RCA Name EXAMPLE: McAfee QA Failure
Report Date 4/19/2012
RCA Owner Brian Hughes - Sologic

Root Cause Analysis Report

Problem Statement

Focal Point Loss of Productivity - tens of thousands of users

When

Start Date	4/21/2010
Start Time	2pm GMT
Unique Timing	After adding detection for variants of the W32/Wecorl.a family of malware

Where

System	McAfee antivirus software for Windows XP SP3
Component	DAT File 5985
Location	Tens of thousands of end users

Actual Impact

		Cost
Customer Service	Thousands of customers impacted	
Revenue	Lost customer productivity	50,000,000.00
Other...	Due to the diversity of businesses impacted, many non financial areas could experience negative impact	
Cost	Internal costs to solve	100,000.00
Cost		
	Actual Impact Total:	$50,100,000.00

Potential Impact

Customer Service	Could have been longer	
Revenue	Could have been longer/wider	100,000,000.00
	Potential Impact Total:	$100,000,000.00

Report Summaries

Cause and Effect Summary

On 4/21/2010 at approximately 2:00PM GMT McAfee released an update to it's Virus Software Enterprise 8.7 (VSE 8.7). The update added detection for variants of the W32/Wecorl.a family of malware. The update included DAT File 5985, which contained an unidentified coding error. This error caused a healthy system file, svchost.exe, to be flagged by VSE 8.7 as being malicious. Once the file was tagged as malicious, VSE 8.7 killed the svchost.exe process. Microsoft has a built-in safety mechanism that kicks in when a system executable is killed. This safety mechanism causes the system to reboot. Upon reboot, VSE 8.7 attempted to remove the now flagged svchost.exe file, disrupting the normal operation of the system. This caused users to experience the "blue screen of death" or an endless series of attempted reboots. Tens of thousands of users were impacted causing an estimated $50 million in lost productivity.

CODING ERROR: DAT 5985 works by monitoring the memory activity of system files. The W32/Wecorl.a malware attempts to gain and maintain control of a system through the use of memory of executable system files. DAT 5985 mistakenly identified normal memory activity of svchost.exe during system startup as an attempt by malware to gain control of the system. This was due to a coding error. It is unknown why the coding error occurred, but two possible fault paths need to be examined.

1) Was there a coding execution error?
2) Was there a specification error?

Either, or both, are possible.

QUALITY SYSTEM FAILURE: McAfee's QA process missed the coding error before going into production. This error only manifests in system failure on Windows XP, Service Pack 3 (XP SP3). XP SP3 was not included in the test configuration for VSE 8.7. Also, there was no peer review of the driver completed before release. Both of these quality system failures require further examination.

Solutions

ID	Label	Description		
1	**Solution**	McAfee: Remove and replace DAT 5985		
	Cause	VSE 8.7 released to public		
	Note			
	Assigned	Choose	**Criteria**	Not Checked
	Due		**Status**	Selected
	Term	Choose	**Cost**	$0.00
2	**Solution**	McAfee: Conduct audit of DAT creation and implementation process		
	Cause	Error not discovered in McAfee QA		
	Note			
	Assigned	Choose	**Criteria**	Not Checked
	Due		**Status**	Selected
	Term	Choose	**Cost**	$0.00
3	**Solution**	McAfee: Strictly enforce rules and processes regarding DAT creation and quality assurance		
	Cause	Error not discovered in McAfee QA		
	Note			
	Assigned	Choose	**Criteria**	Not Checked
	Due		**Status**	Selected
	Term	Choose	**Cost**	$0.00
4	**Solution**	McAfee: Add missing operating systems and product configurations		
	Cause	XP SP3 with VSE 8.7 was not included in the test config		
	Note			
	Assigned	Choose	**Criteria**	Not Checked
	Due		**Status**	Selected
	Term	Choose	**Cost**	$0.00
5	**Solution**	McAfee: Leverage cloud based technologies for false remediation		
	Cause	Windows file svchost.exe flagged as 'malicious'		

	Note			
	Assigned	Choose	**Criteria**	Not Checked
	Due		**Status**	Selected
	Term	Choose	**Cost**	$0.00

6	**Solution**	McAfee: Revise risk assessment criteria		
	Cause	Windows file svchost.exe flagged as 'malicious'		
	Note			
	Assigned	Choose	**Criteria**	Not Checked
	Due		**Status**	Selected
	Term	Choose	**Cost**	$0.00

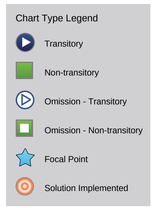
Team

ID	Label	Description	Label	Description
1	**First Name**	Brian	**Last Name**	Hughes
	Phone (1)	206-282-7703	**Phone (2)**	
	Role	Investigator	**Group**	Sologic
	Email	brian.hughes@sologic.com		
2	**First Name**	McAfee	**Last Name**	
	Phone (1)		**Phone (2)**	
	Role		**Group**	
	Email			
3	**First Name**	The Tech Herald	**Last Name**	
	Phone (1)		**Phone (2)**	
	Role		**Group**	
	Email			

Evidence

ID	Label	Description
1	**Evidence**	Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010
	Cause(s)	Update required Malicious processes are terminated by VSE VSE determined svchost.exe was malicious svchost.exe process 'killed' Standard Microsoft safety action Killing svchost.exe causes reboot Error manifests on Win XP SP3 Broadly used platform 5985 DAT examines memory useage by svchost.exe svchost.exe memory is active during startup 5985 DAT returned a false positive svchost.exe svchost.exe file was not malicious Windows file svchost.exe flagged as 'malicious' Malicious files are removed upon reboot by VSE GOTO: svchost.exe file removed attempt to remove svchost.exe svchost.exe file removed svchost.exe file required for normal operation Computers experienced continuous reboot Reboot loop renders computers unusable Large user base of VSE 8.7 + Win XP SP3 Windows XP SP3 in use Malware frequently targets memory of executables
	Location	http://www.thetechherald.com/articles/Quality-Assurance-failure-led-to-McAfee-patch-problems
	Link	
	Contributor	The Tech Herald
	Type	Web Location
	Quality	★★★★☆
2	**Evidence**	McAfee Blog Entry 4/21/2010 4:29pm
	Cause(s)	McAfee created 5985 DAT Coding error in 5985 DAT GOTO: McAfee update returned false positive
	Location	http://siblog.mcafee.com/support/mcafee-response-on-current-false-positive-issue/
	Link	

	Contributor	McAfee
	Type	Web Location
	Quality	★★★★☆
3	**Evidence**	McAfee Blog Entry 4/21/2010 11:14pm
	Cause(s)	
	Location	http://siblog.mcafee.com/support/a-long-day-at-mcafee/
	Link	
	Contributor	McAfee
	Type	Web Location
	Quality	★★★★☆
4	**Evidence**	Speculation
	Cause(s)	
	Location	
	Link	
	Contributor	Choose
	Type	Choose
	Quality	★☆☆☆☆
5	**Evidence**	McAfee FAQ List: Referenced by Tech Herald article, copy not made available
	Cause(s)	W32/Wecorl.a can be polymorphic W32/Wecorl.a found on svchost.exe in some cases Polymorphic detection required 5985 DAT detects W32 / Wecorl.a clusters Peer review of driver not completed XP SP3 with VSE 8.7 was not included in the test config Error not discovered in McAfee QA
	Location	Unknown
	Link	
	Contributor	The Tech Herald
	Type	Document
	Quality	★★★★☆



Loss of Productivity - tens of thousands of users

and or

Computers experienced continuous reboot

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

svchost.exe file required for normal operation

END

Terminated because:

Desired state

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

svchost.exe file removed

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

svchost.exe process 'killed'

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Malicious processes are terminated by VSE

END

Terminated because:

Desired state

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

VSE determined svchost.exe was malicious

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

GOTO: McAfee update returned false positive

END

Terminated because:

GO T

Evidence

McAfee Blog Entry 4/21/2010 4:29pm

McAfee created 5985 DAT

Evidence

McAfee Blog Entry 4/21/2010 4:29pm

5985 DAT detects W32 / Wecorl.a clusters

Evidence

McAfee FAQ List: Referenced by Tech Herald article, copy not made available

W32/Wecorl.a can be polymorphic

END

Terminated because:

Other causal paths more productive

Evidence

McAfee FAQ List: Referenced by Tech Herald article, copy not made available

W32/Wecorl.a found on svchost.exe in some cases

END

Terminated because:

Other causal paths more productive

Evidence

McAfee FAQ List: Referenced by Tech Herald article, copy not made available

Polymorphic detection required

END

Terminated because:

Desired state

Evidence

McAfee FAQ List: Referenced by Tech Herald article, copy not made available

Update required

END

Terminated because:

Desired state

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Killing svchost.exe causes reboot

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Standard Microsoft safety action

END

Terminated because:

Desired state

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Coding error in 5985 DAT

Evidence

McAfee Blog Entry 4/21/2010 4:29pm

Error manifests on Win XP SP3

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

? WHAT IS DIFFERENT ABOUT XP SP3 ?

5985 DAT examines memory useage by svchost.exe

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Malware frequently targets memory of executables

END

Terminated because:

Other causal paths more productive

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

svchost.exe memory is active during startup

END

Terminated because:

Other causal paths more productive

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Windows XP SP3 in use

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Broadly used platform

END

Terminated because:

Desired state

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

? WHY DID ERROR OCCUR?

and or

? EXECUTION ERROR

? SPECIFICATION ERROR ?

5985 DAT returned a false positive svchost.exe

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Windows file svchost.exe flagged as 'malicious'

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Solutions

McAfee: Leverage cloud based technologies for false remediation

Criteria Status Selected

McAfee: Revise risk assessment criteria

Criteria Status Selected

VSE 8.7 released to public

Solutions

McAfee: Remove and replace DAT 5985

Criteria Status Selected

Error not discovered in McAfee QA

Evidence

McAfee FAQ List: Referenced by Tech Herald article, copy not made available

Solutions

McAfee: Conduct audit of DAT creation and implementation process

Criteria Status Selected

McAfee: Strictly enforce rules and processes regarding DAT creation and quality assurance

Criteria Status Selected

Peer review of driver not completed

Evidence

McAfee FAQ List: Referenced by Tech Herald article, copy not made available

? WHY WASN'T PEER REVIEW DONE ?

XP SP3 with VSE 8.7 was not included in the test config

Evidence

McAfee FAQ List: Referenced by Tech Herald article, copy not made available

Solutions

McAfee: Add missing operating systems and product configurations

Criteria Status Selected

? WHY WASN'T VSE 8. TESTED WITH XP SP3

svchost.exe file was not malicious

END

Terminated because:

Other causal paths more productive

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Malicious files are removed upon reboot by VSE

END

Terminated because:

Desired state

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

attempt to remove svchost.exe

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

GOTO: svchost.exe file removed

END

Terminated because:

GOTO

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Reboot loop renders computers unusable

END

Terminated because:

Other causal paths more productive

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010

Large user base of VSE 8.7 + Win XP SP3

END

Terminated because:

Other causal paths more productive

Evidence

Article: Quality Assurance Failure Led to McAfee Patch Problems, Steve Ragan, The Tech Herald, 4/23/2010