Threat Extraction

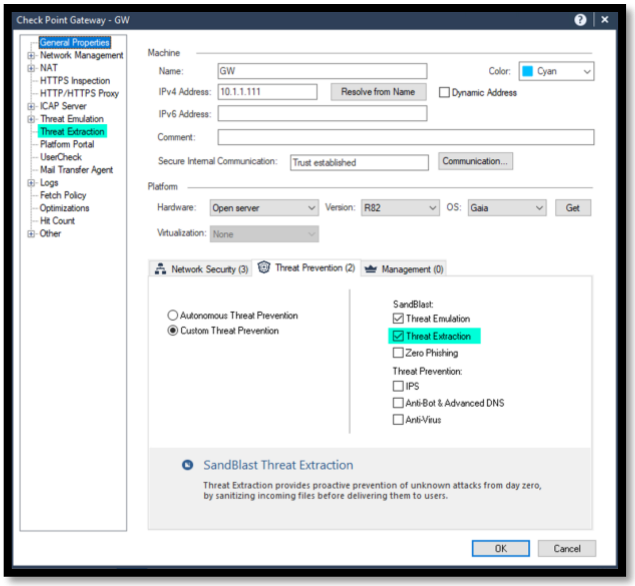
Introduction

The Check Point Threat Extraction blade removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.

Exercise 1: Onboarding

In this exercise, we will enable the Threat Extraction blade and use it to remove the exploitable content from the generated files.

1. Connect to SmartConsole from the Jump Server, edit the GW object and enable Threat Extraction.



Check Point Gateway - GW

Machine
Name: GW
Color: Cyan
IPv4 Address: 10.1.1.111
□ Dynamic Address
IPv6 Address:
Comment:
Secure Internal Communication: Trust established

Platform
Hardware: Open server
Version: R82
OS: Gaia
Virtualization: None

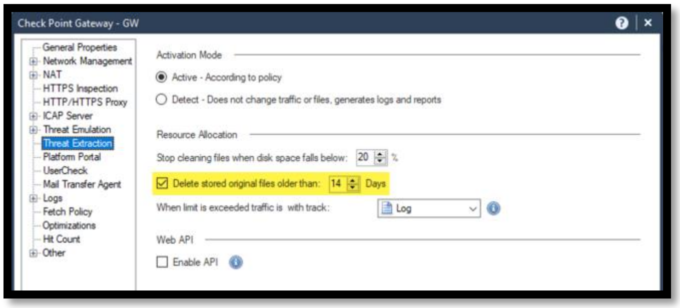
○ Autonomous Threat Prevention
● Custom Threat Prevention

SandBlast:
☑ Threat Emulation
☑ Threat Extraction
□ Zero Phishing
Threat Prevention:
□ IPS
□ Anti-Bot & Advanced DNS
□ Anti-Virus

SandBlast Threat Extraction

Threat Extraction provides proactive prevention of unknown attacks from day zero, by sanitizing incoming files before delivering them to users.

2. Review the default settings under General Properties -> Threat Extraction. And save the changes.



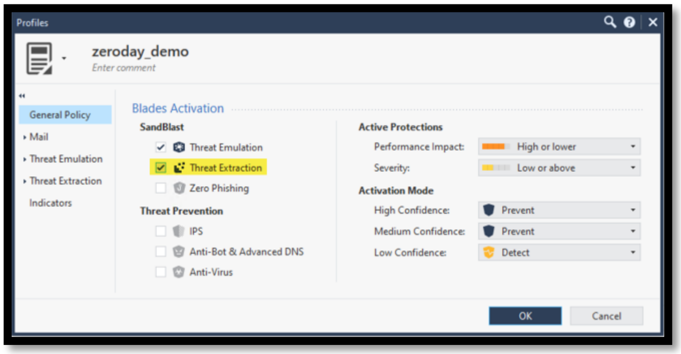
Check Point Gateway - GW

Activation Mode
● Active - According to policy
○ Detect - Does not change traffic or files, generates logs and reports

Resource Allocation
Stop cleaning files when disk space falls below: 20 %
☑ Delete stored original files older than: 14 Days
When limit is exceeded traffic is with track: Log

Web API
□ Enable API

3. Edit the existing profile**, zeroday_demo** and activate Threat Extraction.



Profiles

zeroday_demo
Enter comment

General Policy
- Mail
- Threat Emulation
- Threat Extraction
- Indicators

Blades Activation

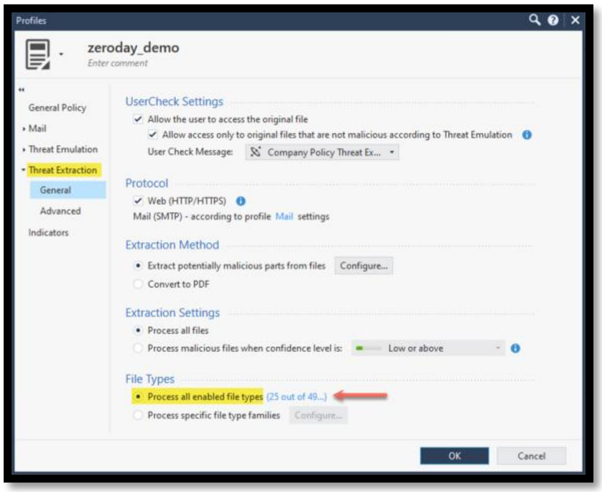
SandBlast
- ☑ Threat Emulation
- ☑ Threat Extraction
- □ Zero Phishing

Threat Prevention
- □ IPS
- □ Anti-Bot & Advanced DNS
- □ Anti-Virus

Active Protections
- Performance Impact: High or lower
- Severity: Low or above

Activation Mode
- High Confidence: Prevent
- Medium Confidence: Prevent
- Low Confidence: Detect

4. Under Threat Extraction -> **General**, there are **25** file types are enabled by default.



Profiles

zeroday_demo
Enter comment

General Policy
- Mail
- Threat Emulation
- Threat Extraction
  - General
  - Advanced
- Indicators

UserCheck Settings
- ☑ Allow the user to access the original file
  - ☑ Allow access only to original files that are not malicious according to Threat Emulation
  - User Check Message: Company Policy Threat Ex...

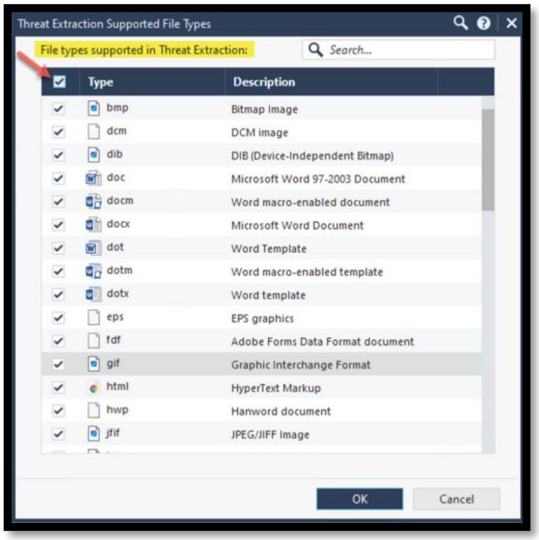
Protocol
- ☑ Web (HTTP/HTTPS)
- Mail (SMTP) - according to profile Mail settings

Extraction Method
- ● Extract potentially malicious parts from files Configure...
- ○ Convert to PDF

Extraction Settings
- ● Process all files
- ○ Process malicious files when confidence level is: Low or above

File Types
- ● Process all enabled file types (25 out of 49...)
- ○ Process specific file type families Configure...

5. Click on the active link and edit the List and enable all file types.

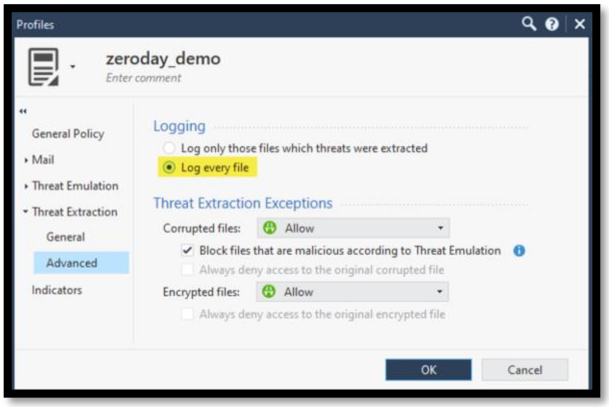


Threat Extraction Supported File Types

File types supported in Threat Extraction:

☑	Type	Description
✓	bmp	Bitmap Image
✓	dcm	DCM image
✓	dib	DIB (Device-Independent Bitmap)
✓	doc	Microsoft Word 97-2003 Document
✓	docm	Word macro-enabled document
✓	docx	Microsoft Word Document
✓	dot	Word Template
✓	dotm	Word macro-enabled template
✓	dotx	Word template
✓	eps	EPS graphics
✓	fdf	Adobe Forms Data Format document
✓	gif	Graphic Interchange Format
✓	html	HyperText Markup
✓	hwp	Hanword document
✓	jfif	JPEG/JIFF Image

6. Under **Advanced**, change the logging option to **Log every file**. This is useful in a demo environment.



zeroday_demo
Enter comment

Logging
○ Log only those files which threats were extracted
● Log every file

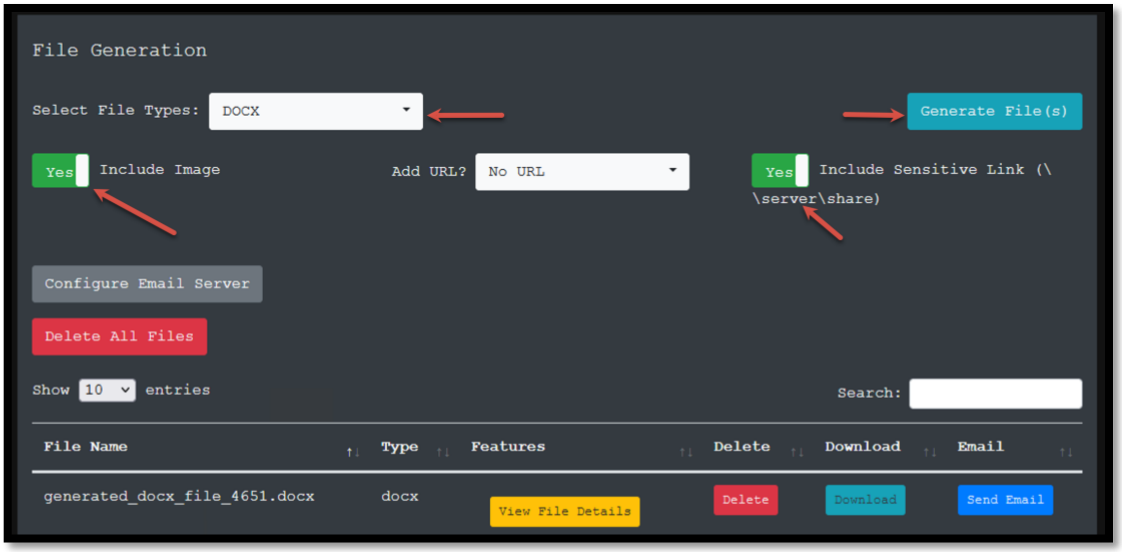
Threat Extraction Exceptions
Corrupted files: Allow
☑ Block files that are malicious according to Threat Emulation
□ Always deny access to the original corrupted file
Encrypted files: Allow
□ Always deny access to the original encrypted file

7. Save the changes and Install the Access Control and Threat Prevention Policy.

Exercise 2: Web Extraction

In this exercise, we will generate and download documents and files with exploitable content and evaluate the cleaned files.

1. From win_client, open a web browser (use Firefox for this lab). Use the file generator to generate a **DOCX** file. Check the box to **Include Image** and **Include Sensitive Link.**



File Generation

Select File Types: DOCX

Yes Include Image

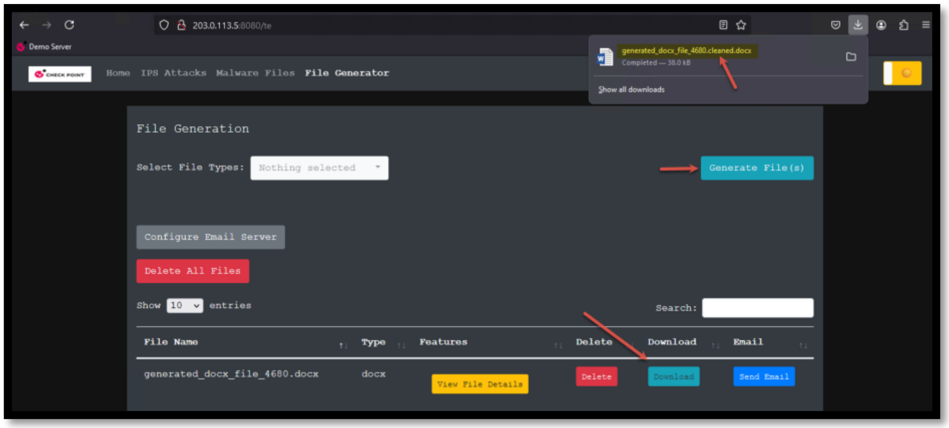
Add URL? No URL

Yes Include Sensitive Link (\\server\share)

Show 10 entries

File Name	Type	Features	Delete	Download	Email
generated_docx_file_4651.docx	docx	View File Details	Delete	Download	Send Email

2. Download the file, notice that the file was renamed to indicate that the file was cleaned.



File Generation

Select File Types: Nothing selected

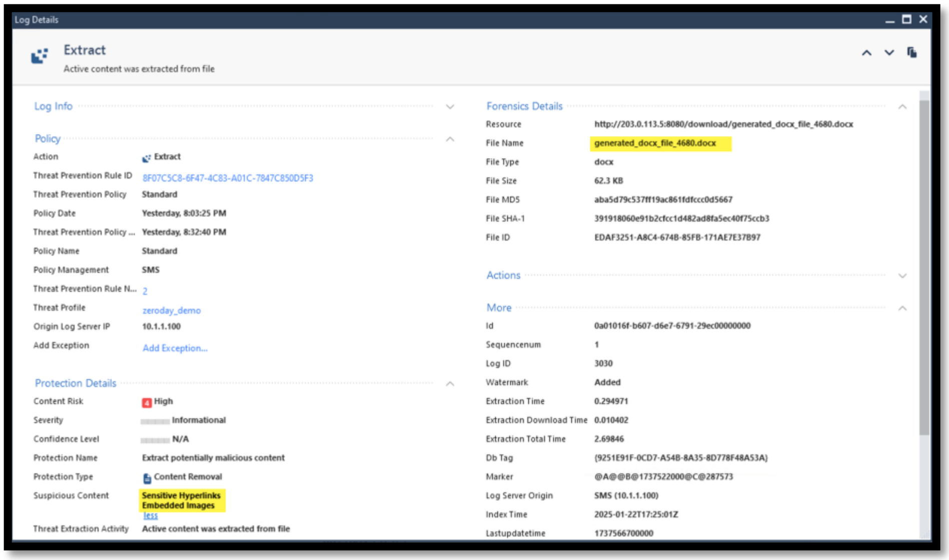
Show 10 entries

Search:

File Name	Type	Features	Delete	Download	Email
generated_docx_file_4680.docx	docx	View File Details	Delete	Download	Send Email

1. It is possible to customize the renaming of the cleaned file. See sk114613.

3. Review the log in SmartConsole. Notice that the log indicates what kind of exploitable content was cleaned from the file.



Extract
Active content was extracted from file

Log Info

Policy

Action	Extract
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-A01C-7847C850D5F3
Threat Prevention Policy	Standard
Policy Date	Yesterday, 8:03:25 PM
Threat Prevention Policy ...	Yesterday, 8:32:40 PM
Policy Name	Standard
Policy Management	SMS
Threat Prevention Rule N...	2
Threat Profile	zeroday_demo
Origin Log Server IP	10.1.1.100
Add Exception	Add Exception...

Protection Details

Content Risk	4 High
Severity	Informational
Confidence Level	N/A
Protection Name	Extract potentially malicious content
Protection Type	Content Removal
Suspicious Content	Sensitive Hyperlinks Embedded Images less
Threat Extraction Activity	Active content was extracted from file

Forensics Details

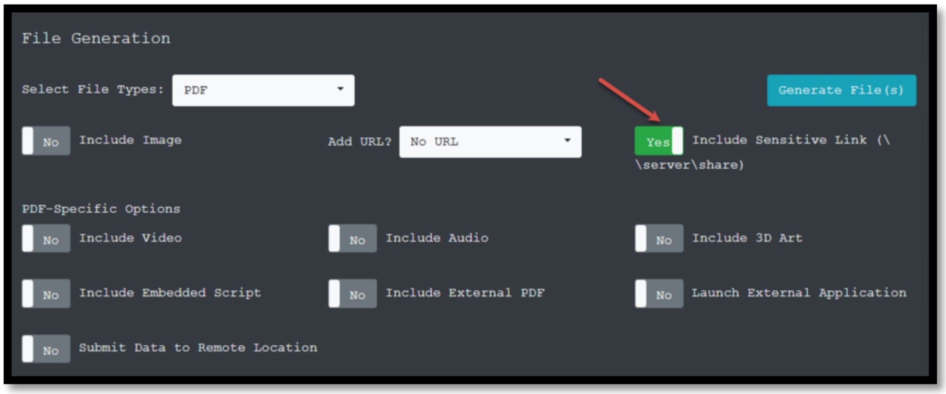
Resource	http://203.0.113.5:8080/download/generated_docx_file_4680.docx
File Name	generated_docx_file_4680.docx
File Type	docx
File Size	62.3 KB
File MD5	aba5d79c537ff19ac861fdfccc0d5667
File SHA-1	391918060e91b2cfcc1d482ad8fa5ec40f75ccb3
File ID	EDAF3251-A8C4-674B-85FB-171AE7E37B97

Actions

More

Id	0a01016f-b607-d6e7-6791-29ec00000000
Sequencenum	1
Log ID	3030
Watermark	Added
Extraction Time	0.294971
Extraction Download Time	0.010402
Extraction Total Time	2.69846
Db Tag	{9251E91F-0CD7-A54B-8A35-8D778F48A53A}
Marker	@A@@B@1737522000@C@287573
Log Server Origin	SMS (10.1.1.100)
Index Time	2025-01-22T17:25:01Z
Lastupdatetime	1737566700000

4. Generate a PDF file that includes a sensitive link (*link to internal Shares*).



File Generation

Select File Types: PDF

No Include Image

Add URL? No URL

Yes Include Sensitive Link (\\server\share)

PDF-Specific Options

No Include Video

No Include Audio

No Include 3D Art

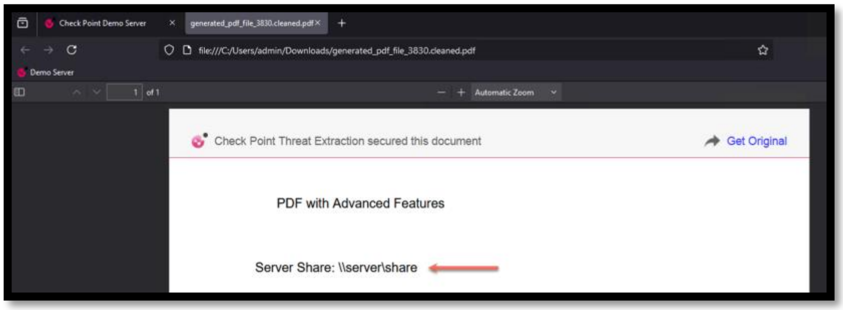
No Include Embedded Script

No Include External PDF

No Launch External Application

No Submit Data to Remote Location

5. Download the file. If you are using Firefox, the file will be opened automatically. Notice that the sensitive link is not a clickable link. Threat Extraction can remove the risk.

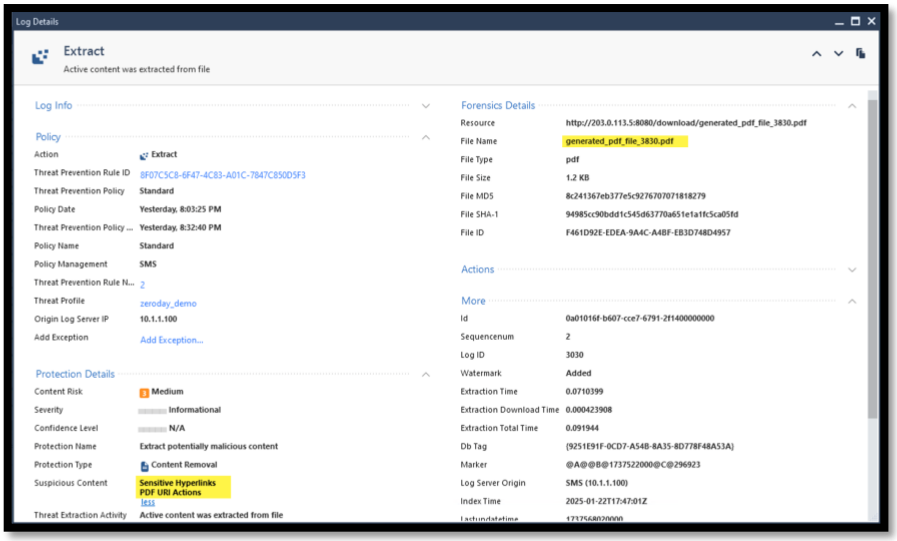

Check Point Demo Server
generated_pdf_file_3830.cleaned.pdf
file:///C:/Users/admin/Downloads/generated_pdf_file_3830.cleaned.pdf
Demo Server
1 of 1
Automatic Zoom

Check Point Threat Extraction secured this document | Get Original

PDF with Advanced Features

Server Share: \\server\share

6. Review the log in SmartConsole. Notice that the **Sensitive hyperlink** was recognized. It is also recognized as **PDF URI Actions**.



Extract
Active content was extracted from file

Log Info

Policy

Action	Extract
Threat Prevention Rule ID	8F07C5C8-6F47-4C83-A01C-7847C850D5F3
Threat Prevention Policy	Standard
Policy Date	Yesterday, 8:03:25 PM
Threat Prevention Policy ...	Yesterday, 8:32:40 PM
Policy Name	Standard
Policy Management	SMS
Threat Prevention Rule N...	2
Threat Profile	zeroday_demo
Origin Log Server IP	10.1.1.100
Add Exception	Add Exception...

Protection Details

Content Risk	3 Medium
Severity	Informational
Confidence Level	N/A
Protection Name	Extract potentially malicious content
Protection Type	Content Removal
Suspicious Content	Sensitive Hyperlinks PDF URI Actions less
Threat Extraction Activity	Active content was extracted from file

Forensics Details

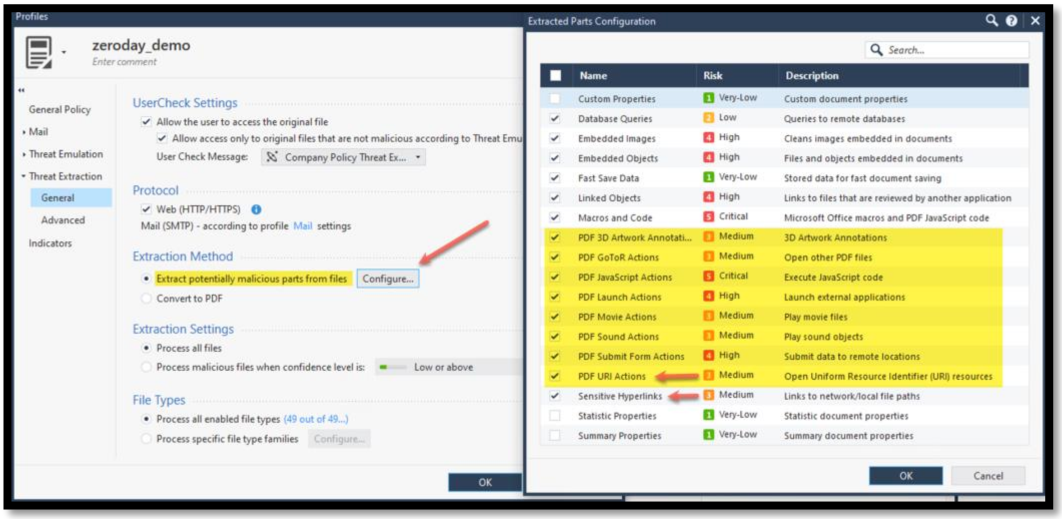
Resource	http://203.0.113.5:8080/download/generated_pdf_file_3830.pdf
File Name	generated_pdf_file_3830.pdf
File Type	pdf
File Size	1.2 KB
File MD5	8c241367eb377e5c9276707071818279
File SHA-1	94985cc90bdd1c545d63770a651e1a1fc5ca05fd
File ID	F461D92E-EDEA-9A4C-A4BF-EB3D748D4957

Actions

More

Id	0a01016f-b607-cce7-6791-2f1400000000
Sequencenum	2
Log ID	3030
Watermark	Added
Extraction Time	0.0710399
Extraction Download Time	0.000423908
Extraction Total Time	0.091944
Db Tag	{9251E91F-0CD7-A54B-8A35-8D778F48A53A}
Marker	@A@@B@1737522000@C@296923
Log Server Origin	SMS (10.1.1.100)
Index Time	2025-01-22T17:47:01Z
Lastupdatetime	1737568020000

7. Review the Threat Profile in use, notice that many Risks are specific to PDF file only.



zeroday_demo
Enter comment

UserCheck Settings
☑ Allow the user to access the original file
☑ Allow access only to original files that are not malicious according to Threat Emu
User Check Message: Company Policy Threat Ex...

Protocol
☑ Web (HTTP/HTTPS)
Mail (SMTP) - according to profile Mail settings

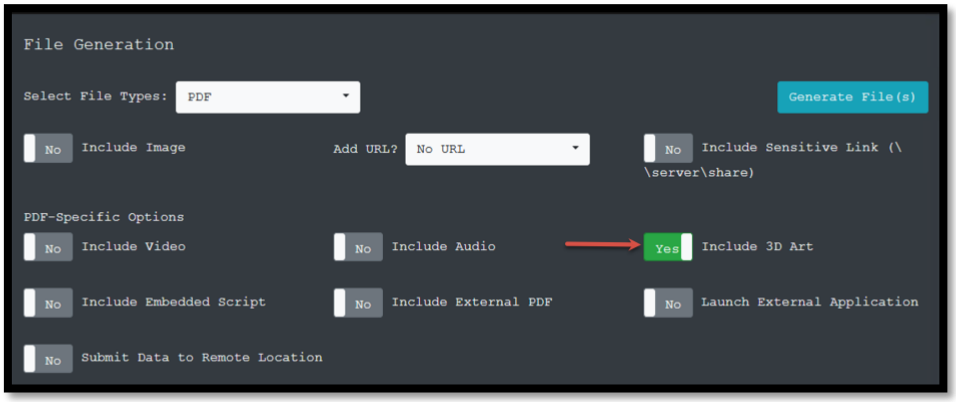
Extraction Method
● Extract potentially malicious parts from files [Configure...]
○ Convert to PDF

Extraction Settings
● Process all files
○ Process malicious files when confidence level is: Low or above

File Types
● Process all enabled file types (49 out of 49...)
○ Process specific file type families [Configure...]

☐	Name	Risk	Description
☐	Custom Properties	1 Very-Low	Custom document properties
☑	Database Queries	2 Low	Queries to remote databases
☑	Embedded Images	4 High	Cleans images embedded in documents
☑	Embedded Objects	4 High	Files and objects embedded in documents
☑	Fast Save Data	1 Very-Low	Stored data for fast document saving
☑	Linked Objects	4 High	Links to files that are reviewed by another application
☑	Macros and Code	5 Critical	Microsoft Office macros and PDF JavaScript code
☑	PDF 3D Artwork Annotati...	3 Medium	3D Artwork Annotations
☑	PDF GoToR Actions	3 Medium	Open other PDF files
☑	PDF JavaScript Actions	5 Critical	Execute JavaScript code
☑	PDF Launch Actions	4 High	Launch external applications
☑	PDF Movie Actions	3 Medium	Play movie files
☑	PDF Sound Actions	3 Medium	Play sound objects
☑	PDF Submit Form Actions	4 High	Submit data to remote locations
☑	PDF URI Actions	3 Medium	Open Uniform Resource Identifier (URI) resources
☑	Sensitive Hyperlinks	3 Medium	Links to network/local file paths
☐	Statistic Properties	1 Very-Low	Statistic document properties
☐	Summary Properties	1 Very-Low	Summary document properties

8. Generate and download a new PDF file and include a **3D Art** object.



File Generation

Select File Types: PDF

No Include Image

Add URL? No URL

No Include Sensitive Link (\\server\share)

PDF-Specific Options

No Include Video

No Include Audio

Yes Include 3D Art

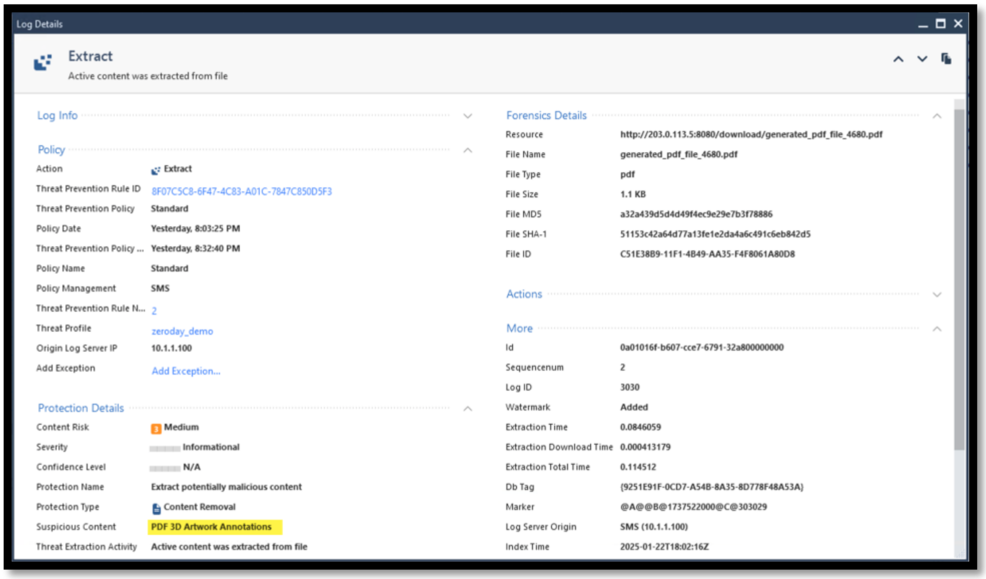
No Include Embedded Script

No Include External PDF

No Launch External Application

No Submit Data to Remote Location

9. Review the log and notice that the item has been identified and logged.



Log Details

Extract
Active content was extracted from file

Log Info

Policy
Action Extract
Threat Prevention Rule ID 8F07C5C8-6F47-4C83-A01C-7847C850D5F3
Threat Prevention Policy Standard
Policy Date Yesterday, 8:03:25 PM
Threat Prevention Policy ... Yesterday, 8:32:40 PM
Policy Name Standard
Policy Management SMS
Threat Prevention Rule N... 2
Threat Profile zeroday_demo
Origin Log Server IP 10.1.1.100
Add Exception Add Exception...

Protection Details
Content Risk 3 Medium
Severity Informational
Confidence Level N/A
Protection Name Extract potentially malicious content
Protection Type Content Removal
Suspicious Content PDF 3D Artwork Annotations
Threat Extraction Activity Active content was extracted from file

Forensics Details
Resource http://203.0.113.5:8080/download/generated_pdf_file_4680.pdf
File Name generated_pdf_file_4680.pdf
File Type pdf
File Size 1.1 KB
File MD5 a32a439d5d4d49f4ec9e29e7b3f78886
File SHA-1 51153c42a64d77a13fe1e2da4a6c491c6eb842d5
File ID C51E38B9-11F1-4B49-AA35-F4F8061A80D8

Actions

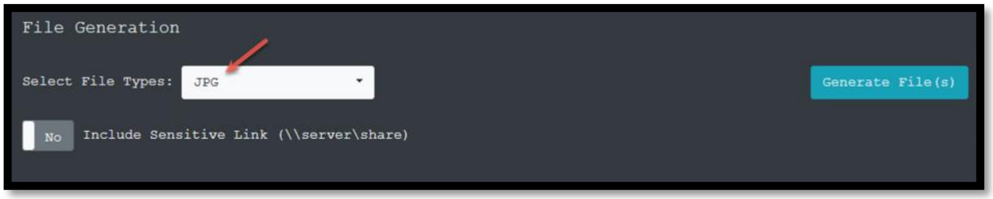
More
Id 0a01016f-b607-cce7-6791-32a800000000
Sequencenum 2
Log ID 3030
Watermark Added
Extraction Time 0.0846059
Extraction Download Time 0.000413179
Extraction Total Time 0.114512
Db Tag {9251E91F-0CD7-A54B-8A35-8D778F48A53A}
Marker @A@@B@1737522000@C@303029
Log Server Origin SMS (10.1.1.100)
Index Time 2025-01-22T18:02:16Z

Exercise 3: Mail Extraction

In the previous exercise, we tested generating and downloading files containing active exploitable content. Threat Extraction is capable of cleaning files that arrive over emails.

Some file type can be cleaned whether they come over email or if they are downloaded from the internet. For example, image files can be extracted when they arrive over emails but not when downloaded from the web. Refer to sk101553 for more details.

- Use the demo server to generate and download a JPG image file.

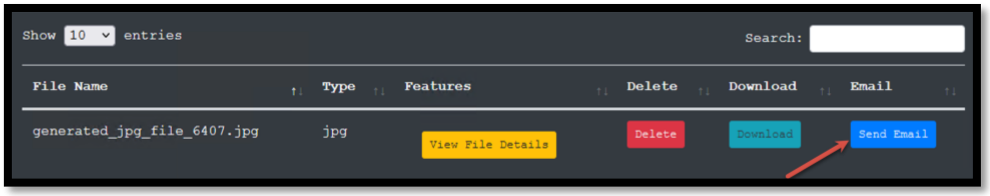


File Generation

Select File Types: JPG

No Include Sensitive Link (\\server\share)

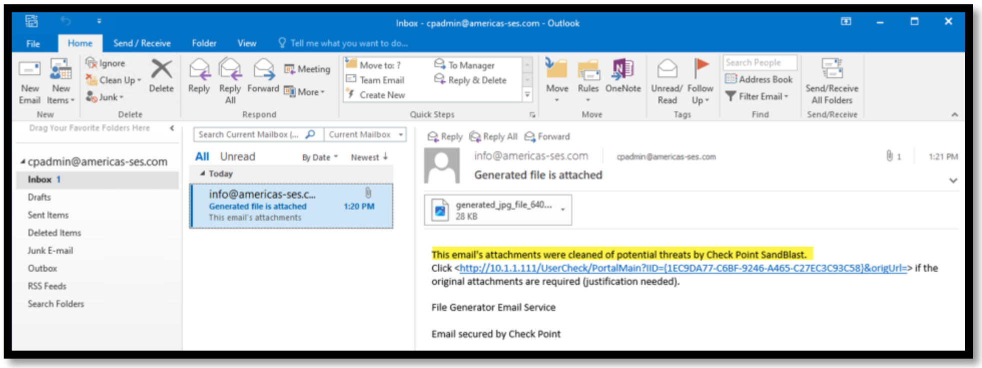
- Try to download the file and notice that the original copy was downloaded, and it was not cleaned.
- Click Send Email to deliver the file over email.



Show 10 entries Search:

File Name	Type	Features	Delete	Download	Email
generated_jpg_file_6407.jpg	jpg	View File Details	Delete	Download	Send Email

- Review the Email. Pay attention to the message indicating that Threat Extraction modified the file.



info@americas-ses.c...
Generated file is attached 1:20 PM
This email's attachments

info@americas-ses.com cpadmin@americas-ses.com 1 1:21 PM
Generated file is attached

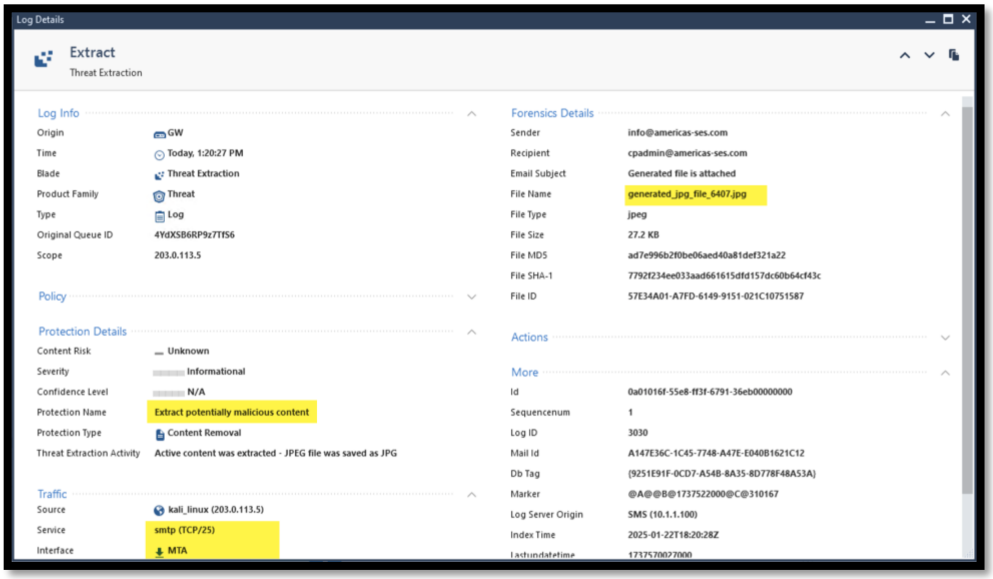
generated_jpg_file_640...
28 KB

This email's attachments were cleaned of potential threats by Check Point SandBlast.
Click <http://10.1.1.111/UserCheck/PortalMain?IID={1EC9DA77-C6BF-9246-A465-C27EC3C93C58}&origUrl=> if the original attachments are required (justification needed).

File Generator Email Service

Email secured by Check Point

- Review the logs in SmartConsole. The file was cleaned as expected.



Extract
Threat Extraction

Log Info

Origin	GW
Time	Today, 1:20:27 PM
Blade	Threat Extraction
Product Family	Threat
Type	Log
Original Queue ID	4YdXSB6RP9z7Tf56
Scope	203.0.113.5

Policy

Protection Details

Content Risk	Unknown
Severity	Informational
Confidence Level	N/A
Protection Name	Extract potentially malicious content
Protection Type	Content Removal
Threat Extraction Activity	Active content was extracted - JPEG file was saved as JPG

Traffic

Source	kali_linux (203.0.113.5)
Service	smtp (TCP/25)
Interface	MTA

Forensics Details

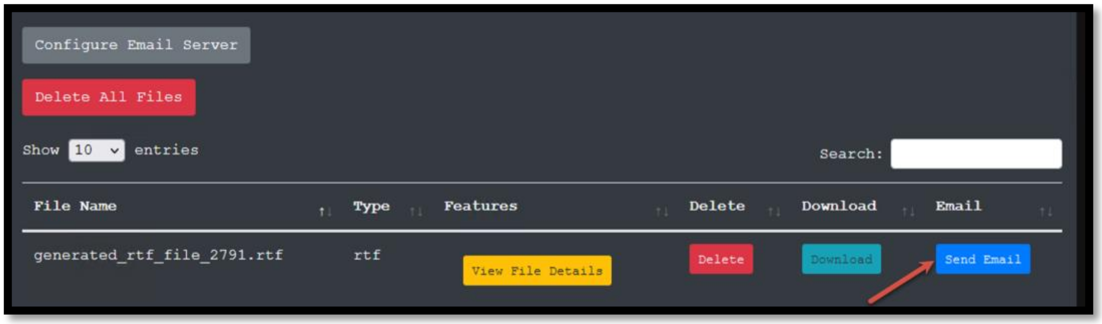
Sender	info@americas-ses.com
Recipient	cpadmin@americas-ses.com
Email Subject	Generated file is attached
File Name	generated_jpg_file_6407.jpg
File Type	jpeg
File Size	27.2 KB
File MD5	ad7e996b2f0be06aed40a81def321a22
File SHA-1	7792f234ee033aad661615dfd157dc60b64cf43c
File ID	57E34A01-A7FD-6149-9151-021C10751587

Actions

More

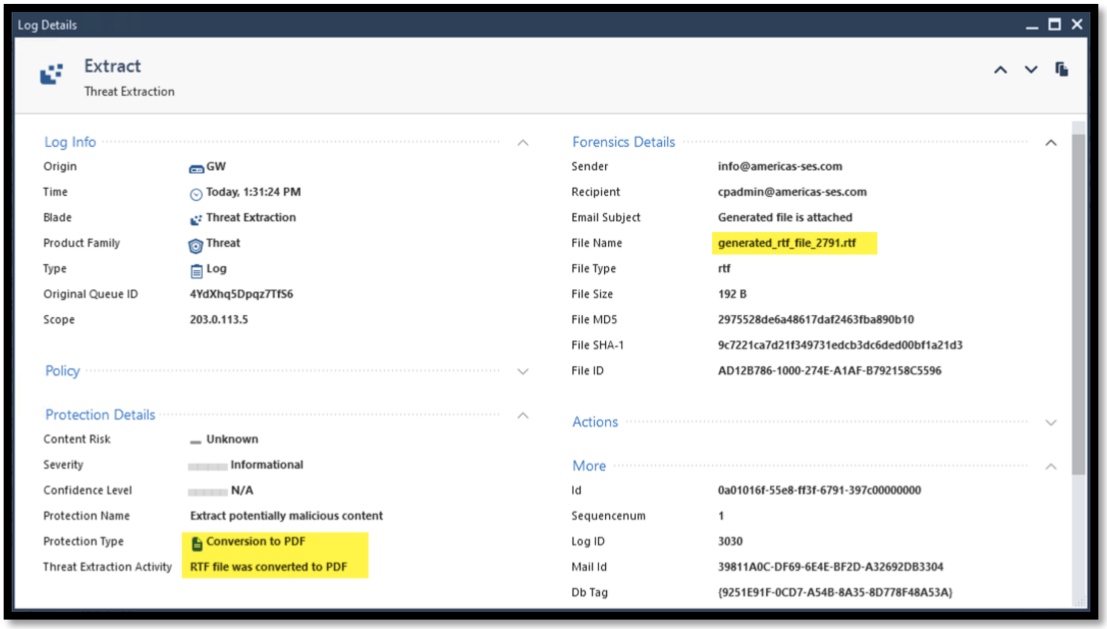
Id	0a01016f-55e8-ff3f-6791-36eb00000000
Sequencenum	1
Log ID	3030
Mail Id	A147E36C-1C45-7748-A47E-E040B1621C12
Db Tag	{9251E91F-0CD7-A54B-8A35-8D778F48A53A}
Marker	@A@@B@1737522000@C@310167
Log Server Origin	SMS (10.1.1.100)
Index Time	2025-01-22T18:20:28Z
Lastupdatetime	1737570027000

- Generate a new RTF file. Sen the file over email.



File Name	Type	Features	Delete	Download	Email
generated_rtf_file_2791.rtf	rtf	View File Details	Delete	Download	Send Email

- Review the logs in SmartConsole. Notice that the log indicates that the file was converted to a PDF file.



Extract
Threat Extraction

Log Info

Origin	GW
Time	Today, 1:31:24 PM
Blade	Threat Extraction
Product Family	Threat
Type	Log
Original Queue ID	4YdXhq5Dpqz7TfS6
Scope	203.0.113.5

Policy

Protection Details

Content Risk	Unknown
Severity	Informational
Confidence Level	N/A
Protection Name	Extract potentially malicious content
Protection Type	Conversion to PDF
Threat Extraction Activity	RTF file was converted to PDF

Forensics Details

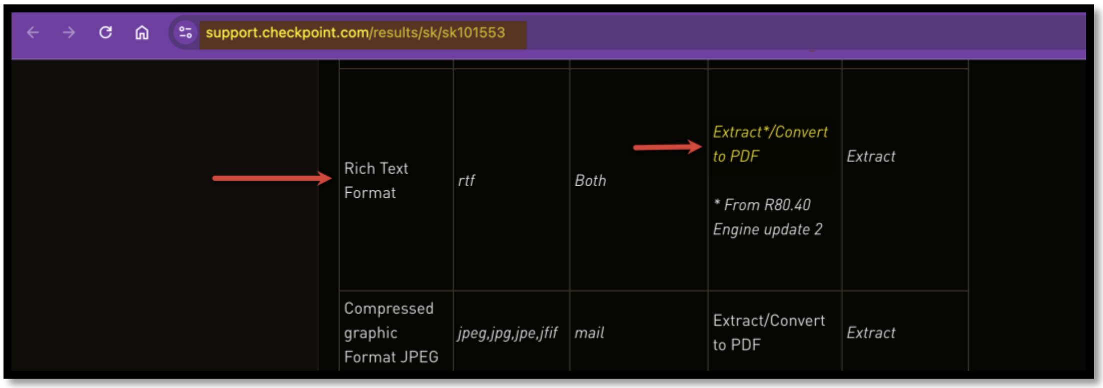
Sender	info@americas-ses.com
Recipient	cpadmin@americas-ses.com
Email Subject	Generated file is attached
File Name	generated_rtf_file_2791.rtf
File Type	rtf
File Size	192 B
File MD5	2975528de6a48617daf2463fba890b10
File SHA-1	9c7221ca7d21f349731edcb3dc6ded00bf1a21d3
File ID	AD12B786-1000-274E-A1AF-B792158C5596

Actions

More

Id	0a01016f-55e8-ff3f-6791-397c00000000
Sequencenum	1
Log ID	3030
Mail Id	39811A0C-DF69-6E4E-BF2D-A32692DB3304
Db Tag	{9251E91F-0CD7-A54B-8A35-8D778F48A53A}

- Note that this behavior above is explained in sk101553.

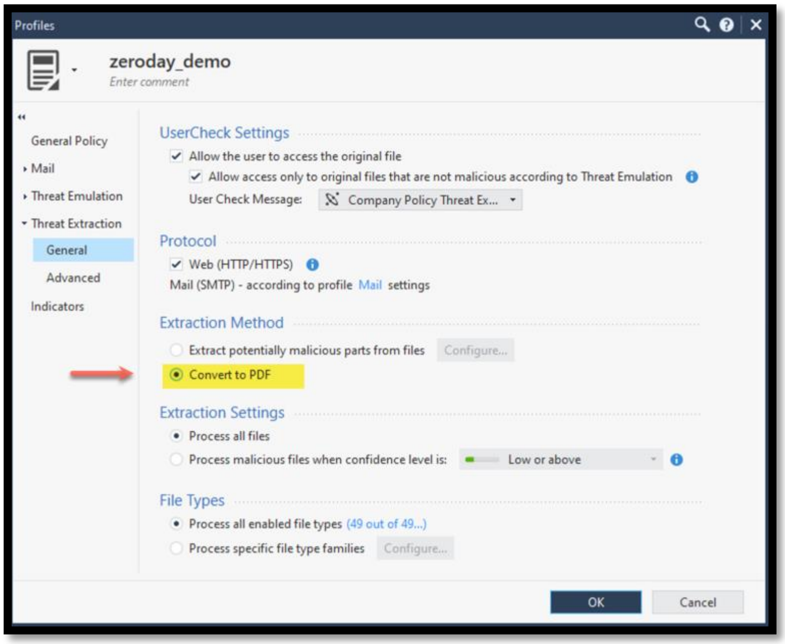


Rich Text Format	*rtf*	*Both*	*Extract*/Convert to PDF* ** From R80.40 Engine update 2*	*Extract*
Compressed graphic Format JPEG	*jpeg,jpg,jpe,jfif*	*mail*	Extract/Convert to PDF	*Extract*

Exercise 4: Extraction Methods

In the previous exercise, used the default configuration to extract the active exploitable content while keeping the original format. In this exercise, we will use a different approach. Convert the original file into text-based PDF file rendering active contents inactive.

1. Edit the Threat profile and change the extraction method to **Convert to PDF** and *Install the Threat Prevention Policy*.



Profiles

zeroday_demo
Enter comment

UserCheck Settings
- ☑ Allow the user to access the original file
  - ☑ Allow access only to original files that are not malicious according to Threat Emulation
- User Check Message: Company Policy Threat Ex...

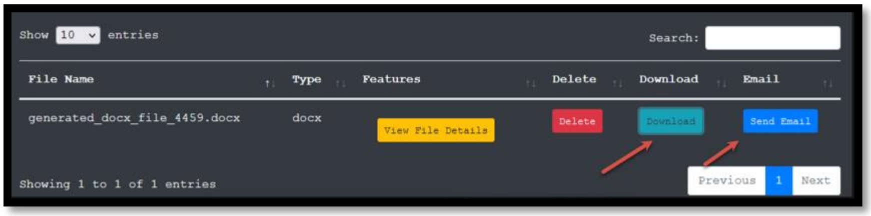
Protocol
- ☑ Web (HTTP/HTTPS)
- Mail (SMTP) - according to profile Mail settings

Extraction Method
- ○ Extract potentially malicious parts from files Configure...
- ● Convert to PDF

Extraction Settings
- ● Process all files
- ○ Process malicious files when confidence level is: Low or above

File Types
- ● Process all enabled file types (49 out of 49...)
- ○ Process specific file type families Configure...

2. From the demo server, generate a **DOCX** file. Download and send the file over email as well.

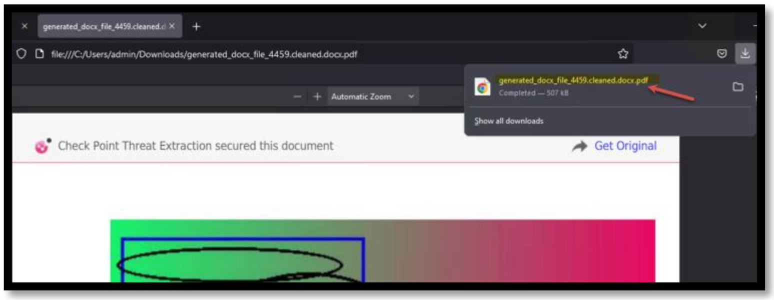


Show 10 entries — Search:

File Name	Type	Features	Delete	Download	Email
generated_docx_file_4459.docx	docx	View File Details	Delete	Download	Send Email

Showing 1 to 1 of 1 entries

3. Notice that the file was converted to a PDF file. This is indicated also in the file name.

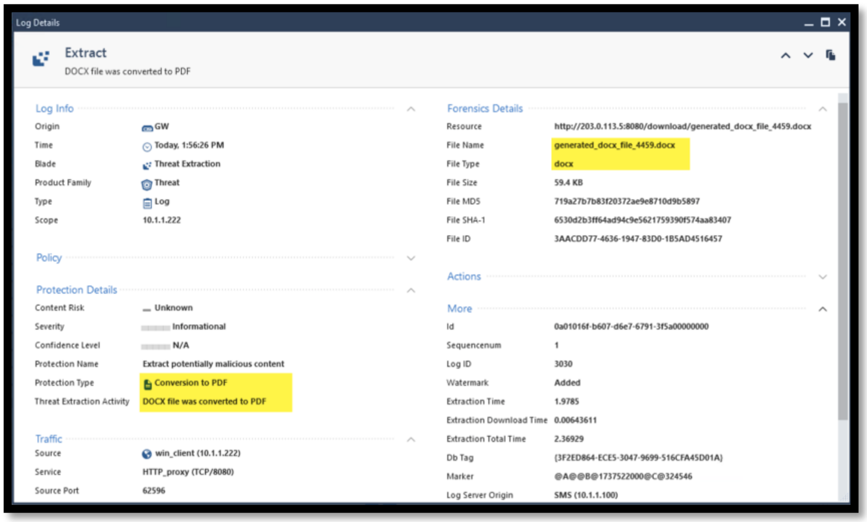


file:///C:/Users/admin/Downloads/generated_docx_file_4459.cleaned.docx.pdf

generated_docx_file_4459.cleaned.docx.pdf
Completed — 507 kB

Check Point Threat Extraction secured this document

4. Review the logs in SmartConsole. The log indicates that the DOCX file converted to a PDF file.



Log Details

Extract
DOCX file was converted to PDF

Log Info

Origin	GW
Time	Today, 1:56:26 PM
Blade	Threat Extraction
Product Family	Threat
Type	Log
Scope	10.1.1.222

Policy

Protection Details

Content Risk	Unknown
Severity	Informational
Confidence Level	N/A
Protection Name	Extract potentially malicious content
Protection Type	Conversion to PDF
Threat Extraction Activity	DOCX file was converted to PDF

Traffic

Source	win_client (10.1.1.222)
Service	HTTP_proxy (TCP/8080)
Source Port	62596

Forensics Details

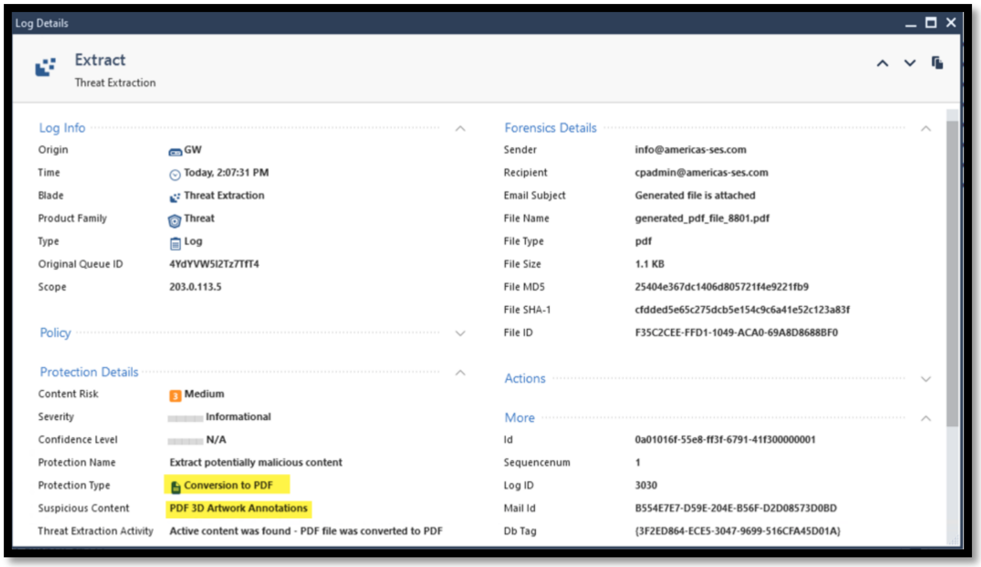
Resource	http://203.0.113.5:8080/download/generated_docx_file_4459.docx
File Name	generated_docx_file_4459.docx
File Type	docx
File Size	59.4 KB
File MD5	719a27b7b83f20372ae9e8710d9b5897
File SHA-1	6530d2b3ff64ad94c9e5621759390f574aa83407
File ID	3AACDD77-4636-1947-83D0-1B5AD4516457

Actions

More

Id	0a01016f-b607-d6e7-6791-3f5a00000000
Sequencenum	1
Log ID	3030
Watermark	Added
Extraction Time	1.9785
Extraction Download Time	0.00643611
Extraction Total Time	2.36929
Db Tag	{3F2ED864-ECE5-3047-9699-516CFA45D01A}
Marker	@A@@B@1737522000@C@324546
Log Server Origin	SMS (10.1.1.100)

5. Generate and download a PDF file. Notice that the log still indicates the Conversion to PDF. However, there are details regarding what contents where cleaned.



Log Details

Extract
Threat Extraction

Log Info

Origin	GW
Time	Today, 2:07:31 PM
Blade	Threat Extraction
Product Family	Threat
Type	Log
Original Queue ID	4YdYVW5I2Tz7TfT4
Scope	203.0.113.5

Policy

Protection Details

Content Risk	3 Medium
Severity	Informational
Confidence Level	N/A
Protection Name	Extract potentially malicious content
Protection Type	Conversion to PDF
Suspicious Content	PDF 3D Artwork Annotations
Threat Extraction Activity	Active content was found - PDF file was converted to PDF

Forensics Details

Sender	info@americas-ses.com
Recipient	cpadmin@americas-ses.com
Email Subject	Generated file is attached
File Name	generated_pdf_file_8801.pdf
File Type	pdf
File Size	1.1 KB
File MD5	25404e367dc1406d805721f4e9221fb9
File SHA-1	cfdded5e65c275dcb5e154c9c6a41e52c123a83f
File ID	F35C2CEE-FFD1-1049-ACA0-69A8D8688BF0

Actions

More

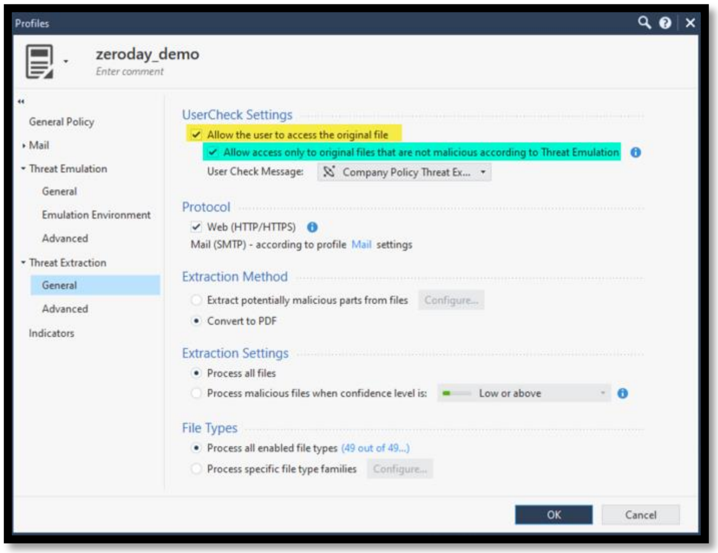
Id	0a01016f-55e8-ff3f-6791-41f300000001
Sequencenum	1
Log ID	3030
Mail Id	B554E7E7-D59E-204E-B56F-D2D08573D0BD
Db Tag	{3F2ED864-ECE5-3047-9699-516CFA45D01A}

Exercise 5: Accessing the Original Files

In some cases, the users need to access the original files before they are cleaned by Threat Extraction. Some of the components that are cleared might be necessary for the functionality of the cleaned file.

My default, the user is allowed to download the file in case Threat Emulation decided that the flie is clean. This behavior can be customized.

1. Review the profile and notice that we are allowing the user to access original files that are not malicious.



Profiles

zeroday_demo
Enter comment

UserCheck Settings
☑ Allow the user to access the original file
☑ Allow access only to original files that are not malicious according to Threat Emulation
User Check Message: Company Policy Threat Ex...

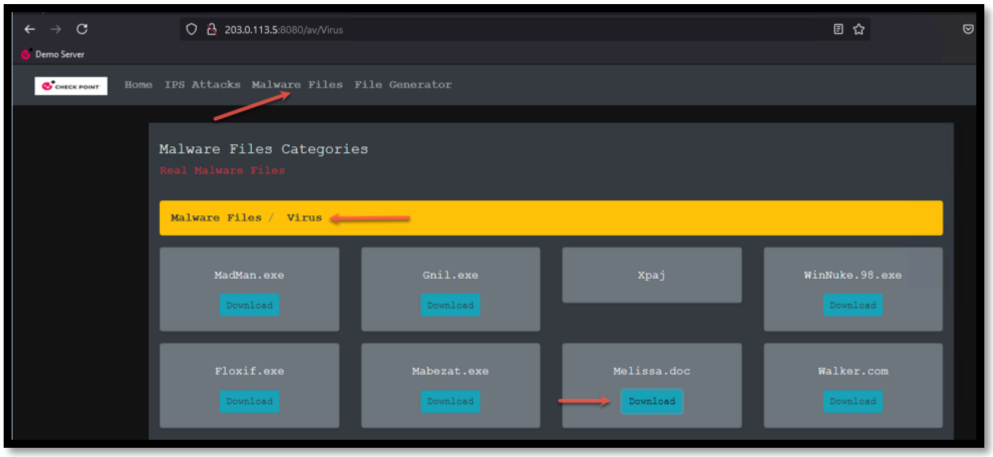
Protocol
☑ Web (HTTP/HTTPS)
Mail (SMTP) - according to profile Mail settings

Extraction Method
○ Extract potentially malicious parts from files Configure...
● Convert to PDF

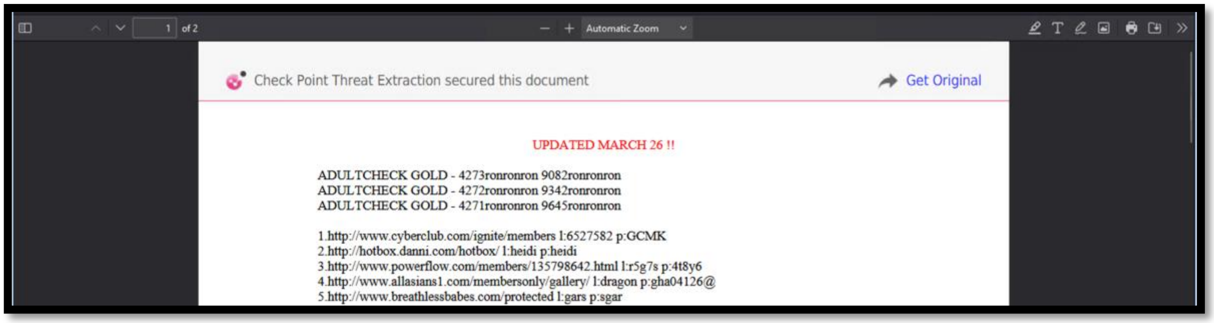
Extraction Settings
● Process all files
○ Process malicious files when confidence level is: Low or above

File Types
● Process all enabled file types (49 out of 49...)
○ Process specific file type families Configure...

2. From the demo server, navigate to Malware Files -> Virus and download the **malicious** document **Melissa.doc.**



3. Download the file. Notice that the cleaned file is accessible, and we can read it.



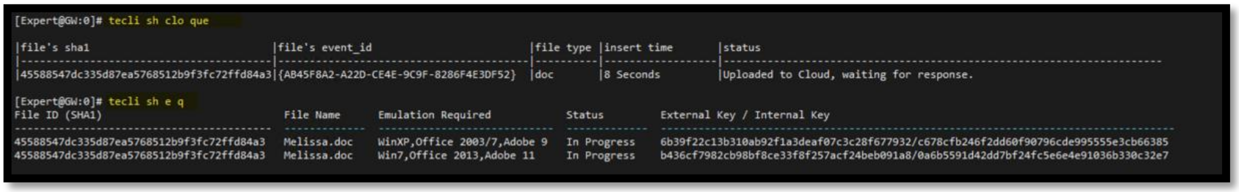
Check Point Threat Extraction secured this document

UPDATED MARCH 26 !!

ADULTCHECK GOLD - 4273ronronron 9082ronronron
ADULTCHECK GOLD - 4272ronronron 9342ronronron
ADULTCHECK GOLD - 4271ronronron 9645ronronron

1.http://www.cyberclub.com/ignite/members l:6527582 p:GCMK
2.http://hotbox.danni.com/hotbox/ l:heidi p:heidi
3.http://www.powerflow.com/members/135798642.html l:r5g7s p:4t8y6
4.http://www.allasians1.com/membersonly/gallery/ l:dragon p:gha04126@
5.http://www.breathlessbabes.com/protected l:gars p:sgar

4. Use the MobaXterm SSH client to connect tot eh GW and review the Threat Emulation queue. Notice that the file is being scanned in the background.



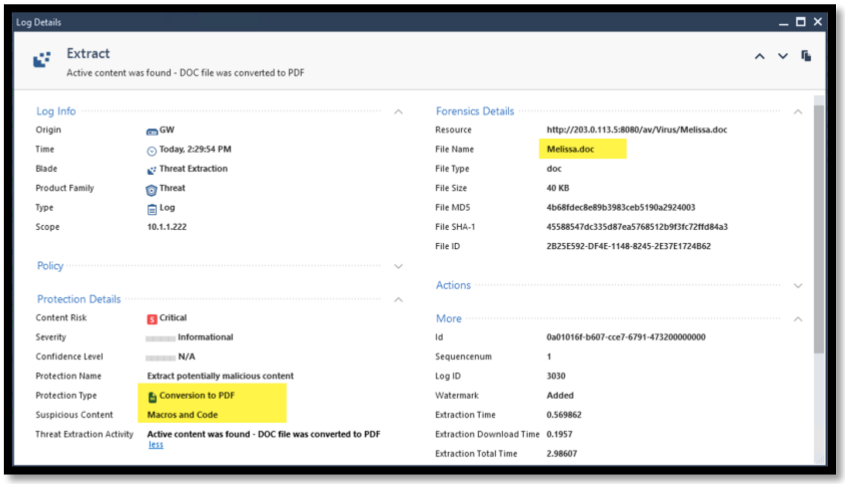
```
[Expert@GW:0]# tecli sh clo que

|file's sha1                             |file's event_id                         |file type |insert time      |status
|----------------------------------------|----------------------------------------|----------|-----------------|--------------------------------------------------------------------
|45588547dc335d87ea5768512b9f3fc72ffd84a3|{AB45F8A2-A22D-CE4E-9C9F-8286F4E3DF52}  |doc       |8 Seconds        |Uploaded to Cloud, waiting for response.

[Expert@GW:0]# tecli sh e q
File ID (SHA1)                            File Name      Emulation Required         Status         External Key / Internal Key
----------------------------------------  -------------  -------------------------  -------------  -------------------------------------------------------------------------------------
45588547dc335d87ea5768512b9f3fc72ffd84a3  Melissa.doc    WinXP,Office 2003/7,Adobe 9  In Progress  6b39f22c13b310ab92f1a3deaf07c3c28f677932/c678cfb246f2dd60f90796cde995555e3cb66385
45588547dc335d87ea5768512b9f3fc72ffd84a3  Melissa.doc    Win7,Office 2013,Adobe 11    In Progress  b436cf7982cb98bf8ce33f8f257acf24beb091a8/0a6b5591d42dd7bf24fc5e6e4e91036b330c32e7
```

- This shows an important benefit of using Threat Extraction. We deliver a proactively cleaned version of the files. Users are only allowed to retrieve the original file if Threat Emulation confirms that the file is clean.

5. Review the Threat Extraction log. It shows what active contents this file had.



Extract
Active content was found - DOC file was converted to PDF

Log Info

Origin	GW
Time	Today, 2:29:54 PM
Blade	Threat Extraction
Product Family	Threat
Type	Log
Scope	10.1.1.222

Policy

Protection Details

Content Risk	5 Critical
Severity	Informational
Confidence Level	N/A
Protection Name	Extract potentially malicious content
Protection Type	Conversion to PDF
Suspicious Content	Macros and Code
Threat Extraction Activity	Active content was found - DOC file was converted to PDF less

Forensics Details

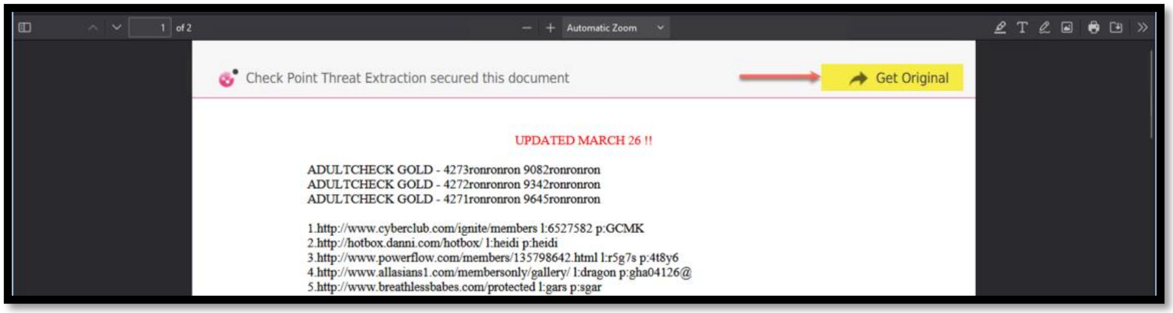
Resource	http://203.0.113.5:8080/av/Virus/Melissa.doc
File Name	Melissa.doc
File Type	doc
File Size	40 KB
File MD5	4b68fdec8e89b3983ceb5190a2924003
File SHA-1	45588547dc335d87ea5768512b9f3fc72ffd84a3
File ID	2B25E592-DF4E-1148-8245-2E37E1724B62

Actions

More

Id	0a01016f-b607-cce7-6791-473200000000
Sequencenum	1
Log ID	3030
Watermark	Added
Extraction Time	0.569862
Extraction Download Time	0.1957
Extraction Total Time	2.98607

6. The cleaned document includes a link to allow users to retrieve the original file via UserCheck. Click the **Get Original** link.



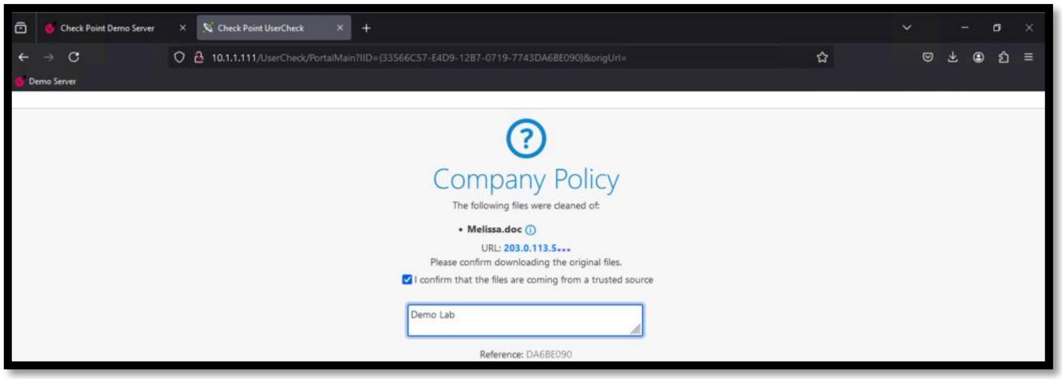
Check Point Threat Extraction secured this document

UPDATED MARCH 26 !!

ADULTCHECK GOLD - 4273ronronron 9082ronronron
ADULTCHECK GOLD - 4272ronronron 9342ronronron
ADULTCHECK GOLD - 4271ronronron 9645ronronron

1.http://www.cyberclub.com/ignite/members l:6527582 p:GCMK
2.http://hotbox.danni.com/hotbox/ l:heidi p:heidi
3.http://www.powerflow.com/members/135798642.html l:r5g7s p:4t8y6
4.http://www.allasians1.com/membersonly/gallery/ l:dragon p:gha04126@
5.http://www.breathlessbabes.com/protected l:gars p:sgar

7. The UserCheck retrieval processes requires a confirmation of the risk of the file.



10.1.1.111/UserCheck/PortalMain?IID={33566C57-E4D9-12B7-0719-7743DA6BE090}&origUrl=

Company Policy

The following files were cleaned of:

- **Melissa.doc**

URL: 203.0.113.5...

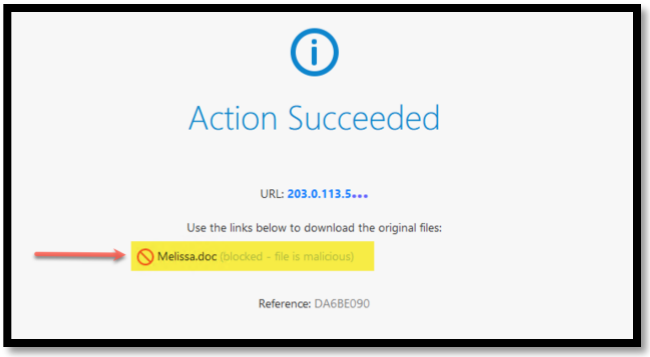
Please confirm downloading the original files.

☑ I confirm that the files are coming from a trusted source

Demo Lab

Reference: DA6BE090

8. As expected, the file was blocked, and the user was denied permission to download the original file.



Action Succeeded

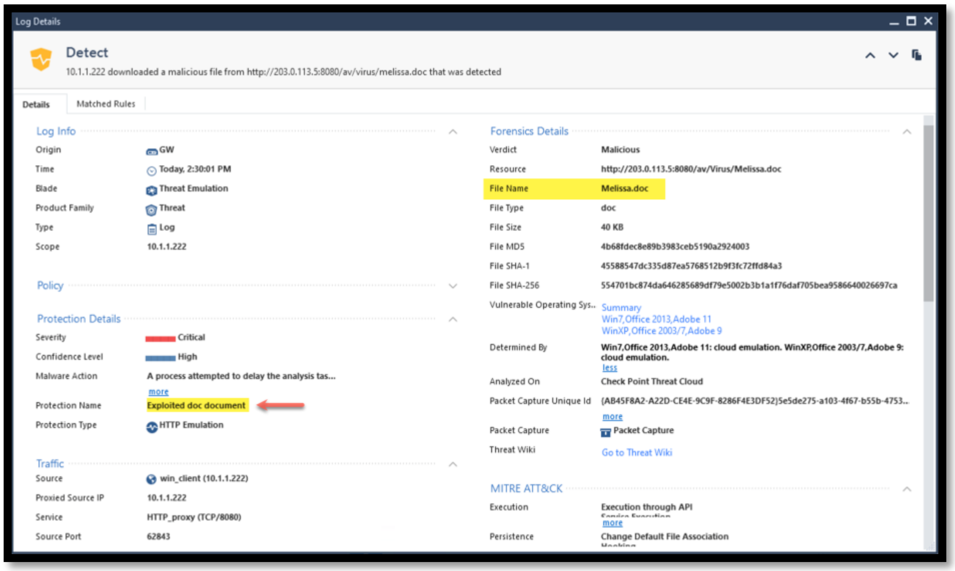
URL: 203.0.113.5...

Use the links below to download the original files:

Melissa.doc (blocked – file is malicious)

Reference: DA6BE090

9. Review the Threat Emulation logs and confirm that the file was found to be malicious by Threat Emulation as expected.



Detect

10.1.1.222 downloaded a malicious file from http://203.0.113.5:8080/av/virus/melissa.doc that was detected

Log Info

Origin	GW
Time	Today, 2:30:01 PM
Blade	Threat Emulation
Product Family	Threat
Type	Log
Scope	10.1.1.222

Policy

Protection Details

Severity	Critical
Confidence Level	High
Malware Action	A process attempted to delay the analysis tas... more
Protection Name	Exploited doc document
Protection Type	HTTP Emulation

Traffic

Source	win_client (10.1.1.222)
Proxied Source IP	10.1.1.222
Service	HTTP_proxy (TCP/8080)
Source Port	62843

Forensics Details

Verdict	Malicious
Resource	http://203.0.113.5:8080/av/Virus/Melissa.doc
File Name	Melissa.doc
File Type	doc
File Size	40 KB
File MD5	4b68fdec8e89b3983ceb5190a2924003
File SHA-1	45588547dc335d87ea5768512b9f3fc72ffd84a3
File SHA-256	554701bc874da646285689df79e5002b3b1a1f76daf705bea9586640026697ca
Vulnerable Operating Sys..	Summary Win7,Office 2013,Adobe 11 WinXP,Office 2003/7,Adobe 9
Determined By	Win7,Office 2013,Adobe 11: cloud emulation. WinXP,Office 2003/7,Adobe 9: cloud emulation. less
Analyzed On	Check Point Threat Cloud
Packet Capture Unique Id	{AB45F8A2-A22D-CE4E-9C9F-8286F4E3DF52}5e5de275-a103-4f67-b55b-4753.. more
Packet Capture	Packet Capture
Threat Wiki	Go to Threat Wiki

MITRE ATT&CK

Execution	Execution through API more
Persistence	Change Default File Association

End of Lab 10