Statistically effective protection against APT attacks

• Study on effectiveness of popular defense measures



Jarno Niemelä. Virus Bulletin 2013 Twitter: @jarnomn





Why This Research Was Made?

- Applying hardening in corporate environment is expensive
- Thus I wanted to give decision making support tools for corporate security
- In this research we evaluated popular hardening approaches against a set of exploits
- Attacks and defenses evolve constantly so we focused more on different styles of approach rather than exact settings or tools
- For tests we obviously used publicly available tools



Exploits Used In Tests

- The used exploit set consisted of ~930 confirmed exploit document samples
- Samples in the wild 2010-2013
- CVE identification was done by scan results
- Most exploits have short lifespan in active use
- APT nature verified by context identification
 - Press events, conference proceedings
 - Diplomatic/political reports, analysis
 - Human rights/activism reports, articles
 - Military reports, events, analysis
 - Business related mail





Analysis Method

- We tested samples with Windows XP SP3
 - Adobe Acrobat 8.0.0
 - Adobe Flashplayer 6.0
 - Office 2003
- We intentionally used obsolete software versions to enable as many exploits as possible
- We used automatic forensics to check for exploit success indicators
 - Network communication
 - Process creation
 - File creation
- Each exploit was verified to work consistently in base system



Protection Methods

- Application memory handling mitigations
- Application Sandboxing
- Hardening application settings
- Hardening operating system



Application Sanboxing

- Chrome, Acrobat, etc popular apps have built in sandboxing
- The problem with them is that attacker has to circumvent them in order to exploit
- Thus we wanted to test exploits against unexpected sandboxing
- We used Sandboxie 3.76 Pro with custom configuration
 - Own sandbox for each document type
 - File execution denied for any files created by sandboxed application
 - No file access outside the sandbox for Acrobat
 - Access to %documents% %recent% and network drives for Office applications



Hardened Security Settings For Client Apps

- Advisories often have mitigation instructions what to do before patch is available
- We wanted to find out how effective those measures are in general
- Who on earth needs a flash content in PDF file in the first place?

Changes to Office

- Installed Office file validation
- Installed MOICE isolation
- Set Macro security level to high
- Disabled trust on add-ons and templates

Changes to Acrobat

- Disabled opening non-PDF attachments
- Disabled trust in multimedia components
- Disabled multimedia player
- Disabled Javascript

After VB paper submission NSA came out with their Acrobat guidelines http://www.nsa.gov/ia/ files/app/Recommendations for Configuring Adobe Acrobat Reader XI in a Windows Environment.pdf



Hardened System Access Policies

- In T2 2011 we announced research pointing to that hardening breaks malware
- However APTs are quite a different beast compared to plain old malware
- We tested the samples against following hardened system settings
- Blocked file writing to roots of
 - C:\, D:\, etc, %localsettings%, %appdata%
- Blocked file writing recursively to
 - C:\windows, %program files%
- Prevented file execution from
 - C:\,%documents%, c:\RECYCLER,%temp%,%APPDATA%,%localsettings%



Application Memory Handling Mitigations

- Memory handling mitigations prevent types of memory operations needed by exploits
- Thus normal apps are mostly unhindered while exploits fail to work
- Currently only tool providing such capabilities is Microsoft EMET
 - Allocation mitigations (SEHOP, Heapspray , ASLR , Null page)
 - Code execution or loading mitigations (DEP, ROP, Bottom up rnd, EAF)
 - Hooking preventions (Deep hooks, Anti detours, Banned functions)

File Options													
Mitigations													
Al Memory ROP Other													
App Name	DEP	SEHOP	NulP	Неар	EAF	Man	Bott	LoadLib	Mem	Caller	SimE	Stac	
ACECNFLT.EXE	V		V		1		V		1				
Acrobat.exe	1	1	V	V	1	1	V	V	1	V	V	V	
Acrobat.exe	1		V	v	1		V	v	1		V	1	
Acrobat.exe	1	V	V	V	1	V	V	V	7	V	V	V	
Acrobat.exe			V	V	1		V	V	1	4	V	1	
AcroRd32.exe	1	V	V	V	1	V	V	V	1	V	V	V	
AcroRd32.exe			V	V	1		V	V	1	4	V	1	
AcroRd32.exe	1	V	V	V	1	V	V	V	1	V	V	V	
AcroRd32.exe			V	V	1		V	V	1		V	1	
AdapterTroubleshooter.exe	1	V	V	V	1	V	V	V	1	V	V	V	
AdapterTroubleshooter.exe			V	V	1		V	V	1		V	1	
addftinfo.exe	1	V	V	V	1	V	V	V	1	V	V	V	
AddInProcess.exe	9	1	4	1	1	4	V	1	1	v	V	1	
AddInProcess.exe	1	V	V	V	1	V	V	V	1	V	V	V	
AddInProcess.exe	9	1	4	1	1	4	V	1	1	v	V	1	
AddInProcess.exe	1	V	V	V	1	V	V	V	1	V	V	V	
AddInProcess.exe			V	V	1		V	V	1		V	1	
AddInProcess32.exe	1	V	V	V	1	V	V	V	1	V	V	V	
AddInProcess32.exe	9	1	4	1	1	4	V	1	1	v	V	1	
AddInProcess32.exe	1	V	V	V	1	V	V	V	1	V	V	V	٧
Add Remove													

• For this research we used Emet 4.0b which was the latest available





Application Sandboxing Results

- Unfortunately Sandboxie interfered with our automatic forensics
- We were able to get results for 452 samples with 100% protection
- Of the remaining samples we tested 60 random samples which had 100% protection
- So we cant say with full certainty, but third party sandboxing seems to be effective
- Built in payloads were dropped but not executed
- Samples which tried to download were blocked



Messages from Sandboxie	_ 🗆 X
SBIE1308 Program cannot start due to restrictions - cmd.exe [DefaultBox]	
SBIE2222 To add the program to Start/Run Access Restrictions, please double-click on this message line SBIE1308 Program cannot start due to restrictions - svohost.exe [DefaultBox] *	-1
Help Hide Close	
Copy Contents to Clipboard and Close Window	



Hardened Client Apps results

Hardening applications gave 80% total protection against exploits •

		Trust Center	and the second set of the life of the second set was set one	() ×
CVE-2010-0188 failed as not all samples were using lavaScript	CVE	Trusted Publishers Trusted Locations	Protected View Protected View opens potentially dangerous files, without any security prompt	s, in a restricted mode to help minimize
samples were dsing savascript	CVE-2004 CVE-2006	Trusted Documents Trusted App Catalogs	harm to your computer. By disabling Protected View you could be exposing yo threats. Enable Protected View for files originating from the Internet	ur computer to possible security
 CVE-2010-0188 failed as we did not think if isolating RTE files 	CVE-2006	Add-ins ActiveX Settings Macro Settings	 Enable Protected View for files located in potentially unsafe locations Enable Protected View for <u>O</u>utlook attachments 	
• CVE-2012-0158 also failed due	CVE-2008 CVE-2009 CVE-2009	Protected View Message Bar File Block Settings Privacy Options		
not isolating RTF files	CVE-2009 CVE-2010			
 In Office 2013 OFV and MOICE are b 	CVE-2010 CVE-2010 CVE-2010			
 In Acrobat the recommendations sti 	CVE-2010			
a Boador	CVE-2010			
This document contains JavaScripts. Do you want to enable JavaScripts from	CVE-2011			OK Cancel
Don't show this message again until this document is reopened		Default behavior	for web sites that are not in the above list:	ped Locations?
	CVE-2012 Grand Tota	Block access	OK Cancel	37
11 October 10, 2013 © F-Secure				Secure

Adob

Hardened System Access Policies results

- Hardened system access policies gave very small total protection of ~10%
- ~7% were partially mitigated
 - Network was blocked in 40 samples
 - Process creation blocked in 28 samples
- So in total system hardening is ineffective

	Failed:	Failed:	Failed:	
	network	file	process	
CVE	event	event	event	Success
CVE-2004-0210		1		
CVE-2006-2492			1	
CVE-2006-3590		3		
CVE-2007-5659	20		1	
CVE-2008-4841		1		
CVE-2009-0927	1			
CVE-2009-3129		159	52	8
CVE-2009-4324	3	2		4
CVE-2010-0188	294	2		
CVE-2010-0806	7	1		
CVE-2010-1297		5		
CVE-2010-2572		2	8	7
CVE-2010-2883	3	27	2	50
CVE-2010-3333	1	82	14	1
CVE-2010-3654		11	12	6
CVE-2011-0097			1	
CVE-2011-0101		4	51	13
CVE-2011-0611		19	2	
CVE-2011-1269		1		
CVE-2012-0158	15	21	7	
CVE-2012-0779	2			
Grand Total	346	341	151	89



Memory Handling Mitigations Results

	EMET was able to stop every single exploit!		failed success	
			0	1
		cve-2006-2492	0	1
•	However 4.0b is newer than samples, so results can be skewed	cve-2006-3590	0	3
		cve-2007-5659	0	21
•	There are claims that EMET can be circumvented		0	1
			0	1
	 But in our tests we could not find a sample that actually does so 		0	219
			0	9
	 Memory handling mitigations are not effective against all exploit types 		0	296
•			0	8
			0	5
	 If exploit is based on other than code execution, EMET will not help 		0	17
			0	82
	Dut such avalate as was case as drug as uld ast field is the wild as sale	cve-2010-3333	0	98
	But such exploits are very rare and we could not find in the wild sample		0	29
		cve-2011-0097	0	1
		cve-2011-0101	0	68
		cve-2011-0611	0	21
		cve-2011-1269	0	1
		cve-2012-0158	0	43
		cve-2012-0779	0	2
		Grand Total	0	927



Defence In Depth, Harden Your Network

Prevent lateral movement within your network

- Isolate everything in network, no inbound to clients no outbound from server
- Block remote execution and RDP from other than admin network segment
- Allow user to login only to his workstations

Isolate email to approved business use only

- Allow email only over company mail server
- Don't allow mail sending without user authentication

Control DNS resolution, do not allow unknown domains to resolve

• Most APT C&C infra rely on being able to resolve domain names



Make data difficult to steal

Use DRM to make stolen documents worthless

- Use rights management server to provide transparent crypto for documents
- Valid users can read documents, stolen docs are worthless outside company Watermark company browsers and check watermark in server
- Have own browser that can access only intra. Check against that in the server
- Water mark can be faked, but hard to get 100% right on the first go -> alarm Use token based email certificates and crypto for all internal mail
- Direct stealing of mail files becomes useless
- Attacker needs to decrypt messages before stealing, which slows down attack and gives you time to react



Conclusions

- With the exception of OS hardening all other methods were very effective
 - Very few attackers aim at anything but default configuration
- Which methods to use depends on what your corporate IT finds easiest to deploy
- As rule of thumb all applications that deal with external data should be hardened
- Personally I would recommend a combination of hardened application settings and EMET
- Sandboxing is also very effective but can require effort to make it transparent to users
- Most important thing to do is not to rely on a single security layer
- Our corporate security product is very good at catching exploits but no single layer is going to be enough

