16560 Len=0	
	20 60.713730	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
	21 61.088749	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
	22 61.094166	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
	23 61.351083	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
	24 61.352547	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1,1	
	25 63.606194	192.168.1.106	209.53.113.223	HTTP	[TCP Retransmission] POST / HTTP/1.1	
	26 63.780390	209.53.113.223	192.168.1.106	HTTP	[TCP Retransmission] HTTP/1.1 200 OK (JPEG JFIF image)	
	27 63.780436	192.108.1.106	209.53.113.223	ICP	LICP DUP ACK 25#1 0ab-sti-c > http [ACK] Seq=5/1 ACK=303 Win=16258 Len=0	
	28 63.866557	209.53.113.223	192.168.1.106	HITP	HIP/I.I 200 OK (JPEG JFIF Image)	
	29 63.870400	192.108.1.106	209.53.113.223	HITP		
	30 64.139773	209.53.113.223	192.108.1.100	HITP	HIP/I.I 200 OK (JPEG JFIF Image)	
	31 64.141114	192.108.1.100	209.03.113.223	HITP	POST / HTTP/I.I	
	32 64.474921 33 64 476439	209.33.113.223	192.108.1.100	HITP	HITP/I.I 200 OK (JPEG JFIF Image)	
	33 04.470428	192.108.1.100	209.33.113.223	HITP	PUSE / HTTP/I.I	
	34 04./30404 25 64 727796	209.33.113.223	192.108.1.100	UTTO	Post / utro /1 1	
	33 04./3//00 26 65 005654	200 52 112 222	102 168 1 106	HTTP	POSI / nTP/1.1	
	27 65 097146	107 169 1 106	200 52 112 222		DOST / UTD/1 1	
	37 03.007140	192.108.1.100	209.53.113.225		TCB Batrasmission1 DOST / HTTD/1 1	
	39 67 021574	209 52 112 222	197 168 1 106	HTTP		
	40 67 023603	192 168 1 106	209 53 113 223	HTTP	POST / HTTP/1 1	
	41 67 297820	209 53 113 223	192 168 1 106	HTTP	HTTP/1 1 200 ok (IPEG IETE image)	
	42 67 299226	192 168 1 106	209 53 113 223	HTTP	POST / HTTP/1 1	
	43 67.636110	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (1PEG 1ETE image)	
	44 67.637562	192,168,1,106	209.53.113.223	HTTP	POST / HTTP/1.1	
	45 67.889087	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JEIF image)	
	46 67.891377	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	
	47 68.250560	209.53.113.223	192.168.1.106	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)	
	48 68.251961	192.168.1.106	209.53.113.223	HTTP	POST / HTTP/1.1	

"Computrace is designed to be activated, deactivated, controlled and managed by the customer using <u>encrypted channels</u>"

http://www.absolute.com/company/pressroom/news/2009/07/refutes\_claim



📶 dump-ı	computrace.pcap	) - Wireshark				
<u>E</u> ile <u>E</u> dit	. <u>V</u> iew <u>G</u> o <u>C</u> ap	oture Analyze Statistics Hr	<u>/</u> elp			
		🕞 🖬 🗙 😂 占	Q (⇔ ⇔) 주 ⊈			2 🖭   🔐 🗵 🍓 💥   💢
Tiller av	44			i - Char A	iti	
Elicer: Jup.	addr eq 209.55.113	3.223 and ip.addr eq 192.100.1.	.106) and (tcp.port eq + Express	Ion Clear Mu		
No. +	Time	Source	Destination	Protocol	Info	
38	5 65.085654	209.53.113.223	192.168.1.106	нпр	НТТР7	1.1 200 ОК (JPEG JFIF 1Mage)
37	65.08/146	192.168.1.106	209.53.113.223	HTTP	POST	C Follow TCP Stream
31		200 53 113 223	197 168 1 106	HITP	HTTP	
40	0.67.023603	192 168.1.106	209 53.113.223	нттр	POST	Stream Content
47	1 67.297820	209.53.113.223	192.168.1.106	НТТР	HTTP	User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;)
47	2 67.299226	192.168.1.106	209.53.113.223	HTTP	POST	Host: search.nameguery.com
47	3 67.636110	209.53.113.223	192.168.1.106	HTTP	HTTP/	Content-Length: 15
44	4 67.637562	192.168.1.106	209.53.113.223	HTTP	POST	Connection: Reep-Arive
4 5	5 67.889087	209.53.113.223	192.168.1.106	HTTP	HTTP/	
46	5 67.891377	192.168.1.106	209.53.113.223	нттр	POST	
4/	/ 68.250560	209.53.113.223	192.168.1.106	HTTP	HTTP/	Server: Microsoft-IIS/6.0
40	3 68.251961	192.168.1.106	209.53.113.223	HTTP	POST	Content-Type: image/jped
49	/ 68.510245 2 68.511702	209.53.113.223	192.168.1.106	HTIP	HTTP/	Content-Length: 548
50	1 68.511703	192.108.1.100	209.33.113.223	НТТР	POST	Econection: Reep-*
57	2 68 8697405	102 168 1 106	200 52 113 223	нттр	POST	Tagit. Busices
57	2 69 125921	209 53 113,223	192 168,1,106	нттр	HTTP	· · · · · · · · · · · · · · · · · · ·
54	4 69.127355	192.168.1.106	209.53.113.223	HTTP	POST	
51	5 69.734737	209-53-113-223	192,168,1,106	<u>Н</u> ТТР	HTTP	
59	6 69.736033	192		TTP	POST	······
57	7 71.043219	192		TTP	TCP	
58	8 71.230774	209		ГТР	HTTP/	
59	a 71.233296	192		TTP	QST /	
60	0 71.296482	209				EindEinstFileA.FindNextFileA.FindCl
63	2 71.506213	209 V O				
62	2 71.507745					N····
6	/1.834983	209				Detri Detri
04	71.830435	192			TCP	Frank / 9
6/	6 73 168028	209		TTP	HTTP	User-Alla // A Commentable, Moto C All
67	7 73.169235	203			TITCP	Nost:311a/4.0 (Cumpatiple; MSIE 6.0;)
67	8 73.169381	192.168.1.106	209.53.113.223	HTTP	POST	
69	9 73.451330	209.53.113.223	192.168.1.106	HTTP	HTTP/	n - Juery.com
79	J 73.452761	192.168.1.106	209.53.113.223	HTTP	POST	EBCDIC C Hex
71	1 73.785478	209.53.113.223	192.168.1.106	HTTP	HTTP/	
72	2 73.786984	192.168.1.106	209.53.113.223	HTTP	POST	
13	3 74.038147	209.53.113.223	192.168.1.106	HTTP	HTTP/	Help
74	74.039615	192.168.1.106	209.53.113.223	HTIP	POST	
	74.406216	209.53.113.223	192.108.1.100	ные	нпруз	I.I 200 OK (SPEG SPIF Mage)
🛨 Frame	e 58 (737 by	tes on wire, 737 by#	tes captured)			
Co. Column	AND TT CHA		(00.10.05.24.06.14) (	Oct · HopHoj/	on 1 and	d.02 (00.22.40.12.dd.02)

"Computrace is designed to be activated, deactivated, controlled and managed by the customer using <u>encrypted channels</u>"

http://www.absolute.com/company/pressroom/news/2009/07/refutes\_claim

Profile: Default



🗖 dump-c	omputrace.pcap	- Wireshark					_ <b>_ _ _ _</b>					
<u>Eile E</u> dit	Eile Edit View Go Capture Analyze Statistics Help											
	≝ ≝ ≝ ≝ ≦   □ 🖬 % 🥄 占   ○, 수 💠 🎝 7 🔽   🗏 📑 🕂 O, O, O, 🗹   🚟 🛛 畅 %   🦉											
Eilter: (ip.	Eilter: (ip.addr eq 209.53.113.223 and ip.addr eq 192.168.1.106) and (tcp.port eq 💌 Expression Clear Apply											
No. +	Time	Source	Destination	Protocol	Info							
30	65.085654	209.53.113.223	192.168.1.106	HITP	HITP/1	.I 200 OK (JPEG JEIF Tmage)						
38	66.668545	192.168.1.106	209.53.113.223	HTTP	TCP	🕂 Follow TCP Stream						
39	67.021574	209.53.113.223	192.168.1.106	HTTP	HTTP/	-Stream Content						
40	67.023603	192.168.1.106	209.53.113.223	HTTP	POST	Content-Type: image/ineg						
41	67.297820	209.53.113.223	192.168.1.106	HTTP	HTTP/:	Content-Length: 13						
43	67.636110	209.53.113.223	192.168.1.106	нттр	HTTPZ	Connection: Keep-Alive						
44	67.637562	192.168.1.106	209.53.113.223	HTTP	POST	Tagin: 8028000/9						
45	67.889087	209.53.113.223	192.168.1.106	HTTP	_нттр/:	· · ·						
46	67.891377	192.168.1.106	209.53.113.223	HTTP	POST	····*··~						
47	68.251961	192.168.1.106	209.53.113.223	HTTP	POST							
49	68.510245	209.53.113.223	192.168.1.106	HTTP	HTTP/	User-Agent: MoziOft-IIS/6.0						
50	68.511703	192.168.1.106	209.53.113.223	HTTP	POST	Host: search, image (ineq						
51	. 68.867463	209.53.113.223	192.168.1.106	HTTP	HTTP/:	Connection . Image/ Jpeg						
53	69.125921	209.53.113.223	192.168.1.106	HTTP	HTTP/	cache-cochgth: 37						
54	69.127355	192.168.1.106	209.53.113.223	HTTP	POST	un: Koon_aliya						
55	69.734737	209 53 113 223	197 168 1 106	HTTP	нттр/	Lile Reep-Arrive	ilesize leile l					
56	69.736033	192		TTP	POST	eHand 05866679	oryA.;). indowsDired					
58	71.043219	209		TTP	HTTP/	Libra						
59	71.233296	192		TTP	DST .	Servi						
60	71.296482	209		<b>1</b> 0	· P	Cont W   kernel32.dll ;~						
61	71.506213	209	hmm	18	X	Eonnurro /1 1						
62	71.507745	192	′ Ⅰ Ⅰ Ⅰ Ι Ι Ι Ι Ι Ι • • •			Tagrou C/ T. T						
64	71.836453	192		TTP	JOST							
65	72.793142	192		TTP	[TCP	POST / t · Mozilla // O (compatible)						
66	73.168028	209		TTP	НТТР/	Tagid: 2. MOZITIA/4.0 (Compacible						
67	73.169235	209	200 52 112 222	EP NTTO	LTCP							
69	73.451330	209.53.113.223	192.168.1.106	HTTP	HTTP		1					
70	73.452761	192.168.1.106	209.53.113.223	HTTP	POST	Eind Save As Print	O ASCII O EBCDIC O Hex (					
71	73.785478	209.53.113.223	192.168.1.106	HTTP	нттр/:	Sptire conversation //						
72	73.786984	192.168.1.106	209.53.113.223	HTTP	POST	Hele Control Society						
74	74.039615	192.168.1.106	209.53.113.223	HTTP	POST							
75	74.406216	209.53.113.223	192.168.1.106	HTTP	НТТР/з	.I ZOU OK (JEEG JEIE IMage)						
Er ame	64 (533 hvr	es on wire 533 hvt	tes cantured)									
E Ether	net II Src	HopHaiPr 1a.dd.02	(00.23.4e.1a.dd.02)	Dst. Cisco-L	i 34.06	14 (00.10.05.34.06.14)						
Tration	net Enstand			5. 200 52 44	2 222 4							
1 une			• 1, 1	. •								
<u> </u>	Omnu	itrace is de	signed to be	activ	atec	deactivated controlled and ma	inaged					
	Joinpu		Signed to De		accu	, acactivatea, controllea ana ma	magea					
[9												
k bi	7 the C	ustomer us	sing encrypt	ed cha	nne	C"						
a Dy	by the customer using <u>enerypted channels</u>											

http://www.absolute.com/company/pressroom/news/2009/07/refutes\_claim

File: "E:\Documents and Settings\aLS\Desktop\d... Packets: 682 Displayed: 631 Marked: 0

-



📶 dump-ce	omputrace.pcap	þ - Wireshark					- 🗆 ×
<u>E</u> ile <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> ap	pture <u>A</u> nalyze <u>S</u> tatistics (	Help				
	ei 💓 💓	🖹 🖀 🗶 🔚	< < < <> < < < < < < < < < < < < < < <				
Eilter: J(ID.4	addr eq 209.53.11.	3.223 and ip.addr eq 192.166.	.1.106) and (tcp.port eq 👻 Express	on <u>C</u> lear Apr	/ply		
No. +	Time	Source	Destination	Protocol	Info		
115	90 112202	792.108.1.100	102 169 1 106	HTTD	HTTP		
116	80.113834	197 168 1 106	200 53 113 223	HTTP	POST	C Follow TCP Stream	
117	80.113034	209 53 113 223	192 168 1 106	нттр	HTTP		
118	80.443387	192 168.1.106	209 53, 113, 223	нттр	POST	Stream Content	
119	80.712933	209.53.113.223	192,168,1,106	нттр	HTTP	POST / HTTP/1.1	
120	80.715401	192,168,1,106	209, 53, 113, 223	нттр	POST	TagId: 805866679	
122	80.968795	209.53.113.223	192.168.1.106	НТТР	HTTP	Usēr-Agent: Mozilla/4.0 (compatible; MSIE 6.0;)	
123	80.970267	192.168.1.106	209.53.113.223	HTTP	POST	Host: search.namequery.com	
124	81.233453	209.53.113.223	192.168.1.106	HTTP	HTTP/	Content-Length: 31	
125	81.234928	192.168.1.106	209.53.113.223	HTTP	POST	Connection: Keep-Alive	
126	81.562939	209.53.113.223	192.168.1.106	HTTP	HTTP/	Cache-Control, no-cache	
127	81.564374	192.168.1.106	209.53.113.223	HTTP	POST	- 033.C:\WINDOWS\s	
128	81.818666	209.53.113.223	192.168.1.106	HTTP	HTTP/	server: Microsoft	
129	81.820141	192		TTP	POST	Content-Type: ir	
130	82.082689	209		TTP	HTTP/	Content-Léngth	
131	82.084159	192		TTP	POST	Connection: [K	
132	82.370182	209		TTP	NTTP/	TagId: 80586	
133	82.371645	192		TTP			
134	82.694471	209				Trong at em321wcennv.dll.l.a.~	
135	82.696100	192				hour futto	
136	82.948731	209			<u> </u>	Tadtd 8058	
137	82.950090	192		TTP	ØST /	Liser-Agent:	
138	83.302601	209		TTP	HTTP/:	Host: search.	
139	83.304015	192		TTP	POST	Content-Length	
140	83.558641	209		TTP	HTTP/:	Connection: KeepOMDATIBLE: MSIE 6.0:)	
141	83.559947	192.168.1.106	209.53.113.223	нттр	POST	Cache-Control: not reaction to the second seco	
142	83.91/06/	209.53.113.223	192.168.1.106	HTTP	HTTP/.		
143	83.919437	192.168.1.106	209.53.113.223	HTTP	POST	□ ►0 \~HTTP/1.1	
144	84.174649	209.53.113.223	192.168.1.106	HTTP	HTTP/	Server: Microsott-115/6.U	
145	84.176090	192.168.1.106	209.53.113.223	HTTP	POST	Content-Type: mage/jpeg	
140	84.531080	209.53.113.223	192.168.1.106	HTTP	HTTP/.	Concent - Lengent 25	
147	84.532499	192.168.1.106	209.53.113.223	HITP	POST		
140	84.794765	209.53.113.223	192.108.1.100	HITP	HITP/	End Start Start Disk Entry (144195 hutps)	
149	84.790220	200 52 112 222	209.03.110.220	HITP	PUST	End Save Ws Fund Chine Conversation (144102 pyces)	
151	95 149424	107 168 1 106	200 52 112 222	HTTP	POST		
152	85 416556	209 52 112 222	192 168 1 106	нттр	HTTP		
153	85 418060	197 168 1 106	209 53 113 222	нттр	POST	Help	
154	85 759939	209 53 113 223	192 168 1 106	нттр	HTTP		
1 104	05.755555	209. 33. 113. 223	192.108.1.100				
\pm Frame	136 (201 b	∧tes on wire, 201 ⊧	bytes captured)				
Ether:	net II. Src	: Cisco-Li 34:e6:1/	4 (00:1e:e5:34:e6:14). r	st: HonHaiF	pr_la:dr	1:02 (00:23:4e:1a:dd:02)	

# Clearly, at this stage, the communication channel is not encrypted at all but... What about that WCEPRV.DLL library?

00b0 30 35 38 36 36 36 37 39 0d 0a 0d 0a 7e 6c b6 1a 05866679 ....~1. File: "E:\Documents and Settings\aLS\Desktop\d... Packets: 682 Displayed: 631 Marked: 0

Profile: Default



# **Encrypted channel: Analysis**

- WCEPRV.DLL downloaded on the first run.
- Encryption algorithm: RC4 stream cipher
- Session key generated on the client
- Key Transmitted on plaintext!



And one more thing... Stub agent: Unauthenticated BIOS code execution



# Second Stage (AIM) loader, Stub Agent (DELL Vostro 1510 Computrace V 70.785)

					!! <b>'</b>	seg000:0227		mov	di, bx	
	seg000:01CF sub_1CF	proc ne	ar	; CODE XREF: sub_27F+20↓p		seg000:0229		sub	di, bp	
	seg000:01CF	push	сх			seg000:022B		shr	di, 2	
	seg000:01D0	pop	es		i i •	seg000:022E		add	di, si	
	seg000:01D1	assume	es:nothing			seg000:0230		inc	di	
	seg000:01D1	mov	si, OBFh ; '+'			seg000:0231		inc	di	
	seg000:01D4	mov	[si+6], cx			seg000:0232		cmp	di, ax	
	seg000:01D7	mov	dl, 80h ; 'Ç'		į L.	seg000:0234		jnz	short loc 1E5	
	seg000:01D9	mov	ah, 42h ; 'B'			segOOO:0236		shl	edx, 10h	
	segOOO:O1DB	int	13h	; DISK -		seg000:023Å				
	segOOO:O1DD	push	es			seg000:023A	loc_23A:			; CODE XREF: sub_1CF+A6_j
	segOOO:O1DE	pop	ds		<b></b>	seg000:023A		mov	esi, [bx]	
г-	segOOO:O1DF	jnb	short loc_1E2		•	seg000:023D		cmp	esi, 3Eh ; '>'	
	seg000:01E1					seg000:0241		ja	short locret_1E1	
	seg000:01E1 locret_1E1:			; CODE XREF: sub_1CF+1B <b>j</b> j	•	seg000:0243		shl	si, 9	
1	seg000:01E1			; sub_1CF+72 <b>↓</b> j		seg000:0246		lea	si, [si+7E00h]	
••••	seg000:01E1	retn				seg000:024A		mov	di, bx	
	seg000:01E2 ;					seg000:024C		sub	di, bp	
	seg000:01E2					seg000:024E		shr	di, 2	
i.	segOOO:O1E2 loc_1E2:			; CODE XREF: sub_1CF+10Tj	•	seg000:0251		dec	di	
<b>'</b>	seg000:01E2	xor	ecx, ecx		•	segOOO:0252		shl	di, 9	
	seg000:01E5					segOOO:0255		lea	di, [di+100h]	
	seg000:01E5 loc_1E5:			; CODE XREF: sub_1CF+2D[j	· · · ·	segOOO:0259		mov	cx, 200h	
	seg000:01E5			; sub_1CF+33 <b>_</b> j		seg000:025C				
	seg000:01E5	inc	cl			segOOO:025C	loc_25C:			; CODE XREF: sub_1CF+9F_j
	seg000:01E7	cmp	cl, 3Eh ; '>'		╏┎╼╼┿╹	seg000:025C		lodsb		
	segUUU:Ul£A	ja	short locret_1E			seg000:025D			dh, al	
	segUUU:U1EC	mov	ebx, ecx			seg000:025F		mov	ah, 8	
	segUUU:UlEr	shi	bx, 9		łi	seg000:0261				
	segUUU:U1F2	Iea	bx, [bx+7E00n]		į į į	seg000:0261	loc_261:			; CODE XREF: sub_1CF+9C <b>j</b>
	segUUU:UIF6	movzx	eax, byte ptr []	ox]	╏╏┏╼╇╹	seg000:0261		shl	dx, 1	
	seguou:01FA	cmp	al, she ; '>'			segOOO:0263		jnb	short loc_269	
		Ja	SHOLD INC INS			seg000:0265		xor	dx, 1021h	
	SEGUDU:UIFE			· CODE VDEE, out OFFICELL		segOOO:0269				
	SEGUOU:01FE 10C_1FE:			, CODE AREF: SUB_27F+3310		segOOO:0269	loc_269:			; CODE XREF: sub_1CF+94Tj
i.	329000:01FE		opy [by+4]	; DATA AREF: Sub_271+300	¦     ≯	seg000:0269		dec	ah	
	3eg000.01FE	dhe.	cax, [DXTT]		¦ į ⊷	segOOO:026B		jnz	short loc_261	
	seg000:0202	Jue	SHOLC INC IES			seg000:026D		stosb		
Ι.	80000.0204 80000.0209	ing.	short log 1E5			seg000:026E		loop	loc_25C	
	seg000.0209	cmp	eav [ebyteav#4.	141		seg000:0270		sub	bx, 4	
į .	seq000:0205	inz	short loc 1F5			segUUU:U273		cmp	bx, bp	
	seq000:0213	mosz	dx [bx+2]		L	segUU0:0275		JNZ	short loc_23A	
	seq000:0216	movzy	ehn, hyte ntr D	1x+11		seguuu:0277		shid	eax, edx, 10h	
	seq000:0218	movax	si, bn			segUUU:U27C		ຣາມວ	ax, dx	
	seq000:021D	lea	bn, [ebx+ebn#4+	41		segUUU:U27E		reth		
	seq000:0212	lea	by [eby+eay#4-	*J		seguuu:U27E	SUD_ICF	endp		
	000000222	ica	py) [chyteay.i-							



#### **Detecting the Rootkit Agent**

A single file to look for:

- system32\rpcnet.exe (Normal Agent)
- system32\rpcnetp.exe (BIOS Persistent Agent)

A service called "Remote Procedure Call (RPC) Net" with no description

Outgoing connections to search.namequery.com (209.53.113.223)

Our Computrace Option Rom Dumper tool



# **Deactivating:**

- Easiest way: hosts file redirection
- Modifying BIOS (only unsigned BIOS!)
- Modifying configuration block (Registry, hard-disk, etc.)
- Modifying nvram, then full HD Wipe.



#### The Past:



See "Implementing and Detecting a PCI Rootkit", Heasman, BlackHat 2007



#### The Future:

Phoenix Failsafe:

- Inside SMM, sounds familiar?
- Always-on OS-independent, Wifi and GPS tracking
- It has "safe" in the name instead of "trace"
- Intel Anti-theft technology:
  - vPro technology
  - Using AMT secondary processor
  - Works even with the notebook turned off!

Other security aplications residing in BIOS

Strong authentication: "Trust us, is for your own protection".



#### This is only the begginning

- More research is needed in this area!
- CoreBoot (LinuxBIOS) project, is computrace-free
- Questions?
- Thanks! Now if you'll just look into the light:

