Root Cause Analysis Report

WannaCry Ransomware Attack

Problem Statement

Report Number	Sol-0051	**RCA Facilitator**	Brian Hughes
Report Date	5/30/2017		

Focal Point: Global Impact from WannaCry malware

When

Start Date: 5/12/2017	End Date: 5/16/2017
Start Time: 7:44 AM UTC	End Time: N/A
Unique Timing	Microsoft was first notified on March 14, 2017 and issued patches, but not everyone had applied them. The National Security Agency (NSA) had previously discovered the vulnerability, but did not alert Microsoft.

Where

	Payload: DoublePulsar (developed by the NSA)
Other	EternalBlue Exploit (also known as MS17-010, developed by the NSA), targeting Windows' Server Message Block protocol. Unsupported versions of Microsoft Windows, such as XP, Server 2003, and Windows 7

Actual Impact

Customer Service	More than 230,000 computers in many major companies in over 150 countries.
Frequency	1 times Year
Frequency Note	In general, ransomware attacks are increasing.

Potential Impact

Customer Service	Could have been much worse if someone had not located a "kill switch" in the malware code.

Report Summaries

Executive Summary

READ THIS FIRST!

We need to disclose that this EXAMPLE RCA is based solely upon publicly available information from a variety of sources (mostly newspaper articles) and not from any independent investigation conducted by Sologic. Sologic has not investigated this incident in any official capacity, and we do not want to imply that we were in any way associated with this event. The only purpose of this root cause analysis report is for it to be used as an example for our students and other interested parties.

A root cause analysis has two primary goals: 1) Organize a wide array of information from disparate, reliable sources in a way that makes it easier to understand, and 2) Identify a set of evidence-based solutions to present to decision makers.

Problem Setup:

After determining the appropriate Focal Point, setting up the first level of causes is extremely important. We chose the Focal Point "Global Impact from WannaCry Malware" because it breaks down nicely into the following causes:

- Data from more than 250,000 computers in 150 countries encrypted: This cause provides us a bridge into the largest part of the analysis examining both the malware as well as how it the infection spread.
- Impact limited by "Kill Switch" activation: This branch introduces a limiting aspect to this particular event. It would have been much worse if not for this action. We often include causes at the top level that allow us the opportunity to examine the extent of the impact, whether limiting (as in this case) or exacerbating (which also happens). In either case, the cause provides value in that it completes the top-level picture and potentially identifies opportunities for solutions.

Here is how it sounds when put back into narrative form:

"The global impact from the 'WannaCry' malware attack was caused by the encryption of data from more than 250,000 computers in 150 companies with an encryption method that was nearly impossible to decode. However, the overall impact was limited by the activation of a 'kill switch' embedded in the malware."

Or something like that.

Follow along with the cause and effect chart as you read the following summary statement.

Cause and Effect Summary

On May 12, 2017 people around the world were greeted by the following splash message:

"Oops, your files have been encrypted!"

The message goes on to explain that, in order to decrypt the files, the user must send a bitcoin payment as ransom. Payment amounts started at about $300, but the message threatens to escalate the amount the longer the person

waits. There was no guarantee that paying the ransom would actually unlock the user's data. But what choice did they have? The encryption method was essentially unbreakable. So unless users had a very recent unencrypted backup, they were basically out of luck.

Many organizations were impacted, including the British National Health Service, Spain's Telefonica, Fed Ex, and Deutsche Bahn, along with thousands of other users. The hack exploited a vulnerability in Microsoft Windows, specifically an app called Server Message Block (SMB). SMB has file-sharing functionality and was intended to facilitate the easy transfer of files between users on the same network. But it also provided an unprotected pathway into the users computer.

A secretive organization called "The Equation Group", supposedly associated with the National Security Agency (NSA) found this vulnerability at some point in the past – we don't know when. Rather than give Microsoft a heads-up, the NSA kept it secret and developed offensive cyber weapons that took advantage of the vulnerability. But an outsider gained access to the files containing these weapons, and then provided them to a hacker group calling themselves "The Shadow Brokers."

The Shadow Brokers' original stated intent was to auction the Equation Group files to the highest bidder. On August 13, 2016, they posted a message with links to some sample data, along with instructions for how to bid on a password that would provide access to the entire library of files. They apparently had no takers, so on October 31, 2016 they released additional information to help stir up demand. Again, apparently no one was interested. So on November 25, 2016, they tried a third time – this time releasing screen shots of file names. And again, they got nothing. They let several months pass until April 8, 2017 when they released a password to decrypt the files they originally released months before. And finally, out of apparent frustration, on April 14, 2017, they released access to the entire library of files.

Someone (or many someone's) must have been watching the Shadow Brokers. On March 14, 2017, Microsoft began releasing patches to the fix the SMB vulnerability. But Microsoft wasn't the only one watching. After the April 14, 2017 message, someone (reportedly hackers linked to North Korea's spy agency, the Reconnaissance General Bureau) put it all together. And on May 12, 2017, they released it to the world.

How the Malware Works:

The name of the payload (the code that does the damage) is EternalBlue. EternalBlue is not exceedingly complex – it simply searches a hard drive for files, encrypts them, passes the ransom message to the user, and then propagates itself to other computers on the same network. But first, it must gain access to a vulnerable computer. It does this through the Server Message Block file transfer feature. In some cases, SMB simply allowed the payload to pass through and install itself. Remember, SMB is used on shared networks, so inbound files would be automatically trusted. In other cases, Windows would not allow software to simply load itself, but instead required proof that the user wanted the software installed. Most of us are familiar with this process – we must enter our username and password to install software. So, included with the malware was a separate file called "DoublePulsar." DoublePulsar is what is known as a backdoor application. Its purpose is to provide validation to the operating system that it's okay to load an application.

It was a 1-2 punch. SMB provided the means to transfer files to vulnerable computers, of which there were many. EternalBlue installed itself, locked up the user's data, and then propagated itself to other computers on the same network. And, if it couldn't install itself, DoublePulsar provided the validation required for the install to proceed.

The spread of this malware would have been much more extensive were it not for the actions of an employee of a web security firm. He was watching the attack take shape and was able to infect an isolated computer, thereby allowing him to examine the malware. In studying the malware code, he noticed that it utilized a web URL. It is standard protocol to attempt to purchase URLs embedded in malware. At the time, he did not realize the impact of this purchase. However, once he bought the URL, he set used it to set a "trap" to capture incoming requests. This essentially killed the spread of the malware in that it could not install or propagate to other networks.

Solutions

SO-0001	**Solution**	Improve quality testing for new software releases.		
	Cause(s)	Microsoft did not discover vulnerability until Shadow Brokers		
	Note	Had the vulnerability been discovered in QA testing, it could have been fixed prior to release. This is an admittedly generic solution - in order to be more specific, we would need more detailed information than Microsoft has released publicly.		
	Assigned		**Criteria**	Passed
	Due		**Status**	Validated
	Term	medium	**Cost**	
SO-0002	**Solution**	Take vulnerabilities into account during software architecture.		
	Cause(s)	Vulnerability exists in SMB		
	Note	SMB was developed as a feature, and features are developed in order to add value. However, there seems to have been a failure of imagination with respect to how this particular feature could be exploited. Feature architecture needs to include a rigorous, imaginative effort to identify and eliminate potential exploitable weaknesses.		
	Assigned		**Criteria**	Passed
	Due		**Status**	Validated
	Term	long	**Cost**	
SO-0003	**Solution**	Update software more frequently.		
	Cause(s)	Many users did not install the MS patch		
	Note	Everyone finds updates annoying. Apple and Microsoft are constantly pushing out updates. However, the infection by, and propagation of, this malware would have been arrested had people kept up-to-date on their software. Of course, pirated copies of software are more difficult to update, but it's hard to have sympathy for a user utilizing stolen software in the first place.		
	Assigned		**Criteria**	Passed
	Due		**Status**	Validated
	Term	medium	**Cost**	
SO-0004	**Solution**	NSA to communicate with companies when they lose assets.		
	Cause(s)	Microsoft did not discover vulnerability until Shadow Brokers		

	Note	The NSA has an obligation to communicate with companies it exploits when it loses control of the weapons it produces. This obligation is primarily owed to the American people, and secondarily to any other innocent user that could become a victim.		
	Assigned		**Criteria**	Passed
	Due		**Status**	Validated
	Term	short	**Cost**	
SO-0005	**Solution**	NSA to conduct a comprehensive review of security.		
	Cause(s)	The Shadow Brokers stole information from Equation Group		
	Note	The loss of these weapons is completely unacceptable. One article equated this theft with losing major conventional weapons, such as a Tomahawk missile. Apparently no one was killed as a result of this malware, but certainly lives were at risk and the value of data asset losses may be incalculable. The NSA must keep better control over their stockpiles.		
	Assigned		**Criteria**	Passed
	Due		**Status**	Validated
	Term	long	**Cost**	
SO-0006	**Solution**	Examine the response to develop lessons-learned report.		
	Cause(s)	Impact limited by "Kill Switch" activation		
	Note	A lot went right with this response, and maybe there were some areas where the response could have been more robust. Examine the response and distribute findings broadly so that future attacks have the best chance of being identified and mitigated.		
	Assigned		**Criteria**	Passed
	Due		**Status**	Validated
	Term	medium	**Cost**	

Team

Facilitator

Brian Hughes

206-282-7703

206-331-2569

Sr. Vice President

brian.hughes@sologic.com

Owner

Chris Eckert

989-835-3402

President

chris.eckert@sologic.com

Participants

Cory Boisoneau

cory.boisoneau@sologic.com

Jon Boisoneau

jon.boisoneau@sologic.com

Brian Hughes

206-282-7703

206-331-2569

Sr. Vice President

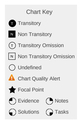
brian.hughes@sologic.com

Evidence

EV-0001	**Evidence**	"Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It," Dell Cameron, Gizmodo, May 13, 2017, 11:00am
	Cause(s)	"The Shadow Brokers" released the vulnerability Backdoor "DoublePulsar" present Corporate users often have very similar configurations Data from more than 250,000 computers in 150 countries encrypted EternalBlue abused Server Message Block (SMB) vulnerability EternalBlue auto-initiates EternalBlue payload identifies and encrypts user files EternalBlue payload installed on each individual computer EternalBlue payload runs on each individual computer EternalBlue payload spreads to other vulnerable computers EternalBlue propagated to vulnerable computers IT departments did not update when notified Large number of vulnerable computers exist Many individual users do not update every time they are notified Many users did not install the MS patch Microsoft did not discover vulnerability until Shadow Brokers Microsoft unaware of issue Microsoft began releasing patches on 3/14/2017 Multiple individual reasons... NSA develops cyber weapons NSA intended to exploit the vulnerability for its own attacks NSA knew about, but did not inform Microsoft of vulnerability Other vulnerable computers exist on same network Patch was not available to unsupported OS's SMB released to the public Server Message Block (SMB) is a network file sharing protocol The Equation Group has many offensive cyber weapons The Equation Group is affiliated with the NSA The Shadow Brokers stole information from Equation Group Users choose their own updates Vulnerability exists in SMB Vulnerability was not patched in infected machines Hackers released it along with EternalBlue SMB exploitable by DoublePulsar Some computers require authentication to install software Purpose of backdoor is to provide authentication DoublePulsar part of leaked files
	Location(s)	https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/

	Attachment(s)	
	Contributor	Brian Hughes
	Type	URL
	Quality	★★★★★
EV-0002	**Evidence**	"WannaCry ransomware that infected Telefonica and NHS hospitals is spreading aggressively, with over 50,000 attacks so far today," from Avast Software Blog.
	Cause(s)	
	Location(s)	https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today
	Attachment(s)	
	Contributor	Brian Hughes
	Type	URL
	Quality	★★★★★
EV-0003	**Evidence**	"An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak," by Thomas Fox-Brewster, Forbes, 5/12/2017
	Cause(s)	
	Location(s)	https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#ae376b8e599b
	Attachment(s)	
	Contributor	
	Type	
	Quality	★★★★★
EV-0004	**Evidence**	"How to Accidentally Stop a Global Cyber Attacks," @MalWareTech, May 13, 2017
	Cause(s)	Employee noticed the inclusion of the URL in the malware code Standard protocol - purchase URLs identified The URL was still available to purchase The original authors wanted to control the spread Checking the URL before installing is a means to control Web security firm employee purchased URL address The malware checks the URL before acting Impact limited by "Kill Switch" activation
	Location(s)	https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
	Attachment(s)	
	Contributor	Brian Hughes
	Type	URL

	Quality	★★★★★
EV-0005	**Evidence**	"The NSA has linked the WannaCry computer worm to North Korea," by Ellen Nakashima, The Washington Post, 6/14/2017
	Cause(s)	Wanted to raise cash? Wanted to cause global disruption? Malware released by hackers linked to North Korea
	Location(s)	https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.184bbb899977
	Attachment(s)	
	Contributor	Brian Hughes
	Type	URL
	Quality	★★★★☆



Global Impact from WannaCry malware

Data from more than 250,000 computers in 150 countries encrypted

EternalBlue payload runs on each individual computer

EternalBlue payload installed on each individual computer

EternalBlue abused Server Message Block (SMB) vulnerability

EternalBlue propagated to vulnerable computers

Server Message Block (SMB) is a network file sharing protocol

END

Terminated Because:

Design intent

EternalBlue auto-initiates

END

Terminated Because:

Design intent

EternalBlue payload spreads to other vulnerable computers

Other vulnerable computers exist on same network

Corporate users often have very similar configurations

END

Terminated Because:

By intent

EternalBlue payload identifies and encrypts user files

END

Terminated Because:

Design intent

Large number of vulnerable computers exist

Connects To:

a Vulnerability was not patched in infected machines

Malware released by hackers linked to North Korea

AND OR

Wanted to raise cash?

Wanted to cause global disruption?

Impact limited by "Kill Switch" activation

Solutions

Examine the response to develop lessons-learned report.

Criteria Pass Status Validated

A lot went right with this response, and maybe there were some areas where the response could have been more robust. Examine the response and distribute findings broadly so that future attacks have the best chance of being identified and mitigated.

Web security firm employee purchased URL address

Employee noticed the inclusion of the URL in the malware code

END

Terminated Because:

Desired State

Standard protocol - purchase URLs identified

END

Terminated Because:

Desired State

The URL was still available to purchase

The malware checks the URL before acting

The original authors wanted to control the spread

END

Terminated Because:

Desired State

Checking the URL before installing is a means to control

END

Terminated Because:

Desired State

b Vulnerability exists in SMB

Solutions

Take vulnerabilities into account during software architecture.

Criteria Pass Status Validated

SMB was developed as a feature, and features are developed in order to add value. However, there seems to have been a failure of imagination with respect to how this particular feature could be exploited. Feature architecture needs to include a rigorous, imaginative effort to identify and eliminate potential exploitable weaknesses.

OR

Original programming error? (Speculative)

Original programming weakness? (Speculative)

SMB released to the public

Microsoft unaware of issue

Backdoor "DoublePulsar" present

Hackers released it along with EternalBlue

Some computers require authentication to install software

END

Terminated Because:

Other causual paths more productive

Purpose of backdoor is to provide authentication

END

Terminated Because:

Other causual paths more productive

DoublePulsar part of leaked files

END

Terminated Because:

Other causual paths more productive

SMB exploitable by DoublePulsar

Connects To:

b Vulnerability exists in SMB

a Vulnerability was not patched in infected machines

Microsoft did not discover vulnerability until Shadow Brokers

Solutions

Improve quality testing for new software releases.

Criteria Pass Status Validated

Had the vulnerability been discovered in QA testing, it could have been fixed prior to release. This is an admittedly generic solution - in order to be more specific, we would need more detailed information than Microsoft has released publicly.

NSA to communicate with companies when they lose assets.

Criteria Pass Status Validated

The NSA has an obligation to communicate with companies it exploits when it loses control of the weapons it produces. This obligation is primarily owed to the American people, and secondarily to any other innocent user that could become a victim.

Microsoft began releasing patches on 3/14/2017

NSA knew about, but did not inform Microsoft of vulnerability

NSA intended to exploit the vulnerability for its own attacks

END

Terminated Because:

Other causual paths more productive

"The Shadow Brokers" released the vulnerability

The Shadow Brokers stole information from Equation Group

Solutions

NSA to conduct a comprehensive review of security.

Criteria Pass Status Validated

The loss of these weapons is completely unacceptable. One article equated this theft with losing major conventional weapons, such as a Tomahawk missile. Apparently no one was killed as a result of this malware, but certainly lives were at risk and the value of data asset losses may be incalculable. The NSA must keep better control over their stockpiles.

The Equation Group has many offensive cyber weapons

The Equation Group is affiliated with the NSA

END

Terminated Because:

Other causual paths more productive

NSA develops cyber weapons

END

Terminated Because:

Intent of agency

Weapons potentially stolen by contractor? (Speculative)

END

Terminated Because:

Separate problem

OR

Weapons accessed through a hacking operation? (Speculative)

END

Terminated Because:

Separate problem

Shadow Brokers wishes to profit by auctioning more powerful code?

Many users did not install the MS patch

Solutions

Update software more frequently.

Criteria Pass Status Validated

Everyone finds updates annoying. Apple and Microsoft are constantly pushing out updates. However, the inflection by, and propagation of, this malware would have been arrested had people kept up-to-date on their software. Of course, pirated copies of software are more difficult to update, but it's hard to have sympathy for a user utilizing stolen software in the first place.

AND OR

Patch was not available to unsupported OS's

END

Terminated Because:

Other causual paths more productive

Many individual users do not update every time they are notified

Users choose their own updates

END

Terminated Because:

Desired State

Multiple individual reasons...

END

Terminated Because:

Other causual paths more productive

IT departments did not update when notified