2501 Washington Street
Midland, MI 48642, USA
info@sologic.com

Example[1] Root Cause Analysis Report

Focal Point: Loss of Productivity

Report Number: RCA 2012.430
Report Date: 04/30/2012
RCA Owner: Problem Management

Problem Statement

Focal Point Loss of Productivity

When

Date:	04/21/2010
Time:	2:00PM GMT
Unique:	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
Customers Impacted:	Tens of thousands of end users

Impact

	Actual	Potential	Cost:
Customer Service:	Thousands of customers impacted	Could have been longer	
Revenue:	Lost customer productivity	Could have been longer/wider	$50,000,000
Cost:	Internal costs to solve problem	Due to the diversity of businesses impacted, many non-financial areas could experience negative impact	$100,000
PR:	Widespread negative publicity		?
Total:			$50,100,000
Frequency:	Unknown		

[1] Note: This is an example only! All information used in this report comes from the public domain. It is intended to demonstrate the steps and format of the Sologic™ root cause analysis method and Causelink™ software. For questions or comments, please contact us at www.sologic.com

Cause and Effect Summary

On 4/21/2010 at approximately 2:00PM GMT McAfee released an update to its 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 coding specification error?

Either alternative, or a combination of both, is 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[2]

ID:	Label:	Item:
1	Cause:	VSE 8.7 released to public
	Solution:	McAfee: Remove and replace DAT 5985
	Assigned:	McAfee Team
	Due:	ASAP
	Term:	Short
	Note:	*This solution is required – but it is more classic incident management instead of problem management. This gets users back to where they were before the incident, but does nothing to keep the problem from happening again in the future.*
	Est. Cost:	Unknown at this time

[2] Note: These are solutions that McAfee reportedly developed and apparently implemented. This example is used for format only – Sologic did not provide additional solution ideas. However, we have provided commentary for each solution in the Notes field.

ID:	Label:	Item:
2	Cause:	Error not discovered in McAfee QA
	Solution:	McAfee: Conduct audit of DAT creation and implementation process
	Assigned:	McAfee Team
	Due:	ASAP
	Term:	Short
	Note:	*Conducting an audit is a different way of saying they need to investigate further. If this audit was actually conducted, the results were not made public.*
	Est. Cost:	Unknown at this time
3	Cause:	Error not discovered in McAfee QA
	Solution:	McAfee: Strictly enforce rules and processes regarding DAT creation and quality assurance
	Assigned:	McAfee Team
	Due:	ASAP
	Term:	Short
	Note:	*It would be a good idea for McAfee to understand why rules and processes were disregarded – if in fact they actually were. This is a classic surface-level solution that will have little long-term impact on risk unless additional causes are discovered.*
	Est. Cost:	Unknown at this time
4	Cause:	XP SP3 with VSE 8.7 was not included in the test config
	Solution:	McAfee: Add missing operating systems and product configurations
	Assigned:	McAfee Team
	Due:	ASAP
	Term:	Short
	Note:	*This is another example of incident management – not problem management. Unless McAfee understands exactly why the operating systems and product configurations were missing from the test protocol, this solution will do little to reduce the risk of recurrence.*
	Est. Cost:	Unknown at this time
5	Cause:	?
	Solution:	McAfee: Leverage cloud-based technologies for false remediation
	Assigned:	McAfee Team
	Due:	ASAP
	Term:	Short
	Note:	*This solution does not seem to address any identified causes. How this solution will impact future risk of recurrence is not clear.*
	Est. Cost:	Unknown at this time
	Cause:	Windows file svchost.exe flagged as 'malicious'

ID:	Label:	Item:
6		
	Solution:	McAfee: Revise risk assessment criteria
	Assigned:	McAfee Team
	Due:	ASAP
	Term:	Short
	Note:	*Again, unless McAfee determines the causes of why the risk assessment criteria were flawed, this solution will have little long-term impact on reducing the risk of future recurrence.*
	Est. Cost:	Unknown at this time

Cause boxes that are pointed on the right-hand side indicate that further investigation must be conducted to identify the causes. Explanation points indicate that the cause needs further definition, such as; evidence, cause type, termination point, or cause description.