Cisco Advanced Malware Protection (AMP) for Endpoints Security Testing

7 September 2018

DR180821E

Miercom.com

www.miercom.com

Contents

1.0 Executive Summary

When there are thousands of nodes in a network, finding malware can be daunting. Administrators use layers of security for handling defense - intelligence, sandboxing, quarantining. But an evolving threat landscape leads eventually leads to ineffective and isolated security solutions.

Cisco Advanced Malware Protection (AMP) offers an integrated, comprehensive approach to endpoint security. Continuous analysis and telemetry features keep its finger on the pulse of network anomalies, and all suspicious activity is investigated. Contextual reporting highlights trends for administers, helping them reassess network architecture to close vulnerable points of entry. Also important is its flexible deployment, which makes it simple for any organization to tailor its endpoint security.

Cisco Systems, Inc. engaged Miercom to perform a performance assessment of its AMP solution for endpoints using real world threats, such as Locky ransomware and Kovter malware, in a simulated enterprise environment. The threats were introduced in a series of phases to determine if AMP security could identify a threat at any time during exploit execution to show whether it could protect even if one or more defense mechanisms were bypassed.

Key Findings

- **Metasploit malicious document detected and quarantined with full protection enabled**
- **Kovter malware detected and blocked with full protection enabled, with behavioral-only protection and during post-infection mitigation**
- **Locky ransomware was blocked with either full or behavioral-only protection enabled**
- **Retrospection engine provides insightful detection and response capabilities**
- **Mimikatz Rubber Ducky exploit detected and blocked with either full or behavioral-only protection enabled**

Based on our observations, Cisco Advanced Malware Protection successfully demonstrated detection and response capabilities for several malware use cases. Its impressive security against real-world exploits earn the Cisco AMP solution the ***Miercom Performance Verified*** certification.

Robert Smithers

CEO

Miercom

2.0 Test Summary

Table 1: Component Security Status

Run	Metasploit Malicious Document	Kovter Malware	Locky Ransomware	Retrospection Malware	Mimikatz Rubber Ducky Delivery (Win7 Only)
1	Pass	Pass	Pass	Pass	Pass
2	Pass	Pass	Pass		Pass
3	Marginal Pass; While detecting the exploit, AMP did not see the Meterpreter instance in memory	Pass	N/A; cannot detect encrypted artifacts	Detected samples are added to the database and blocked	N/A; no artifacts to detect

3.0 Product Tested

Cisco Advanced Malware Protection (AMP) provides next generation security for endpoints against evolving threats. This solution offers the following endpoint security defenses:

Prevention	This first line of defense equips the network with global threat intelligence, behavioral detection, vulnerability detection and built-in sandboxing.
Impressive Time-to-Detection	Instead of the typical 100-day detection, Cisco AMP identifies threats within hours. By using continuous analysis, telemetry and prioritization, any potential or existing breaches are quickly found for easy remediation.
Integrated Security Architecture	Many security analysts must balance multiple tools to carry out security across the network. Cisco AMP integrates security for faster detection by using cloud-based technology and correlated threat intelligence by monitoring data across all network nodes.
Flexible Deployment	Sometimes endpoint security requires restructuring the network architecture. Cisco AMP gives deployment options for cloud or on-premise use and protection for any type of endpoint, regardless of operating system. This flexibility allows organizations to setup endpoint security in a way that makes sense to their operations.
Comprehensive Analytics	Cisco AMP can identify patterns and Indicators of Compromise (IoC) with continuous detection – even after initial prevention. This approach includes other features such as: • Retrospective Detection – automatically detect and block malicious activity which evaded initial detection • File Trajectory – view file propagation for improved visibility to reduce time-to-detection • Elastic Search – search across telemetry and global security intelligence for contextual understanding of potential threats • Device Trajectory – displays continuous endpoint even history to strengthen security intelligence for better vulnerability and threat detection • Prevalence – reveals previous, undetected threats across all endpoints and automatically prevents them from affecting the broader network • Outbreak Control – contain suspicious files or infections for immediate remediation
Contextual Reporting	Actionable dashboards go beyond point-in-time technology by providing context and prioritization while highlighting trends specific to the environment.

4.0 How We Did It

Miercom evaluated the Cisco AMP solution by subjecting protected endpoints to its proprietary malware suite and different types of exploits during different phases of protection.

Exploit tests were performed in a series of three runs:

1. Run exploit with full protection enabled
2. Run exploit with signature-based (behavioral) detection mechanisms in audit mode to test the behavioral engine
3. Run exploit without Cisco AMP security enabled, then activate protection, to determine if previous detection artifacts are found and mitigated

The following threats were used:

- Metasploit Word Document
- Kovter Malware
  Locky Ransomware
- Retrospection Targeted Malware
- Mimikatz Rubber Ducky Delivery (Windows 7 Only)

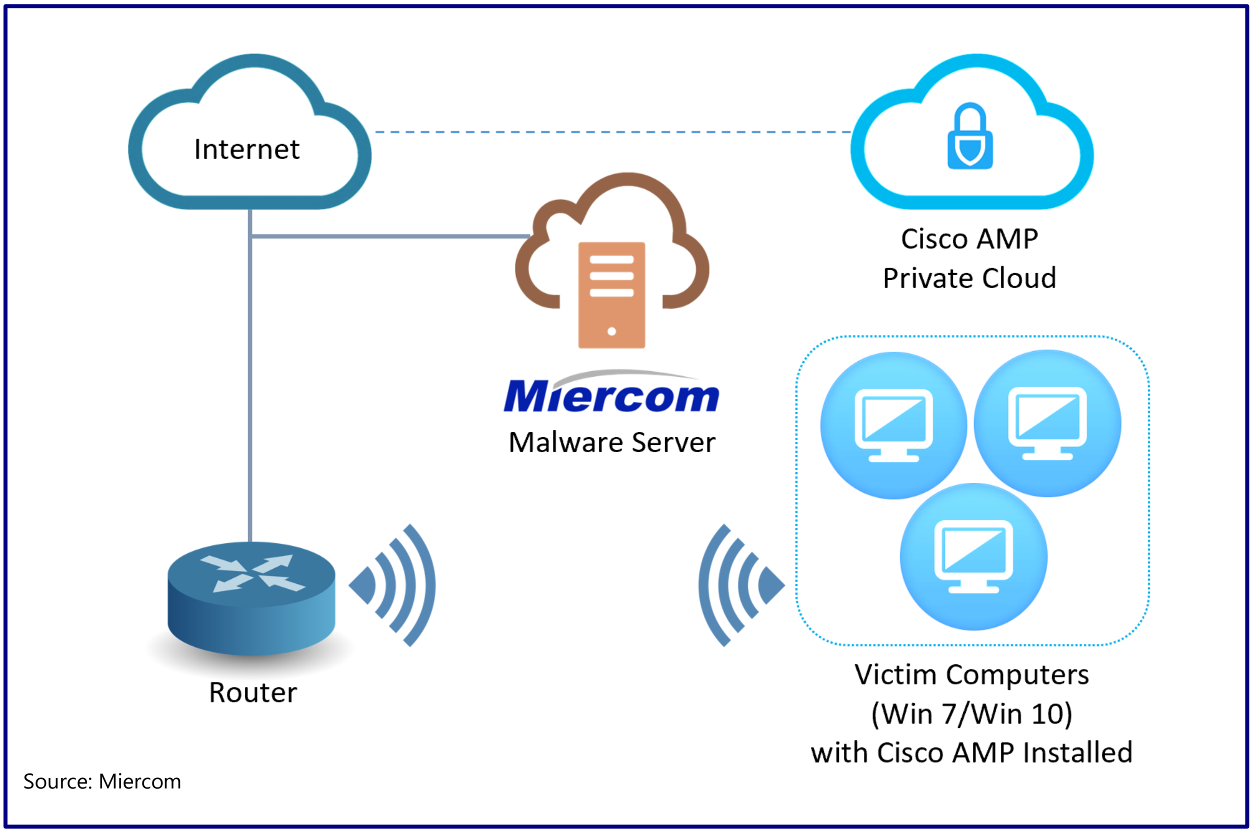
4.1 Test Environment

Test Tools

Firebind
ixia | A Keysight Business
NMAP
SPIRENT Communications
Nessus vulnerability scanner
metasploit
idappcom
KALI LINUX
savvius Omnipeek
THC Hydra
Wireshark

Source: Miercom

Cisco AMP Cloud



Source: Miercom

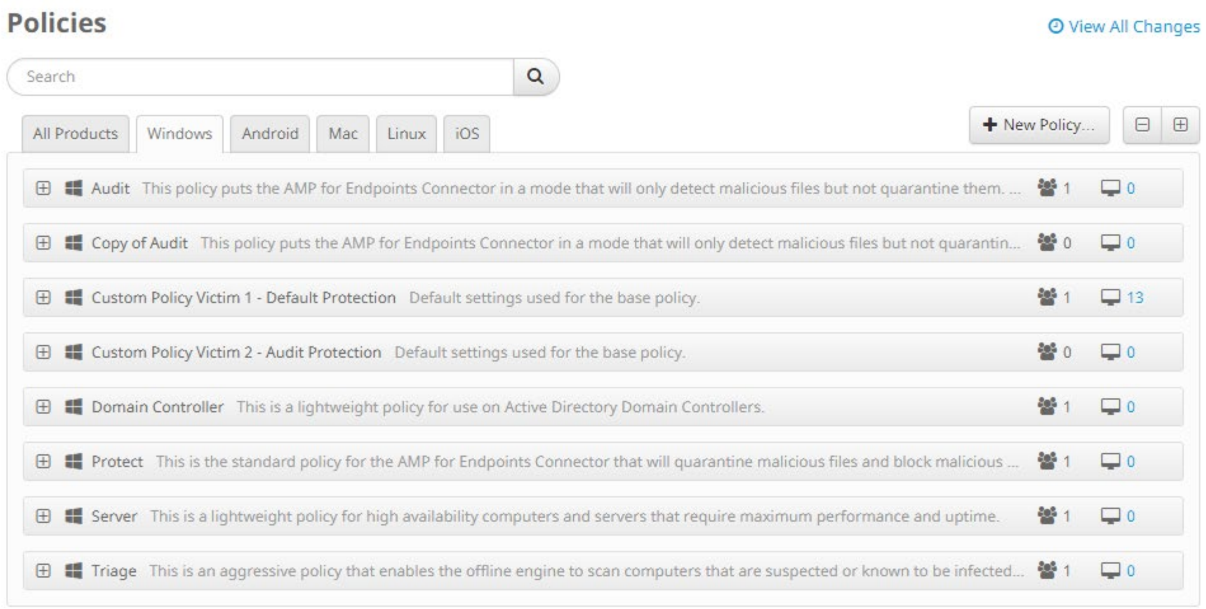
Connector Setup

The setup for Cisco AMP is very simple. It uses a single executable, run on the client, which links to the AMP cloud console. The computer information is automatically set up, and the proper policy is downloaded. This setup can be altered from the cloud at any time and will be updated on the client upon the next update.

Cloud Interface Options and Control

In the cloud interface, the default policies can be adjusted very easily. A screenshot of the policy page is shown below.

Figure 1: Cisco AMP Cloud Interface Policy Page



Audit	This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ...	1	0
Copy of Audit	This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantin...	0	0
Custom Policy Victim 1 - Default Protection	Default settings used for the base policy.	1	13
Custom Policy Victim 2 - Audit Protection	Default settings used for the base policy.	0	0
Domain Controller	This is a lightweight policy for use on Active Directory Domain Controllers.	1	0
Protect	This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ...	1	0
Server	This is a lightweight policy for high availability computers and servers that require maximum performance and uptime.	1	0
Triage	This is an aggressive policy that enables the offline engine to scan computers that are suspected or known to be infected...	1	0

Source: Miercom

Two custom policies were used in testing: default protection and audit protection. These policies are slightly altered versions of the "Protect" and "Audit" policies. The main alterations are for user feedback. By default, AMP hides many detailed alerts from the resident client to prevent confusion for a non-administrative user. In this test case, all local alerts were enabled to obtain instant feedback on the victim device.

Configuration

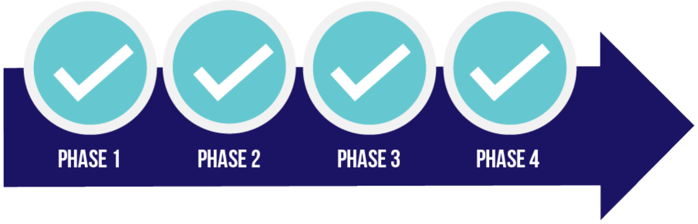
Installation and configuration consisted of cloning and altering the Protect Policy, downloading and installing the AMP endpoint application, and waiting for successful sync.

5.0 Test Cases

5.1 Locky Ransomware

The Locky ransomware test case demonstrates the behavioral detection engine of the AMP product. The attack contains multiple stages, starting from a malicious word document and ending with the victim's files encrypted via Locky malware.

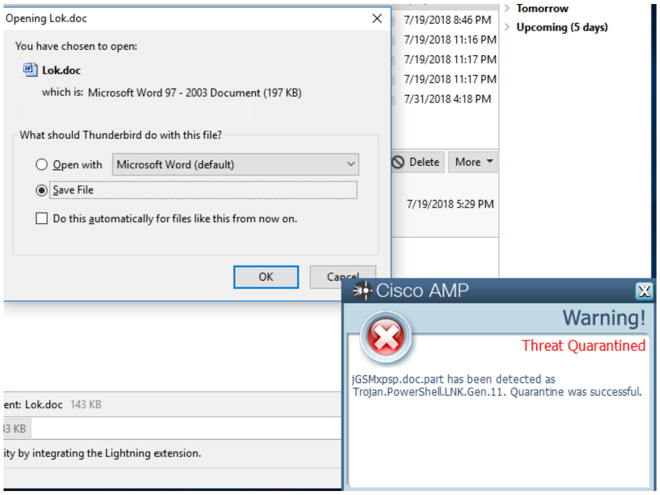
Attack phases include the retrieval of the malicious document as an email attachment, opening and execution of the infected word document, spawning of Locky ransomware, and finally the encryption of the victim. These four phases of attack are assessed for detection and blocking capabilities of Cisco AMP. The ability to detect through each phase is depicted below.



Phase 1: Initial Malware Download

In this phase, AMP blocked the download of the malicious document associated with the initial infection. A screenshot of the AMP application blocking the attempted retrieval of the malicious attachment can be seen below.

Figure 2: Malicious Document Download Detection and Quarantine



Opening Lok.doc

You have chosen to open:

Lok.doc

which is: Microsoft Word 97 - 2003 Document (197 KB)

What should Thunderbird do with this file?

○ Open with Microsoft Word (default)

● Save File

□ Do this automatically for files like this from now on.

Cisco AMP

Warning!

Threat Quarantined

jGSMxpsp.doc.part has been detected as Trojan.PowerShell.LNK.Gen.11. Quarantine was successful.

ent: Lok.doc 143 KB

ity by integrating the Lightning extension.

Source: Miercom

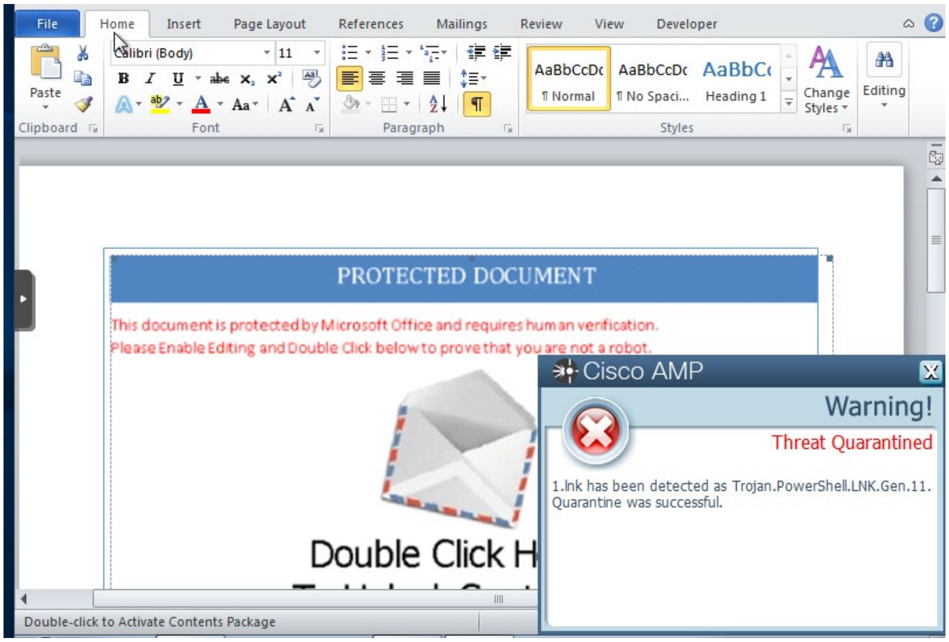
The malicious Word document was detected during attempted retrieval from the infected email. AMP successfully quarantined the document.

Phase 2: Malware Execution

After confirming Cisco AMP's ability to detect the malicious file download, AMP was disabled, and the file was transferred onto the computer. This simulated the event in which a file has managed to bypass the protection and is resident on the victim computer. Once the file was saved, AMP was reenabled and the file was attempted to be opened and run.

In this case, upon opening the Word document, the malicious content was detected and blocked.

Figure 3: Detection and Quarantine of Malicious Word Document Execution



PROTECTED DOCUMENT

This document is protected by Microsoft Office and requires human verification.
Please Enable Editing and Double Click below to prove that you are not a robot.

Double Click H

Double-click to Activate Contents Package

Cisco AMP

Warning!

Threat Quarantined

1.lnk has been detected as Trojan.PowerShell.LNK.Gen.11.
Quarantine was successful.

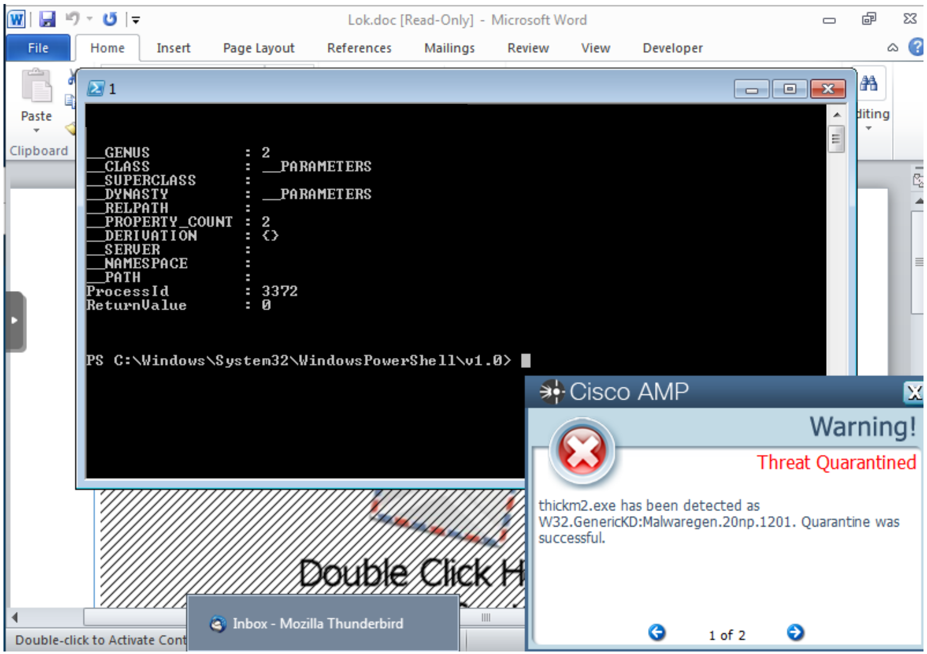
Source: Miercom

Malicious content was detected upon opening the Word document, and it was quarantined before the user could activate it.

Phase 3: Locky Ransomware Spawning

If the executed infection was not detected, the malicious content in the Word document spawned another process to begin encrypting the computer's files.

Figure 4: Successful Protection from Locky Ransomware



```
__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 2
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
ProcessId        : 3372
ReturnValue      : 0


PS C:\Windows\System32\WindowsPowerShell\v1.0>
```

thickm2.exe has been detected as W32.GenericKD:Malwaregen.20np.1201. Quarantine was successful.

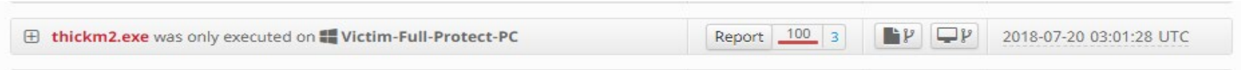
Source: Miercom

The attempted execution of the Locky ransomware sample was successfully detected and prevented from running.

Phase 4: Victim Encryption

Lastly, if this executable was not detected, the victim computer would be encrypted. For the malware to get to this point in the process, the AMP product was disabled, reenabled and the malware was run as in the previous cases. This case is only applicable to the first run of this exploit. This version of the malware had not been previously seen and became a great example of the retrospection engine's capabilities. Malware signatures were detected and logged.

Figure 5: Retrospection Engine: Detected Malware Log Entry



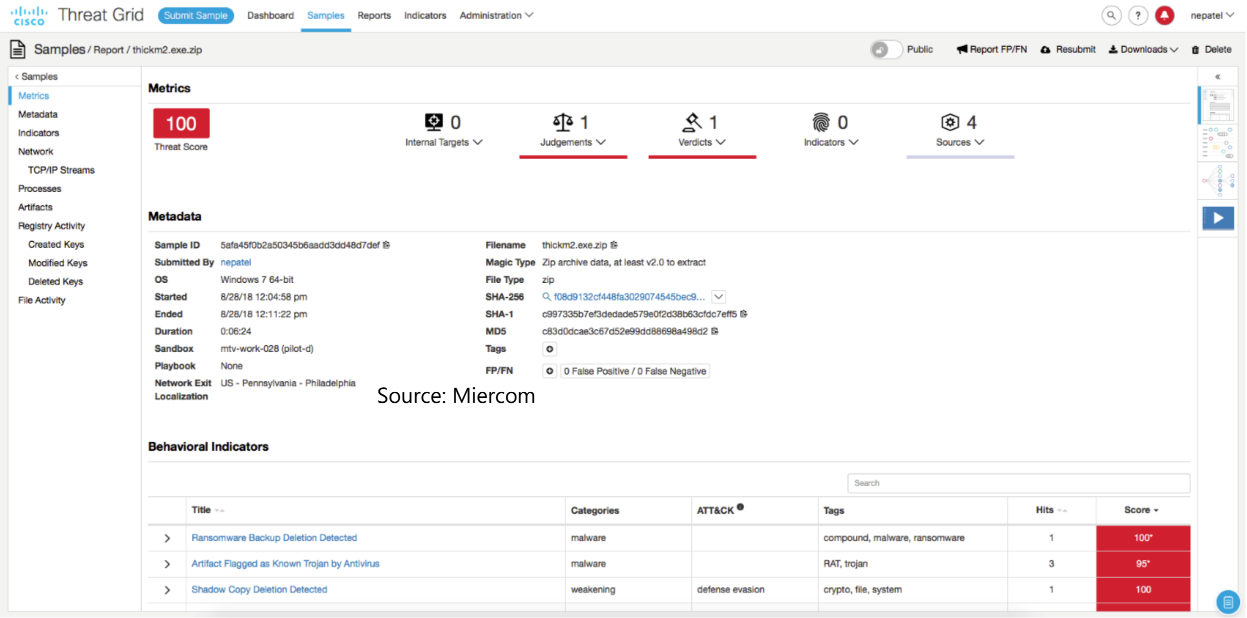
⊞ thickm2.exe was only executed on Victim-Full-Protect-PC | Report | 100 | 3 | 2018-07-20 03:01:28 UTC

Source: Miercom

The log entry of retrospection detection was seen in the AMP cloud interface. The executable was marked as malicious with 100 percent confidence. Upon creation of this entry, the exploit scenario no longer worked and would be stopped at any of the above phases before for the computer had been encrypted.

The detection of the executable also can be further analyzed using the report link that can be seen in the screenshot above. This link will provide the end user with the Threat Grid Analysis Report. This report lists the behavioral indicators along with traffic analysis, linked processes analysis, artifact analysis, registry activity, and filesystem analysis.

Figure 6: Cisco AMP Threat Grid Analysis Report



Metrics

100 Threat Score

0 Internal Targets

1 Judgements

1 Verdicts

0 Indicators

4 Sources

Metadata

Sample ID	5afa45f0b2a50345b6aadd3dd48d7def	Filename	thickm2.exe.zip
Submitted By	nepatel	Magic Type	Zip archive data, at least v2.0 to extract
OS	Windows 7 64-bit	File Type	zip
Started	8/28/18 12:04:58 pm	SHA-256	f08d9132cf448fa3029074545bec9...
Ended	8/28/18 12:11:22 pm	SHA-1	c997335b7ef3dedade579e0f2d38b63cfdc7eff5
Duration	0:06:24	MD5	c83d0dcae3c67d52e99dd88698a498d2
Sandbox	mtv-work-028 (pilot-d)	Tags	
Playbook	None	FP/FN	0 False Positive / 0 False Negative
Network Exit Localization	US - Pennsylvania - Philadelphia		

Source: Miercom

Behavioral Indicators

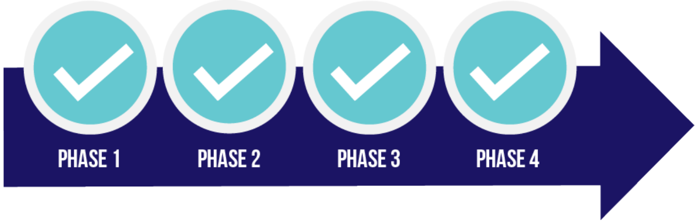
Search

	Title	Categories	ATT&CK	Tags	Hits	Score
›	Ransomware Backup Deletion Detected	malware		compound, malware, ransomware	1	100*
›	Artifact Flagged as Known Trojan by Antivirus	malware		RAT, trojan	3	95*
›	Shadow Copy Deletion Detected	weakening	defense evasion	crypto, file, system	1	100

The Threat Grid analysis was provided when investigating flagged malware by the retrospection engine. The behavioral aspects that mark the sample as malicious can be seen in red.

5.2 Kovter Exploit

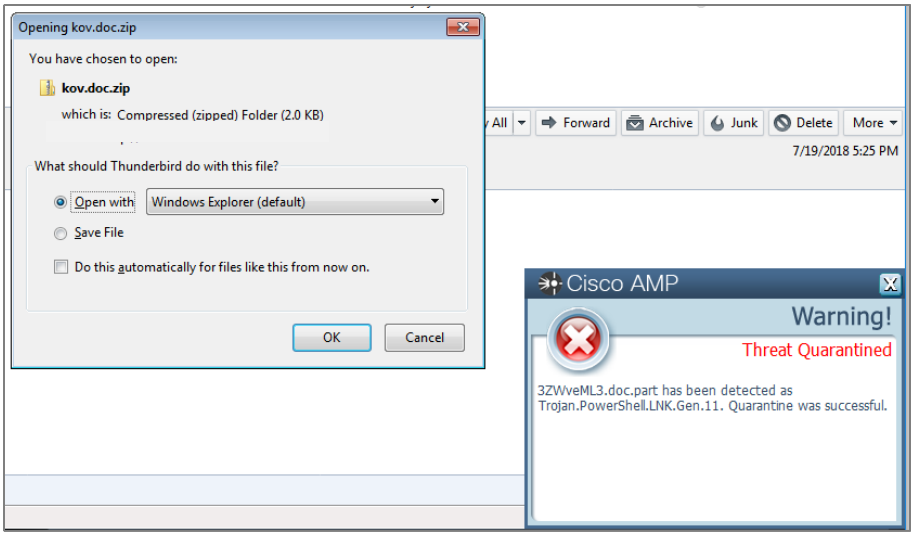
This test case utilized a malicious JavaScript that spawned an infection resulting in the Kovter malware to establish fileless persistence on the victim computer. Phases of the attack included the initial execution of the obfuscated JavaScript, the retrieval and execution of a secondary piece of JavaScript that fetches and implements the malware, the execution of the malware, and the establishment of the fileless persistence on the victim machine. A summary of successful detection for each of the four phases can be seen in the graphic below.



Phase 1: Malicious JavaScript Execution

In the first phase of the Kovter attack scenario, the malicious JavaScript attempted to be executed. This JavaScript should be detected and blocked upon attempted execution. This file simulated a JavaScript that utilizes a ".doc" extension before the ".js" extension to fool the end user into believing they were opening a document, not running a malicious JavaScript.

Figure 7: Detection of Initial Malicious JavaScript



Opening kov.doc.zip

You have chosen to open:

kov.doc.zip

which is: Compressed (zipped) Folder (2.0 KB)

What should Thunderbird do with this file?

● Open with Windows Explorer (default)

○ Save File

□ Do this automatically for files like this from now on.

7/19/2018 5:25 PM

Cisco AMP

Warning!

Threat Quarantined

3ZWveML3.doc.part has been detected as Trojan.PowerShell.LNK.Gen.11. Quarantine was successful.

Source: Miercom

The initial malicious JavaScript was successfully detected and quarantined.

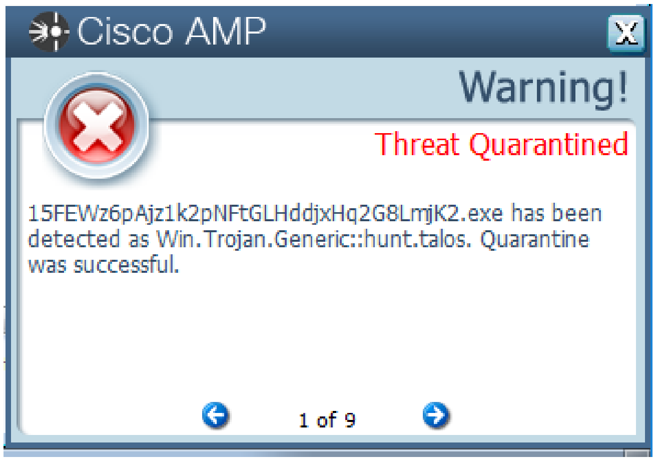
Source: Miercom

Phase 2: Secondary JavaScript Fetch to Initiate Kovter Malware

If the initial malicious file went undetected by the initial scan, the user would then attempt to open the document which in turn executes the JavaScript. Upon execution, the script fetched a second script into memory and executed it. The second JavaScript downloaded the Kovter malware and attempted to execute it.

The attempted downloads were successfully found and quarantined in this instance.

Figure 8: Successful Quarantine of Embedded JavaScript



Cisco AMP

Warning!

Threat Quarantined

15FEWz6pAjz1k2pNFtGLHddjxHq2G8LmjK2.exe has been detected as Win.Trojan.Generic::hunt.talos. Quarantine was successful.

1 of 9

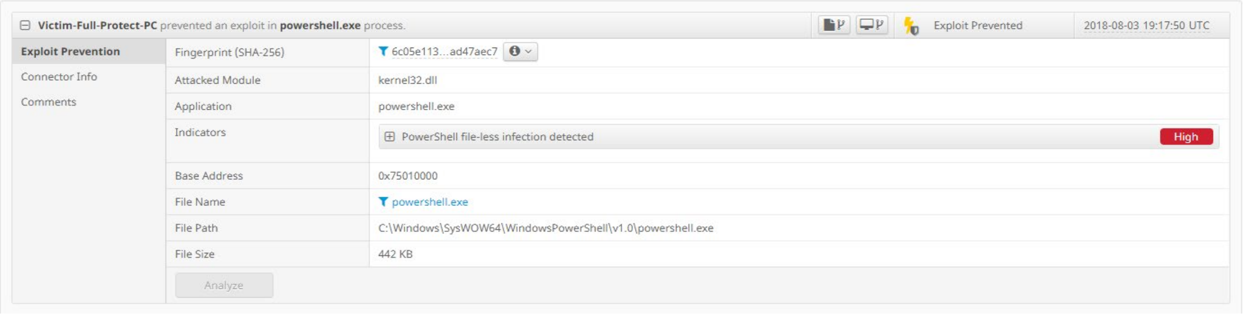
Source: Miercom

A quarantine alert was generated when the second phase of the Kovter test case was executed.

Phase 3: Kovter Malware Execution

In the third phase of the infection, the malware was executed to create fileless persistence on the victim machine. AMP was disabled to get the malware onto the computer. After reenabling AMP, the malware was run, and the attack was prevented. In this case, AMP detected the malicious utilization of PowerShell and killed the process; the attack was stopped.

Figure 9: Cisco AMP Cloud Interface Alert of Prevented Kovter Exploit



⊟ **Victim-Full-Protect-PC** prevented an exploit in **powershell.exe** process. | Exploit Prevented | 2018-08-03 19:17:50 UTC

Exploit Prevention

Connector Info

Comments

Fingerprint (SHA-256)	6c05e113...ad47aec7
Attacked Module	kernel32.dll
Application	powershell.exe
Indicators	⊞ PowerShell file-less infection detected High
Base Address	0x75010000
File Name	powershell.exe
File Path	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Size	442 KB

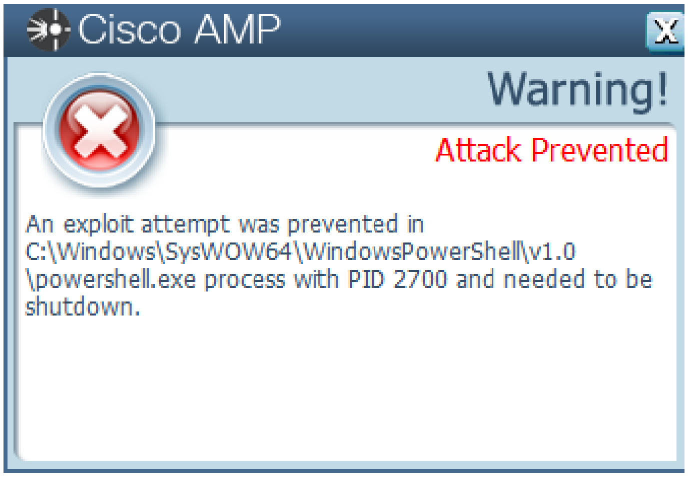
Source: Miercom

The alert shown above was produced by the AMP cloud interface when the exploit was prevented. AMP detected the use of PowerShell to establish a fileless infection.

Phase 4: Kovter Malware Establishment of Fileless Persistence

In the final phase, the malware was installed on the victim without AMP active. The victim was rebooted, and the malware attempted to launch via fileless persistence on the unprotected victim. AMP was then reactivated, and the malware tried to reinitialize itself. AMP detected this persistence attempt and quarantined associated items to block the attack. This persistence was detected when a PowerShell exploit attempted to initialize the malware.

Figure 10: Successful Block of Kovter PowerShell



An exploit attempt was prevented in C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe process with PID 2700 and needed to be shutdown.

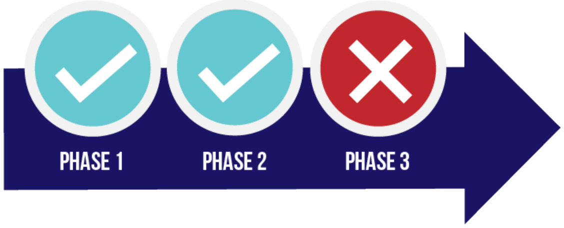
Source: Miercom

The PowerShell portion of the Kovter malware persistent infection was prevented, and the end user was alerted.

5.3 Metasploit Meterpreter

The Metasploit Meterpreter test case used a Word document containing a malicious macro that invoked the Meterpreter payload into memory on the victim machine. The exploit launched a PowerShell script; PowerShell itself is not necessarily malicious and was not analyzed for prevention. However, the download, execution and existence of the exploit itself within the network should be detected and blocked by the AMP solution.

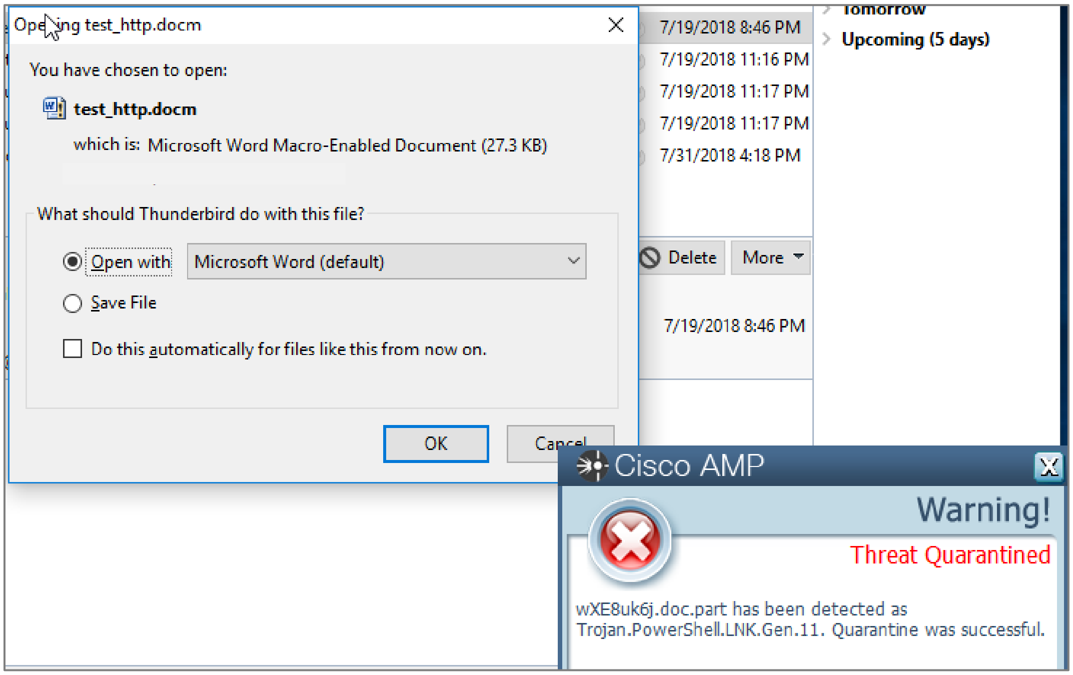
Metasploit is an industry standard tool and is used to help highlight AMP's capabilities. This test case consists of three main phases: initial file download, macro execution and the fileless Meterpreter instance. This test case's performance is outlined in the graphic below.



Phase 1: Download Email Attachment

In the first phase of this test, the malware was downloaded via an email attachment. The email attachment was immediately identified and quarantined by AMP upon attempted download.

Figure 11: Successful Quarantine of Attempted Malicious Email Attachment



Opening test_http.docm

You have chosen to open:

test_http.docm

which is: Microsoft Word Macro-Enabled Document (27.3 KB)

What should Thunderbird do with this file?

● Open with Microsoft Word (default)

○ Save File

□ Do this automatically for files like this from now on.

Warning!

Threat Quarantined

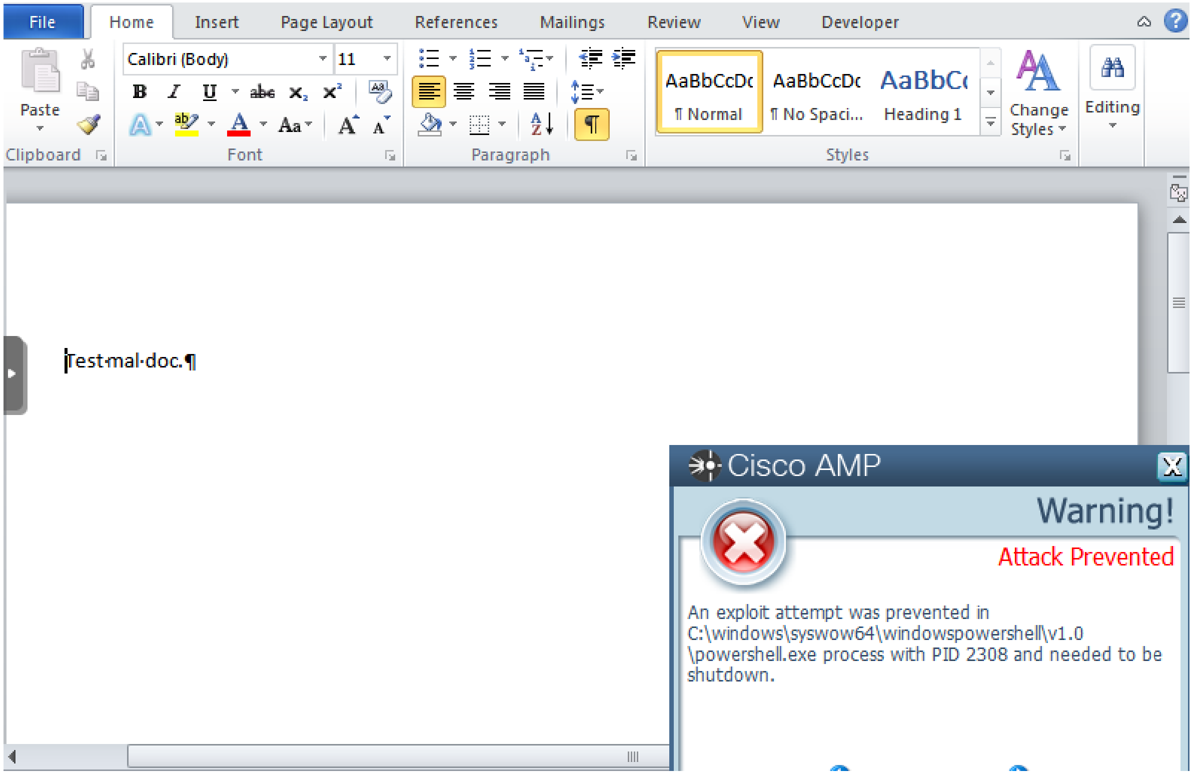
wXE8uk6j.doc.part has been detected as Trojan.PowerShell.LNK.Gen.11. Quarantine was successful.

Source: Miercom

Phase 2: Macro Execution

AMP was disabled, and the malicious document was downloaded. After reenabling AMP, the malware was attempted to be run. AMP successfully detected the initialization of the malicious PowerShell instance and blocks the attack. This instance was detected when PowerShell attempted to establish a new thread.

Figure 12: Prevention of Metasploit Malicious Macro



Test·mal·doc.¶

Cisco AMP

Warning!

Attack Prevented

An exploit attempt was prevented in C:\windows\syswow64\windowspowershell\v1.0 \powershell.exe process with PID 2308 and needed to be shutdown.

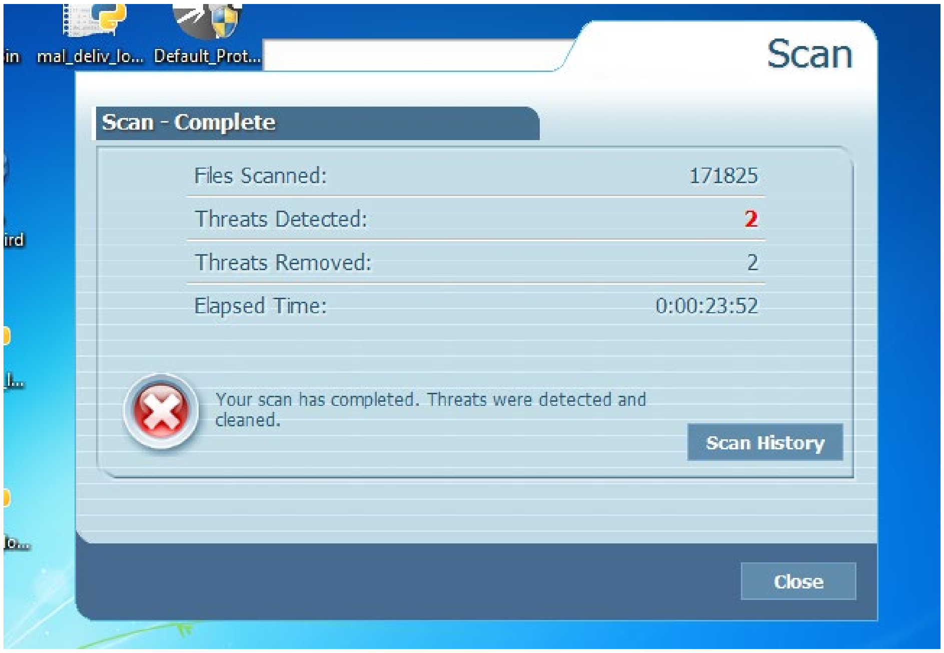
Source: Miercom

This screenshot shows the successful prevention of a Metasploit attack via a malicious macro in a Word document.

Phase 3: Fileless Meterpreter Execution

AMP was disabled, and the malware fully executed. This spawned a Meterpreter instance in memory of the victim. This session allowed an attacker to perform malicious activities such as keylogging or webcam capture. AMP was able to successfully identify the malicious file upon scanning but did not detect the Meterpreter session running in memory.

Figure 13 Cisco AMP Detection of Malicious File



Scan - Complete

Files Scanned:	171825
Threats Detected:	2
Threats Removed:	2
Elapsed Time:	0:00:23:52

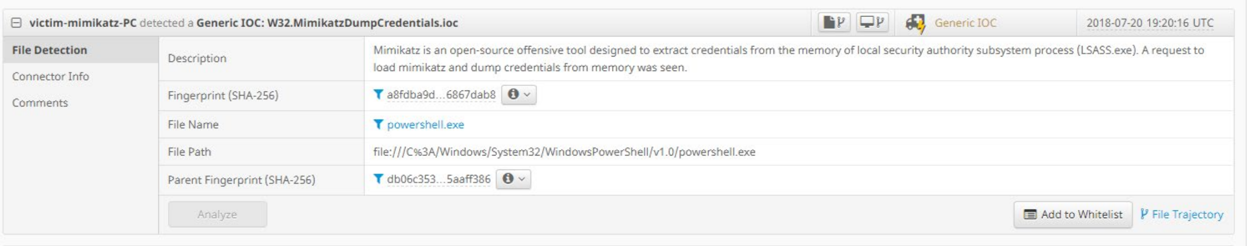
Your scan has completed. Threats were detected and cleaned.

Source: Miercom

5.4 Mimikatz Exploit

The Mimikatz test case utilized a known Windows 7 vulnerability to retrieve the username, password, and domain information of the victim computer. In this test case, a malicious USB drive spawned and executed the Mimikatz exploit. Successful execution of this exploit returned the username and password of the Windows 7 victim. This test case was assessed in a single phase in which the exploit is run. AMP successfully protected the victim computer from the vulnerability.

Figure 14: Successful Block of Mimikatz Exploit



⊟ **victim-mimikatz-PC** detected a **Generic IOC: W32.MimikatzDumpCredentials.ioc** — Generic IOC — 2018-07-20 19:20:16 UTC

File Detection	Description	Mimikatz is an open-source offensive tool designed to extract credentials from the memory of local security authority subsystem process (LSASS.exe). A request to load mimikatz and dump credentials from memory was seen.
Connector Info	Fingerprint (SHA-256)	a8fdba9d…6867dab8
Comments	File Name	powershell.exe
	File Path	file:///C%3A/Windows/System32/WindowsPowerShell/v1.0/powershell.exe
	Parent Fingerprint (SHA-256)	db06c353…5aaff386

Source: Miercom

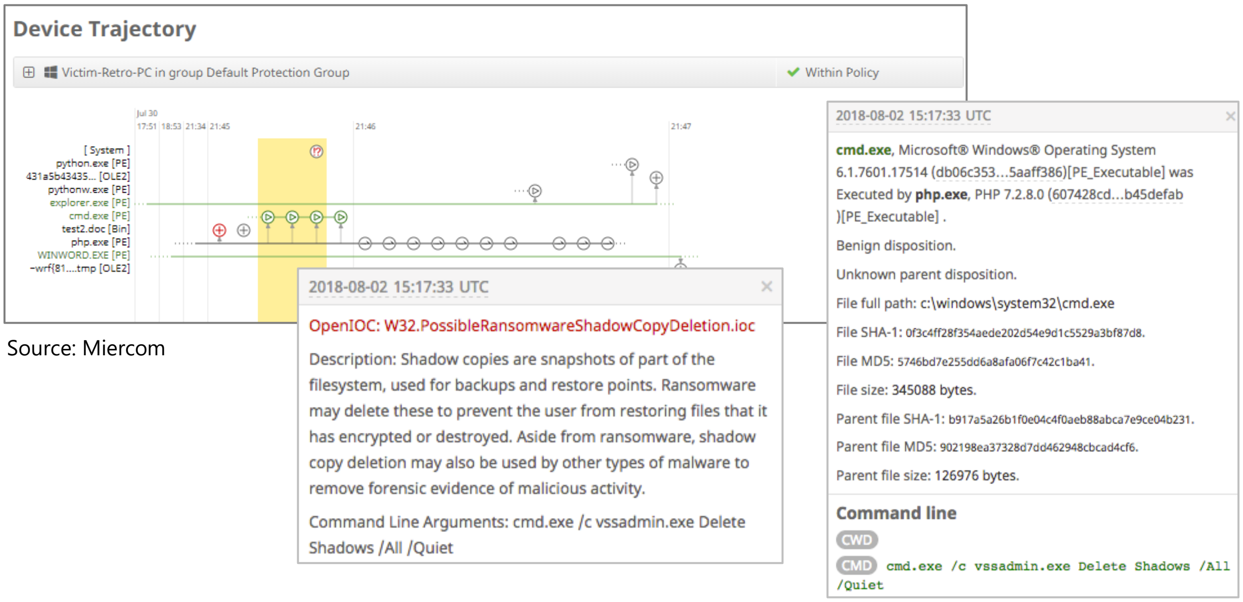
The user was alerted of successful prevention of the Mimikatz exploit in the cloud interface. This alert notifies the administrator of the attempted Mimikatz credential dump.

5.5 Retrospection Analysis

A malicious scenario was created using samples specifically tailored to bypass AMP's initial detection. The first phase of attack used an encrypted Word document delivered via email. Phase two launched a ransomware attack with a PHP script to encrypt the victim's files. The exploit should run successfully the first time and block by AMP in future iterations.

Cisco AMP provided insight for this unique attack. Cisco AMP produced alerts and warnings of serious potential for compromise for investigation. Utilizing the device trajectory and events created by AMP, a clear understanding of the attack vector was reconstructed for analysis. This use case successfully proved the detection and incident response capabilities of Cisco AMP.

Figure 15: Detection of Possible Ransomware Compromise



2018-08-02 15:17:33 UTC

OpenIOC: W32.PossibleRansomwareShadowCopyDeletion.ioc

Description: Shadow copies are snapshots of part of the filesystem, used for backups and restore points. Ransomware may delete these to prevent the user from restoring files that it has encrypted or destroyed. Aside from ransomware, shadow copy deletion may also be used by other types of malware to remove forensic evidence of malicious activity.

Command Line Arguments: cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet

2018-08-02 15:17:33 UTC

cmd.exe, Microsoft® Windows® Operating System 6.1.7601.17514 (db06c353…5aaff386)[PE_Executable] was Executed by **php.exe**, PHP 7.2.8.0 (607428cd…b45defab)[PE_Executable] .

Benign disposition.

Unknown parent disposition.

File full path: c:\windows\system32\cmd.exe

File SHA-1: 0f3c4ff28f354aede202d54e9d1c5529a3bf87d8.

File MD5: 5746bd7e255dd6a8afa06f7c42c1ba41.

File size: 345088 bytes.

Parent file SHA-1: b917a5a26b1f0e04c4f0aeb88abca7e9ce04b231.

Parent file MD5: 902198ea37328d7dd462948cbcad4cf6.

Parent file size: 126976 bytes.

Command line

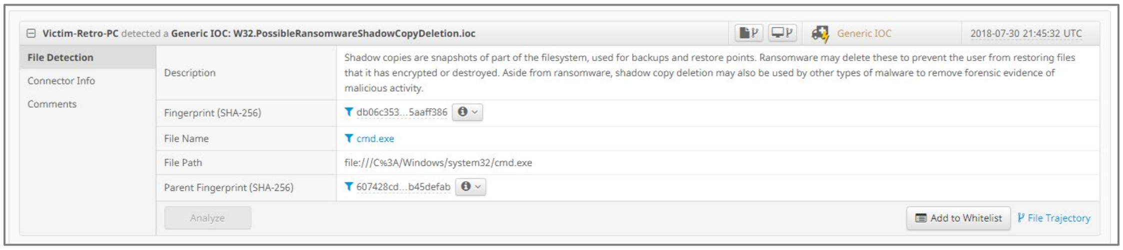
CWD

CMD `cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet`

Source: Miercom

Detection of a possible compromise is highlighted by the AMP interface. This identification is triggered by the detection of probable ransomware action in which shadow copies are deleted.

Figure 16: Ransomware Attack Alert



Victim-Retro-PC detected a **Generic IOC: W32.PossibleRansomwareShadowCopyDeletion.ioc** 2018-07-30 21:45:32 UTC

Description	Shadow copies are snapshots of part of the filesystem, used for backups and restore points. Ransomware may delete these to prevent the user from restoring files that it has encrypted or destroyed. Aside from ransomware, shadow copy deletion may also be used by other types of malware to remove forensic evidence of malicious activity.
Fingerprint (SHA-256)	db06c353…5aaff386
File Name	cmd.exe
File Path	file:///C%3A/Windows/system32/cmd.exe
Parent Fingerprint (SHA-256)	607428cd…b45defab

Source: Miercom

The end user is alerted of shadow copy deletions indicative of ransomware with a description.

6.0 Conclusion

Cisco AMP was able to successfully prevent all exploits tested, while providing alerts and insight on remediation.

Locky Ransomware (Section 5.1) – This exploit was prevented during download, infection, spawning and execution phases. The Cisco AMP Threat Grid offered investigation of the flagged malware via the retrospection engine.

Kovter (Section 5.2) – This exploit was prevented during two phases of JavaScript, malware execution and fileless persistence. A warning was issued to the ender user for threat visibility.

Metasploit Meterpreter (Section 5.3) – This exploit was prevented during the download and macro execution phases, showing two detected and removed threats during the scan.

Mimikatz (Section 5.4) – This exploit was prevented, and the user was alerted of the attempted credential dump via the cloud interface.

Retrospection Analysis (Section 5.5) – Possible compromise and ransomware execution was detected, and Cisco AMP provided alerts and incident response options.

Based on our observations, the Cisco Advanced Malware Protection product secured the network during multi-phase exploit attempts, earning the ***Miercom Performance Verified*** accreditation.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.