Spring 2017

Virus Testing Across Multiple Platforms

Ryan Ignaciuk
University of Southern Maine

Louis Hychko
University of Southern Maine

Systems Engineering
Get Ahead of IT

Virus Testing Across Multiple Platforms

Ryan Ignaciuk - Student Associate, MCSC & Louis Hychko – Student Associate, MCSC
Edward Sihler, Technical Director, MCSC

MAINE CYBER SECURITY CLUSTER

Abstract

Systems Engineering, as a value added re-seller, has noticed a number of organizations questioning the value of anti-virus / anti-malware applications in addition to native operating system protections. So the Maine Cyber Security Cluster (MCSC) at USM teamed up with Systems Engineering in Portland to find out exactly what would happen if a great deal of viruses and malware made it onto your computer that is protected with anti-virus programs they recommend to clients. We used a variety of different operating systems with an assortment of anti-virus programs. These are all either currently in use by Systems Engineering or are being considered for future distribution. During each test we injected a fixed amount of viruses and malware on each system upon which we found varying effectiveness. The focus of this testing was to provide the end user the most effective anti-virus program pared with their operating system.

Background

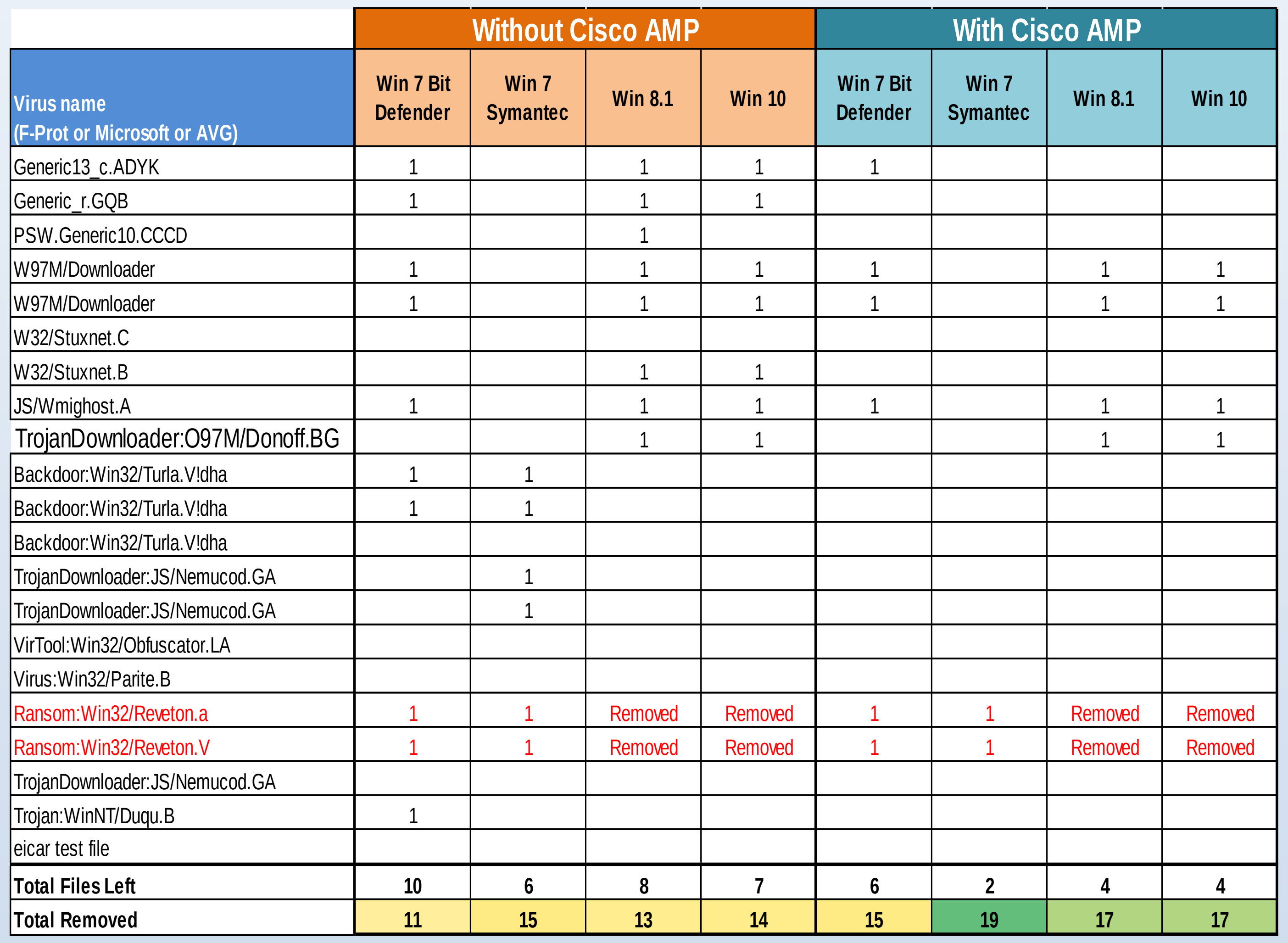
With the rush of "advanced malware" protection products to the market, due to the overwhelming threat, it was important to separate hope from reality. This is of particular importance for the product System Engineering is going to market with at this time, Cisco AMP for Endpoints. We performed the test of exposing a variety of Windows OS, Anti-Virus software and Cisco AMP to a payload of viruses and malware.

Objective

The purpose of these tests were to (1) define a process which could provide repeatable results for evaluating the effectiveness of anti-malware/virus solutions and (2) to determine to what extent Cisco AMP for Endpoints made a measurable difference in protecting the end-point from infection and/or exploitation.

Test Procedure

The first set of tests were against quiescent files on a USB drive. This test Virtual Machine was to connected a USB drive containing these files and monitor to see how many of the malware files were found without doing anything else (Figure 2 – Test Environment). The second test consisted of starting a manual scan of the USB drive and monitoring to see how many more of the malware files were found and/or removed (Figure 3 – Virus Detection). A final ransomware specific test was to open one of the two recent ransom ware variants on the "Win 7/Bit Defender/AMP" VM to see how AMP would respond.



	Without Cisco AMP				With Cisco AMP			
Virus name (F-Prot or Microsoft or AVG)	Win 7 Bit Defender	Win 7 Symantec	Win 8.1	Win 10	Win 7 Bit Defender	Win 7 Symantec	Win 8.1	Win 10
Generic13_c.ADYK	1		1	1	1			
Generic_r.GQB	1		1	1				
PSW.Generic10.CCCD			1					
W97M/Downloader	1		1	1	1		1	1
W97M/Downloader	1		1	1	1		1	1
W32/Stuxnet.C								
W32/Stuxnet.B			1	1				
JS/Wmighost.A	1		1	1	1		1	1
TrojanDownloader:O97M/Donoff.BG			1	1			1	1
Backdoor:Win32/Turla.V!dha	1	1						
Backdoor:Win32/Turla.V!dha	1	1						
Backdoor:Win32/Turla.V!dha								
TrojanDownloader:JS/Nemucod.GA		1						
TrojanDownloader:JS/Nemucod.GA		1						
VirTool:Win32/Obfuscator.LA								
Virus:Win32/Parite.B								
Ransom:Win32/Reveton.a	1	1	Removed	Removed	1	1	Removed	Removed
Ransom:Win32/Reveton.V	1	1	Removed	Removed	1	1	Removed	Removed
TrojanDownloader:JS/Nemucod.GA								
Trojan:WinNT/Duqu.B	1							
eicar test file								
Total Files Left	**10**	**6**	**8**	**7**	**6**	**2**	**4**	**4**
Total Removed	**11**	**15**	**13**	**14**	**15**	**19**	**17**	**17**

Figure 1. Virus Removal Table

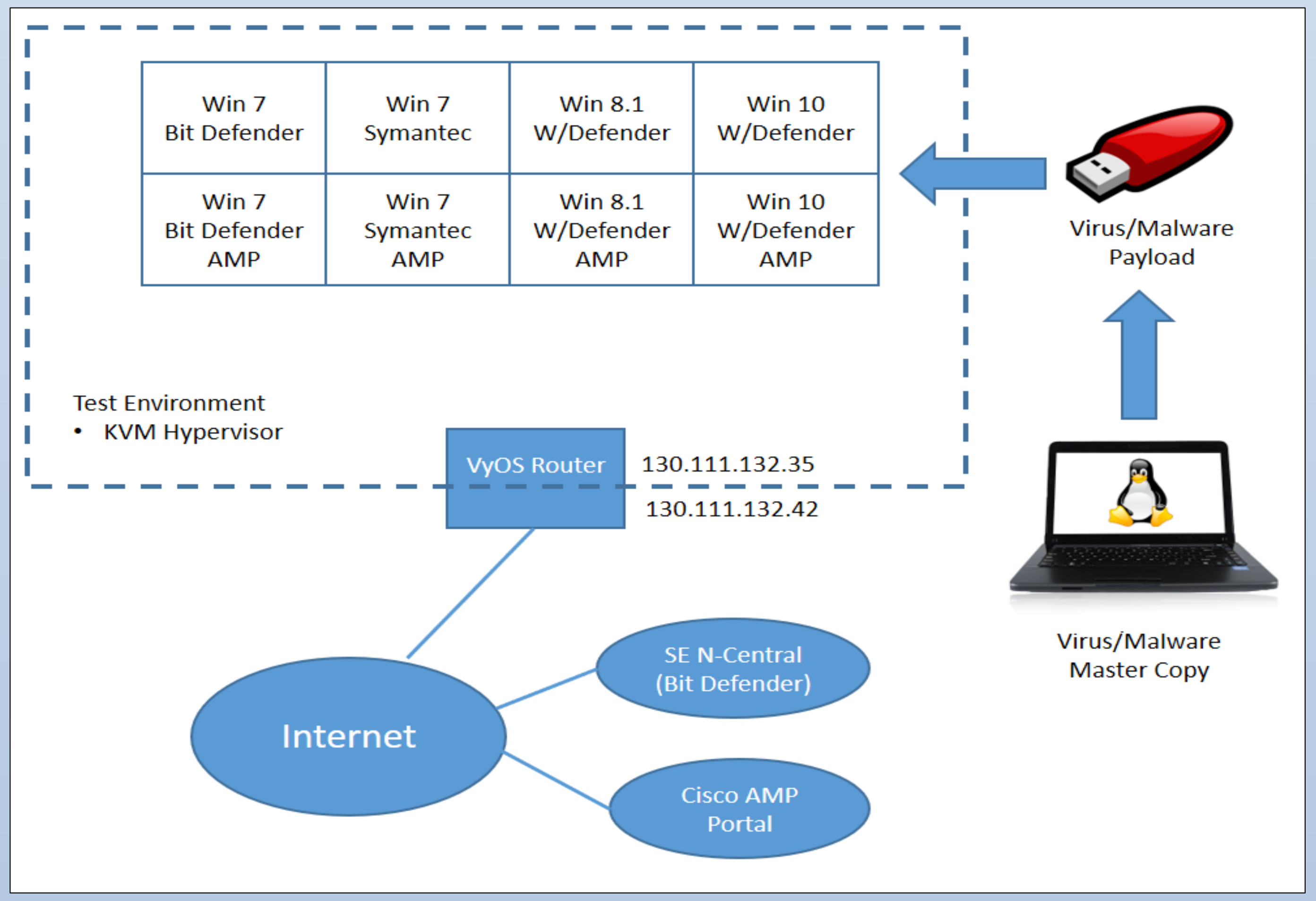


Figure 2. Test Environment

When Detected	Win 7 Bit Defender	Win 7 Symantec	Win 10 Win/Defender
Standalone			
On Inspection	10	16	18
After Scan	10	6	7
With Cisco AMP			
On Inspection	10	16	18
After Scan	6	2	4

Figure 3. Virus Detection

Results

Overall fewer files remained after running the AMP for Endpoints scan, which would indicate that files would also be scanned and removed upon a user attempting to open. Bit Defender conflicted with the scanning by AMP and likely effected results. (Figure 1 – Virus Removal Table)

Conclusions

There was measurable improvement, in most cases, where AMP was combined with the existing endpoint protection leaving as few as 2 files but no combination removed 100% of threats. Tuning of the existing AV solution to work with AMP will be an essential part of any deployment and setting the expectation that AMP for Endpoints is one more layer with additional forensic capabilities which will help with any required remediation.

There were issues where AMP and Bit Defender were each was wrestling for access to quarantined files. We'll need to research the scan and automatic protection exclusions a little further to prevent that.

Of note, the only solution that removed the two ransomware files was Windows 8.1 and Windows 10 with the built-in Windows Defender anti-virus, see Figure 1 – Virus Removal Table

Next Steps

Systems Engineering is proposing Cisco AMP for Endpoints, they must first set the exception that this, like all malware protection solutions, is not going to stop 100% of the threats. It will further mitigate risk and is expected to provide good forensic data as to which endpoints were affected in the case of an attack.

Systems Engineering has determined they will need to revisit Windows 10 and AMP combination in the near future to see if they will make a firm recommendation that greatest protection and value is to use Windows Defender with AMP for its clients.

Acknowledgements:
Thank you Systems Engineering for allowing the MCSC to participate by conducting your virus testing and providing us with your software to implement these tests. A big thanks to our mentor and Technical Director Edward Sihler of the MCSC for the opportunity to work on this project and allowing us the space and resources needed along with the rest of the MCSC staff.

References

Systems Engineering Virus Testing (Hychko & Iggnaciuk, 2016)
Benton, Mark. Cisco AMP for Endpoints lab Test

UNIVERSITY OF SOUTHERN MAINE
PORTLAND • GORHAM • LEWISTON • ONLINE