

Threat Emulation

Expected Time: 45 Minutes

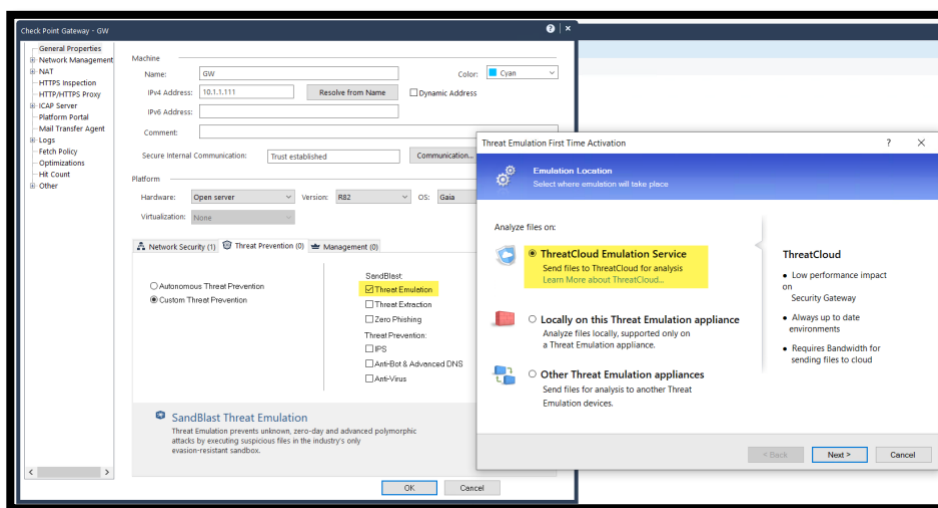
Introduction

The Check Point Threat Emulation quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network. The emulation service reports and automatically shares the newly identified threat information with other customers.

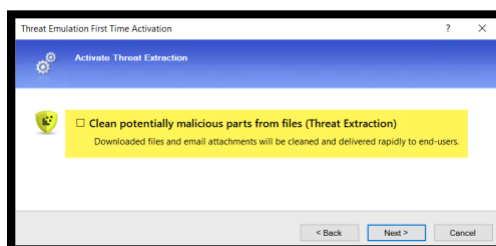
Exercise 1: Onboarding

In this exercise, we will enable the Threat Emulation blade. We do not have a local TE appliance, and we will be sending the files to the Threat Cloud for emulation.

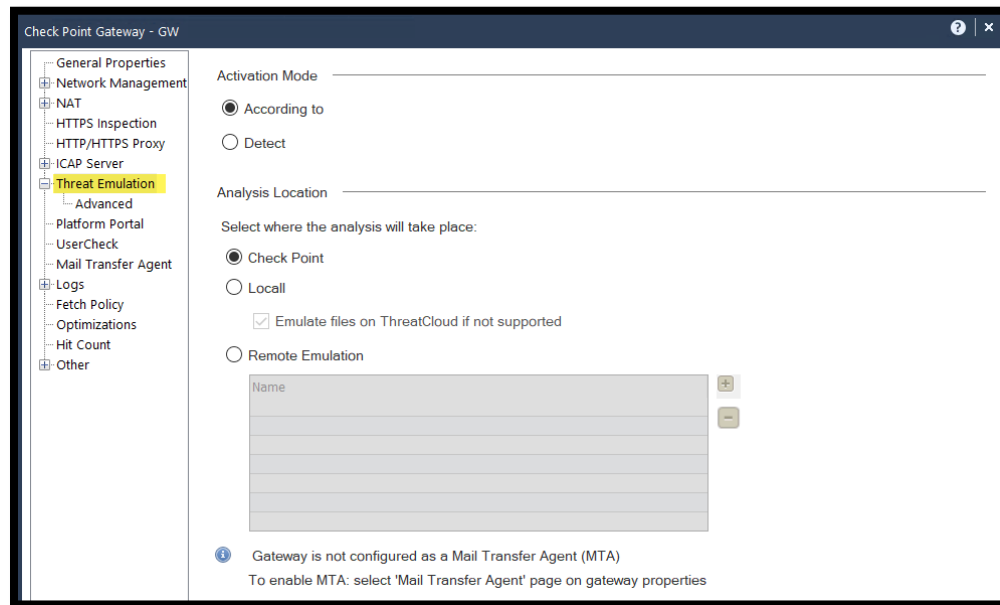
1. Edit the GW object and enable the Threat Emulation blade. Disable all other Threat Prevention blades.



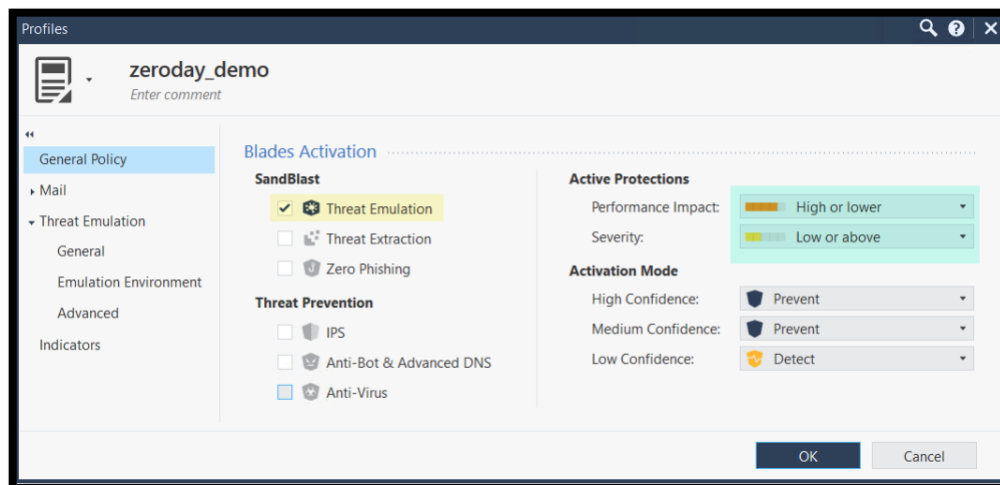
2. In the activation wizard, use the default choice to send the files to the Threat Cloud, and uncheck the option to enable Threat Extraction for now.



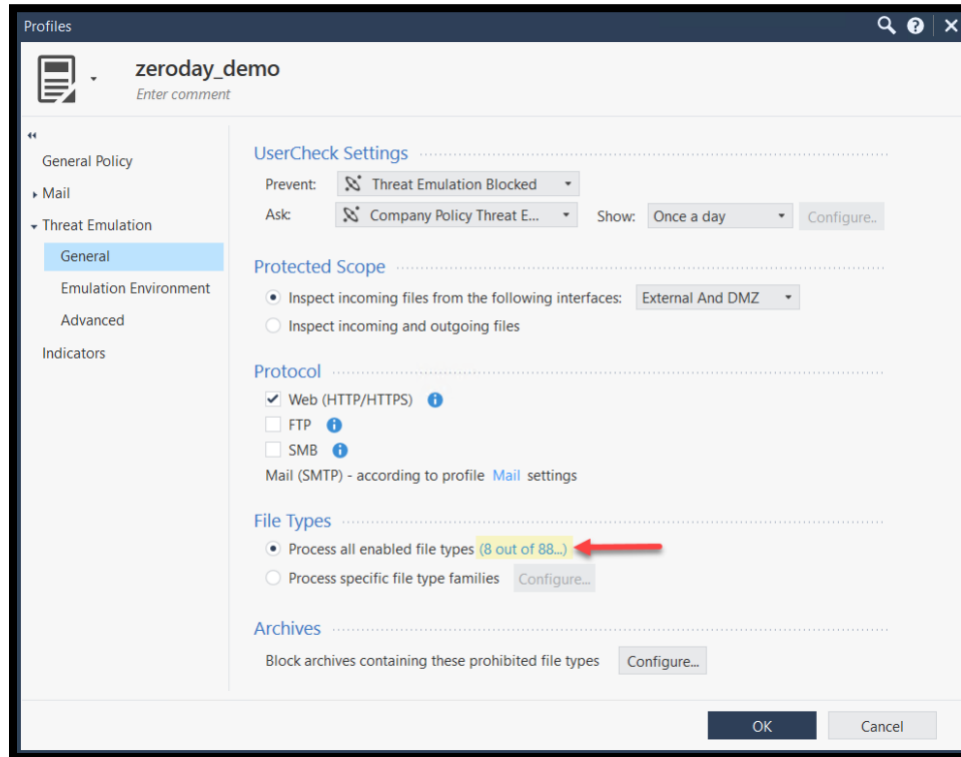
- Review the Threat Emulation tab, notice that all the choices we made via the First Time Wizard can be modified later. Click OK to close the object.



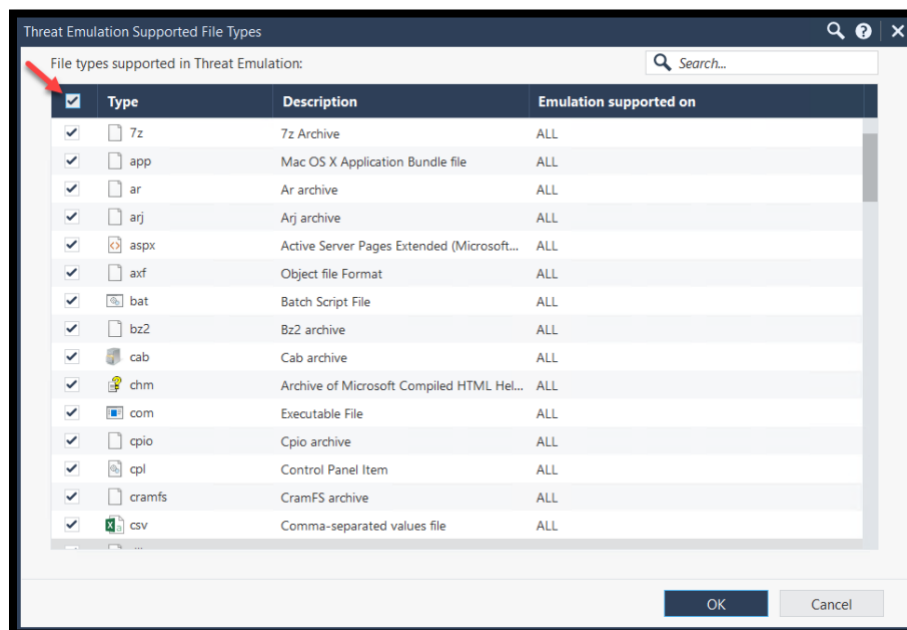
- Go to the Threat Prevention -> Profiles and then create a new profile with only Threat Emulation Enabled.



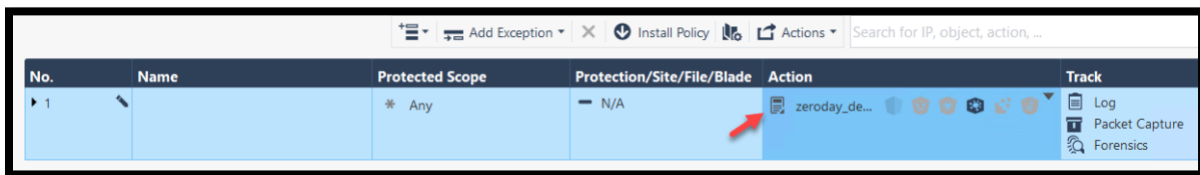
- Review the settings under the General tab and click on the enabled file link. By default, only a few file types are enabled by default.



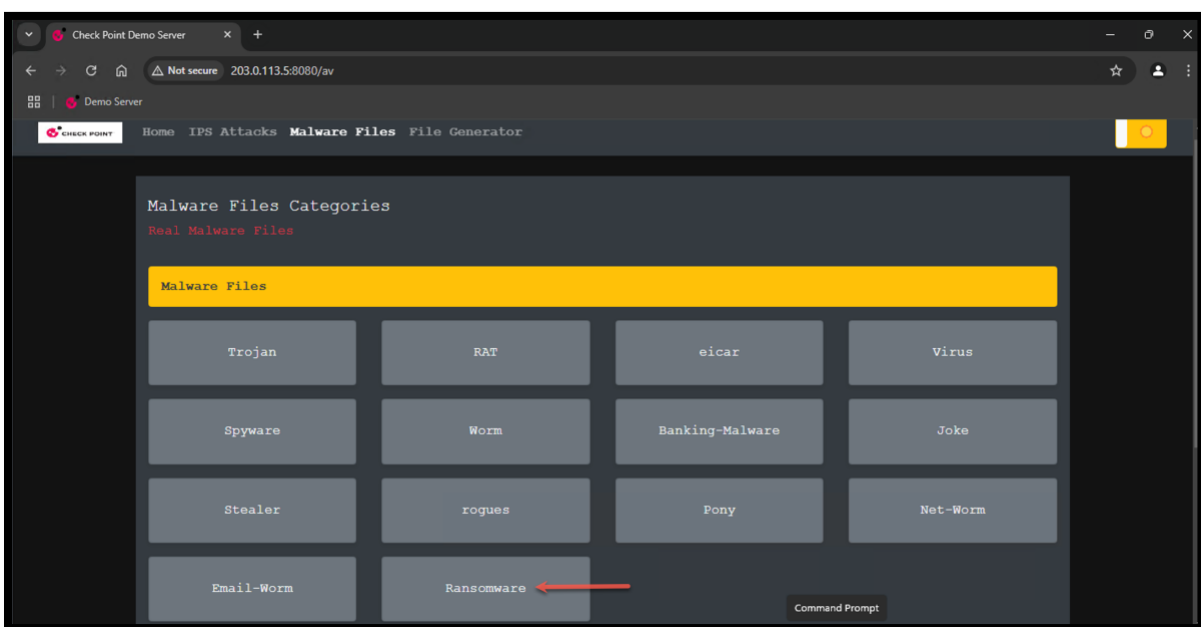
6. Check all supported file types, click Ok through the Pop-up about Emulation files are enabled immediately, the Threat Emulation blade will investigate all supported file types. Click OK to create the new profile.



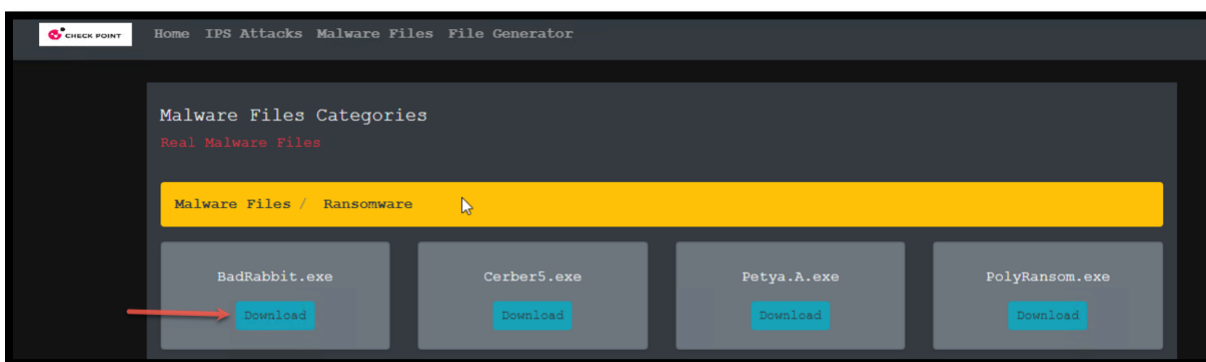
- Confirm that the correct profile is assigned to the Threat Prevention rule and Install the Access Control and Threat Prevention Policies.



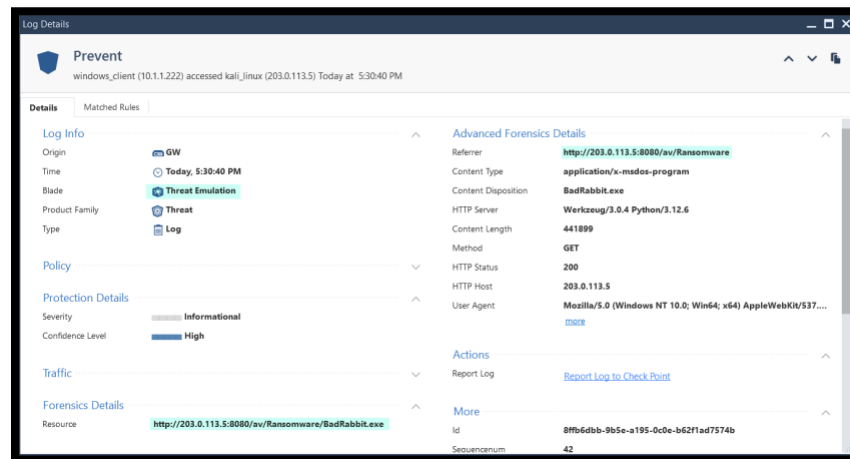
- From the Windows client, open the demo server and open the Ransomware directory



- Try to download the BadRabbit.exe ransomware.



- Check the log in SmartConsole, notice that the log still has limited fields. The investigation is expected to take around 5 minutes to complete even though the file is blocked instantly.

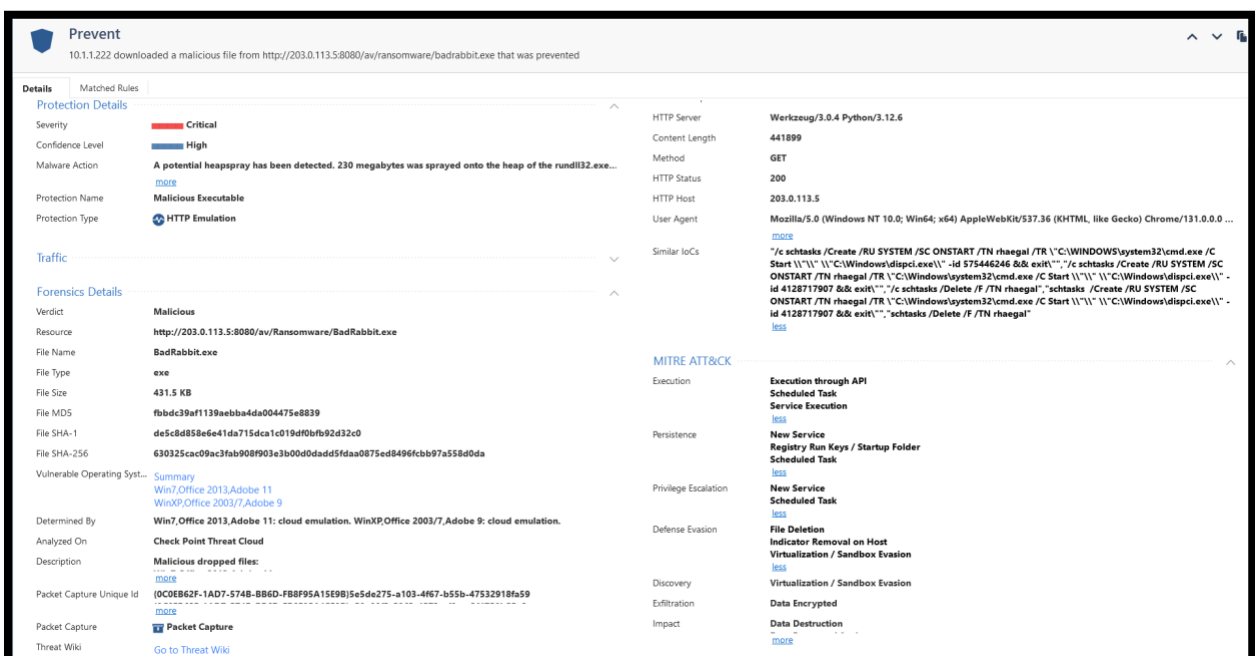


11. To monitor the progress of the file investigation on the cloud, connect to the GW over ssh and use the command **tecli show cloud queue**.

```
[Expert@GW:0]# tecli sh e q
```

File ID (SHA1)	File Name	Emulation Required	Status	External Key / Internal Key
de5c8d858e6e41da715dca1c019df0fb92d32c0	BadRabbit.exe	WinXP,Office 2003/7,Adobe 9	In Progress	48f70eeb356b623bc91c7b50409e8b2dc8d
50d5a/5279fa349265e841dc22961748114c83b1128c74	BadRabbit.exe	Win7,Office 2013,Adobe 11	In Progress	932e3f6ae34c0098a63d5ac904f0622843a
de5c8d858e6e41da715dca1c019df0fb92d32c0	BadRabbit.exe	Win7,Office 2013,Adobe 11	In Progress	932e3f6ae34c0098a63d5ac904f0622843a
44a36/b4a2eeaf8b3550c44bdaa8fabfaac30378c1aeec				

12. Once the investigation is done and the queue is empty, refresh the logs and notice that the log file was updated with the full investigation results.



Exercise 2: Threat Emulation Reports

When a malicious file is detected, multiple reports are regenerated by default. A summary report and a separate report for each of the OS versions used for the investigation.

1. Open the prevent log and click on the summary report link to open it.

Forensics Details

Verdict	Malicious
Resource	http://203.0.113.5:8080/av/Ransomware/BadRabbit.exe
File Name	BadRabbit.exe
File Type	exe
File Size	431.5 KB
File MD5	fbbdc39af1139aebba4da004475e8839
File SHA-1	de5c8d858e6e41da715dca1c019df0bfb92d32c0
File SHA-256	630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcb97a558d0da
Vulnerable Operating Syst...	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.
Analyzed On	Check Point Threat Cloud
Description	Malicious dropped files: more
Packet Capture Unique Id	{0C0EB62F-1AD7-574B-BB6D-FB8F95A15E9B}5e5de275-a103-4f67-b55b-47532918fa59 more
Packet Capture	Packet Capture
Threat Wiki	Go to Threat Wiki

2. Review the report and notice that the malicious file can be downloaded (password protected) via the Actions menu. The default password is (infected) and can be changed.

Threat Details Report

Download File

Copy Path to Clipboard

Contact Incident Response Team

630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcb97a558d0da

SIZE: 431.54 KB

TYPE: EXE

HASH list

Verdict

Malicious

Action (Defined in Profile)

Prevent

Confidence

High

Secure / Risk

Critical

Classification

Ransomware, Trojan

Learn more with Horizon XDR Intelligence

ATTACK VECTOR

27/11/2024 17:33

http://203.0.113.5:8080/av/Ranso...

203.0.113.5

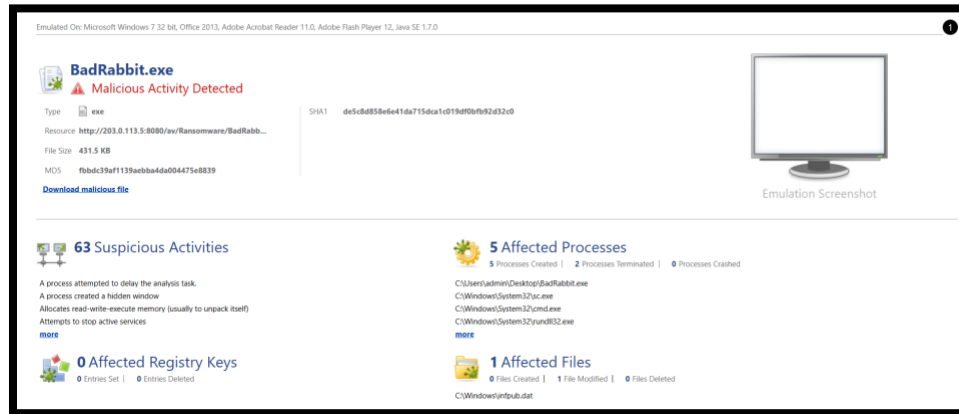
→

BadRabbit.exe

10.1.1.222

©2025 Check Point Software Technologies Ltd. All rights reserved | P. 6

- Open the other two reports and review the level of details for activities made during the investigation on each OS.



- Try to download multiple Ransomware files and make sure the logs are generated.

★ Queries < > 🔍 Last 24 Hours blade:"Threat Emulation"

Found 31 results (229 ms)

Time	B...	A...	T...	Seve...	Con...	Protection Ty...	Protection Na...	File Name	Event Type	File Size	File MD5	File Type	Resource	Source
Today, 12:27:20 PM						HTTP Emulati...	Malicious Execut...	WannaCry.exe		224 KB	5c7fb0927d...	exe	http://203.0...	windows_client (...)
Today, 12:27:14 PM						HTTP Emulati...	Malicious Execut...	RedBoot.exe		1.2 MB	e0340f456f...	exe	http://203.0...	windows_client (...)
Today, 12:27:12 PM						HTTP Emulati...	Malicious Execut...	NotPetya.exe		390 KB	5b7e6e352...	exe	http://203.0...	windows_client (...)
Today, 12:27:09 PM						HTTP Emulati...	Malicious Execut...	CryptoWall.exe		132 KB	919034c8ef...	exe	http://203.0...	windows_client (...)
Today, 12:27:07 PM						HTTP Emulati...	Malicious Execut...	UIWIX.exe		211.8 KB	a933a1a40...	dll	http://203.0...	windows_client (...)

- Notice that some files were not blocked at the first attempt and the logs show a Detect log!

Detect 10.1.1.222 downloaded a malicious file from http://203.0.113.5:8080/av/ransomware/uiwix.exe that was detected

Log Info

- Origin: GW
- Time: Today, 12:27:07 PM
- Blade: Threat Emulation
- Product Family: Threat
- Type: Log
- Scope: 10.1.1.222

Policy

- Action: **Detect**
- Threat Prevention Rule ID: 8f07c5c8-6f47-4c83-a01c-7847c85005f3
- Threat Prevention Policy: Standard
- Policy Date: Today, 12:24:23 PM
- Threat Prevention Policy D...: Today, 12:26:55 PM
- Policy Name: Standard
- Policy Management: SMS
- Threat Profile: zeroday_demo
- Origin Log Server IP: 10.1.1.100
- Add Exception...

Protection Details

- Severity: Critical
- Confidence Level: High
- Malware Action: Behaves like a known malware (Generic.MALWARE.Bed7)
- Protection Name: Malicious Executable
- Protection Type: HTTP Emulation

Forensics Details

- Verdict: Malicious
- Resource: http://203.0.113.5:8080/av/Ransomware/UIWIX.exe
- File Name: UIWIX.exe
- File Type: dll
- File Size: 211.8 KB
- File MD5: a933a1a402775cf94b6bee0963f4b46
- File SHA-1: 18aa7b02f933c73989ba3d16698a5ee3a4d9420
- File SHA-256: 146581f0b3fbc00026ec3e6e68797b0e57f9d1d8aacc99fd3290e9cfad0fc
- Vulnerable Operating Syst...: Summary Win7,Office 2013,Adobe 11 Win9,Office 2003,7,Adobe 9
- Determined By: Win7,Office 2013,Adobe 11: cloud emulation. WinXP,Office 2003,7,Adobe 9: cloud emulation.
- Analyzed On: Check Point Threat Cloud
- Description: File type reclassified to: dll.
- Packet Capture Unique Id: (E882A412-4457-2549-BE82-FA38F7919389)5e5de275-a103-4f67-b55b-47532918fa59
- Packet Capture: Packet Capture
- Threat Wiki: Go to Threat Wiki

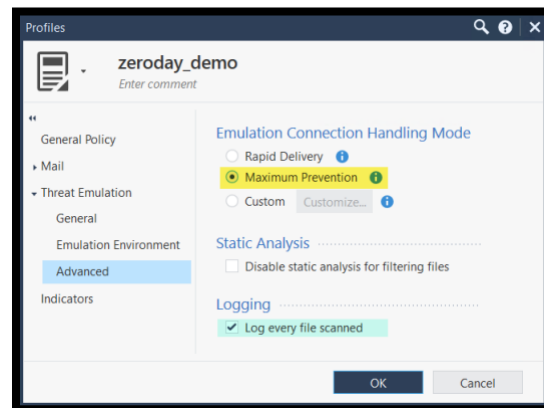
Actions

- Remediation: Go to Remediation Options
- Report Log: Report Log to Check Point

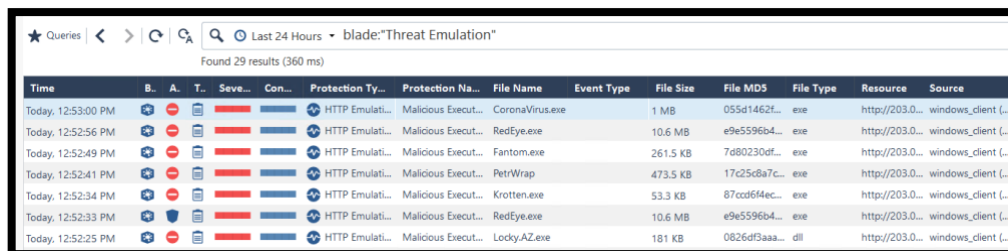
More

- Id: 3bf82be-8993-91f7-e882-a41244572549
- Sequencium: 1
- Log ID: 4000

- Change the profile settings to Maximum Prevention. In this mode, the user will not be allowed to get a copy of the file at the first attempt until the analysis is done and we can confirm that it is not malicious. Notice that we also log every file scanned. A log will be generated even if it found to be clean.

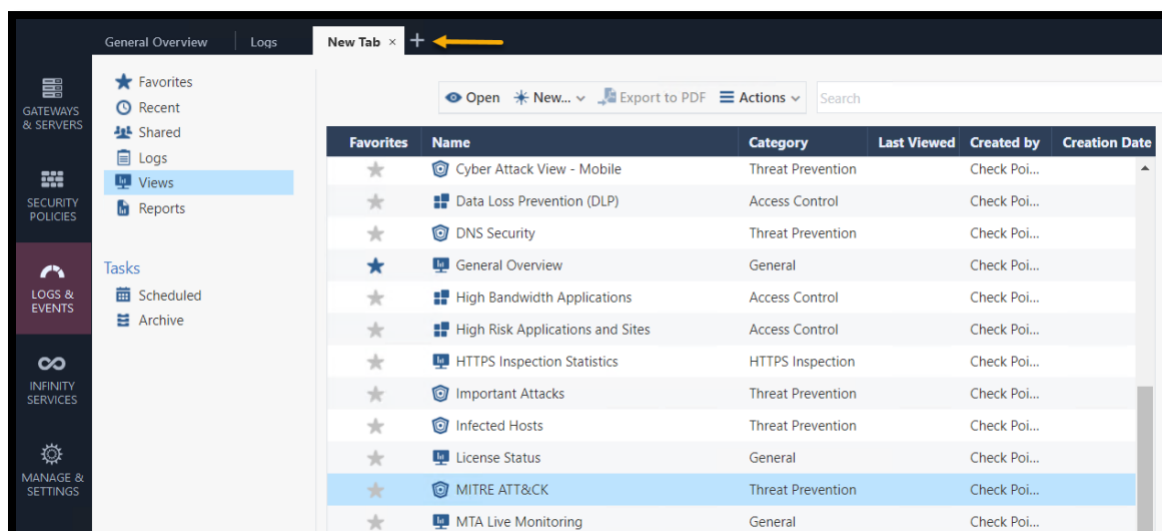


- Install the Threat Prevention Policy and test more files. Make sure we are preventing malicious files at the first download attempt!



Time	B.	A.	T.	Seve...	Con...	Protection Ty...	Protection Na...	File Name	Event Type	File Size	File MD5	File Type	Resource	Source
Today, 12:53:00 PM						HTTP Emulati...	Malicious Execut...	CoronaVirus.exe		1 MB	055d1462f...	exe	http://203.0... windows_client (...)	
Today, 12:52:56 PM						HTTP Emulati...	Malicious Execut...	RedEye.exe		10.6 MB	e9e5596b4...	exe	http://203.0... windows_client (...)	
Today, 12:52:49 PM						HTTP Emulati...	Malicious Execut...	Fantom.exe		261.5 KB	7d80230df...	exe	http://203.0... windows_client (...)	
Today, 12:52:41 PM						HTTP Emulati...	Malicious Execut...	PetrWrap		473.5 KB	17c25c8a7c...	exe	http://203.0... windows_client (...)	
Today, 12:52:34 PM						HTTP Emulati...	Malicious Execut...	Krotten.exe		53.3 KB	87cc06f4ec...	exe	http://203.0... windows_client (...)	
Today, 12:52:33 PM						HTTP Emulati...	Malicious Execut...	RedEye.exe		10.6 MB	e9e5596b4...	exe	http://203.0... windows_client (...)	
Today, 12:52:25 PM						HTTP Emulati...	Malicious Execut...	Locky.AZ.exe		181 KB	0826df3aaa...	dll	http://203.0... windows_client (...)	

- Open a new tab in the logs view and select and open **MITRE ATT&CK** view.



- Review the results and generate more logs by downloading more malware files. Review other out of the box views and reports.

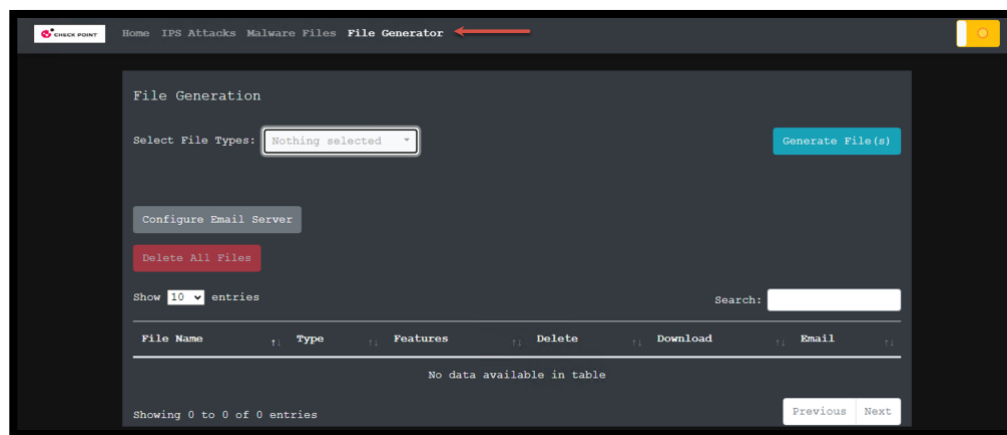
General Overview | Logs | MITRE ATT&CK

Queries | Last 24 Hours | Enter search query (Ctrl+F)

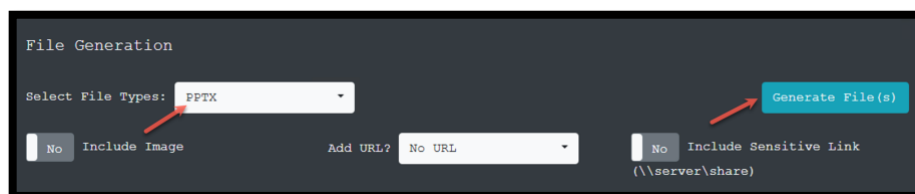
MITRE ATT&CK

Initial Access 0	Execution 9	Persistence 6	Privilege Escalation 3	Defense Evasion 9	Credential Access 3	Discovery 8	Lateral Movement 0	Collection 4	Command and Control 0	Exfiltration 8	Impact 8
Drive-by Compromise (0)	AppleScript (0)	.bash_profile and .bashrc (0)	Access Token Manipulation (0)	Access Token Manipulation (0)	Account Manipulation (0)	Account Discovery (0)	AppleScript (0)	Audio Capture (0)	Commonly Used Port (0)	Automated Exfiltration (0)	Account Access Removal (0)
Exploit Public-Facing Application (0)	CMSTP (0)	Accessibility Features (0)	Accessibility Features (0)	Binary Padding (0)	Bash History (0)	Application Window Discovery (2)	Application Deployment Software (0)	Automated Collection (0)	Communication Through Removable Media (0)	Data Compressed (2)	Data Destruction (8)
External Remote Services (0)	Compiled HTML File (1)	Account Manipulation (0)	AppCert DLLs (0)	ByPass User Account Control (0)	Credential Dumping (0)	Browser Bookmark Discovery (1)	Component Object Model and Distributed COM (0)	Clipboard Data (2)	Data from Information Repositories (0)	Data Encrypted (8)	Data Encrypted for Impact (7)
Hardware Additions (0)	Component Object Model and Distributed COM (0)	AppCert DLLs (0)	Appinit DLLs (0)	Clear Command History (0)	Credentials from Web Browsers (0)	Domain Trust Discovery (0)	Exploitation of Remote Services (0)	Data from Local System (1)	Custom Command and Control Protocol (0)	Data Transfer Size Limits (0)	Defacement (1)
Replication Through Removable Media (0)	Control Panel Items (0)	Application Shimming (0)	Bypass User Account Control (0)	CMSTP (0)	Credentials in Files (0)	File and Directory Discovery (0)	Internal Spearphishing (0)	Data from Network Shared Drive (0)	Custom Cryptographic Protocol (0)	Exfiltration Over Alternative Protocol (0)	Disk Content Wipe (0)
Spearphishing Attachment (0)	Dynamic Data Exchange (0)	Authentication Package (0)	DLL Search Order Hijacking (0)	Code Signing (0)	Credentials in Registry (0)	Network Service Scanning (0)	Logon Scripts (0)	Data from Removable Media (0)	Data Obfuscation (0)	Exfiltration Over Command and Control Channel (0)	Disk Structure Wipe (0)
Spearphishing Link (0)	Execution through API (9)	BITS Jobs (0)	Dylib Hijacking (0)	Compiled HTML File (1)	Exploitation for Credential Access (0)	Network Share Discovery (0)	Pass the Hash (0)	Data Staged (0)	Data Encoding (0)	Exfiltration Over Other Network Medium (0)	Endpoint Denial of Service (0)
Spearphishing via Service (0)	Execution through Module Load (0)	Bootkit (0)	Elevated Execution with Prompt (0)	Component Firmware (0)	Forced Authentication (0)	Network Sniffing (0)	Pass the Ticket (0)	Email Collection (0)	Domain Obfuscation (0)	Exfiltration Over Physical Medium (0)	Firmware Corruption (0)
Supply Chain	Exploitation for	Change Default File Association (3)	Exploitation for Privilege Escalation (0)	Component Object Model Hijacking (0)	Hooking (1)	Password Policy Discovery (0)	Remote Desktop Protocol (0)	Input Capture (3)	Domain Fronting (0)	Exfiltration Over Scheduled Transfer (0)	Inhibit System Recovery (1)
							Remote File Copy (0)	Man in the Browser			Network Denial of Service (0)

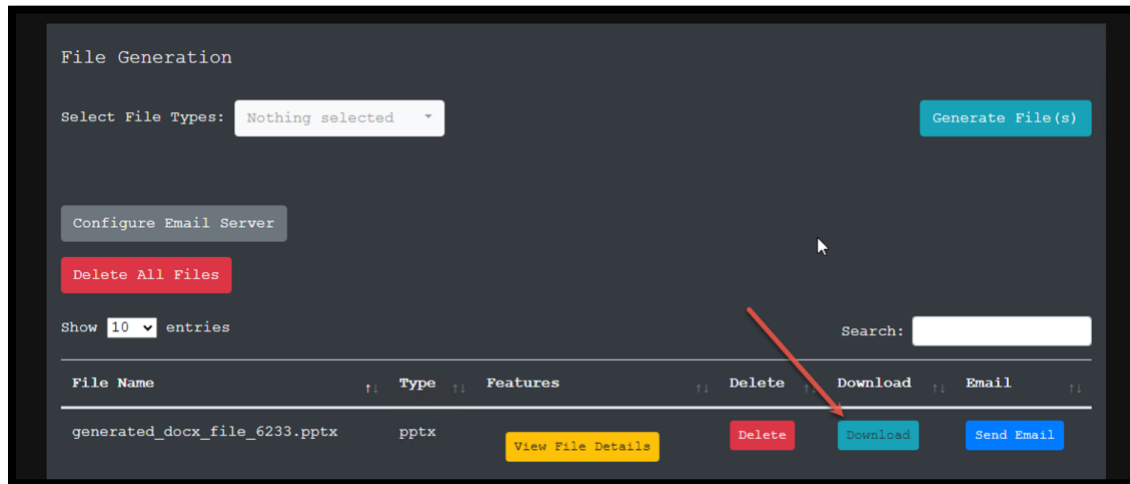
- From **win_client**, browse to the Demo Server to the File Generator. You can use this service to generate new unique files to confirm they have not been analyzed by Threat Cloud before.



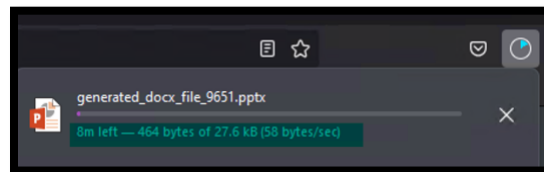
- Select a file type to generate, for example, select **PPTX** and click Generate File(s).



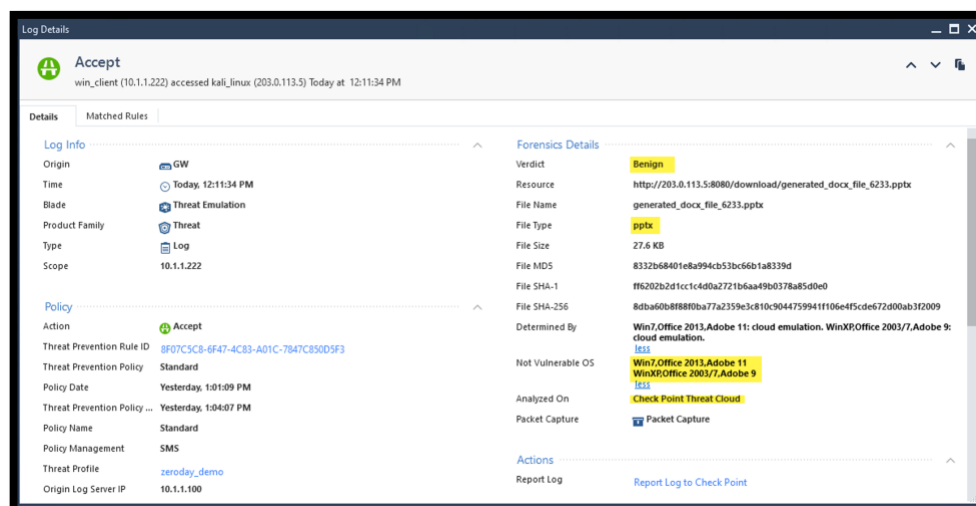
11. A unique **PPTX** file will be generated. Click download to download the file.



12. Notice that the file download shows a progress slower than normal for a small file. This is because the file is being scanned in the background by Threat Emulation and is handled by the Maximum Prevention Mode. The file download will not be allowed to complete unless the cloud response indicates the file was benign.



13. Review the log and pay attention to the analysis location and the verdict

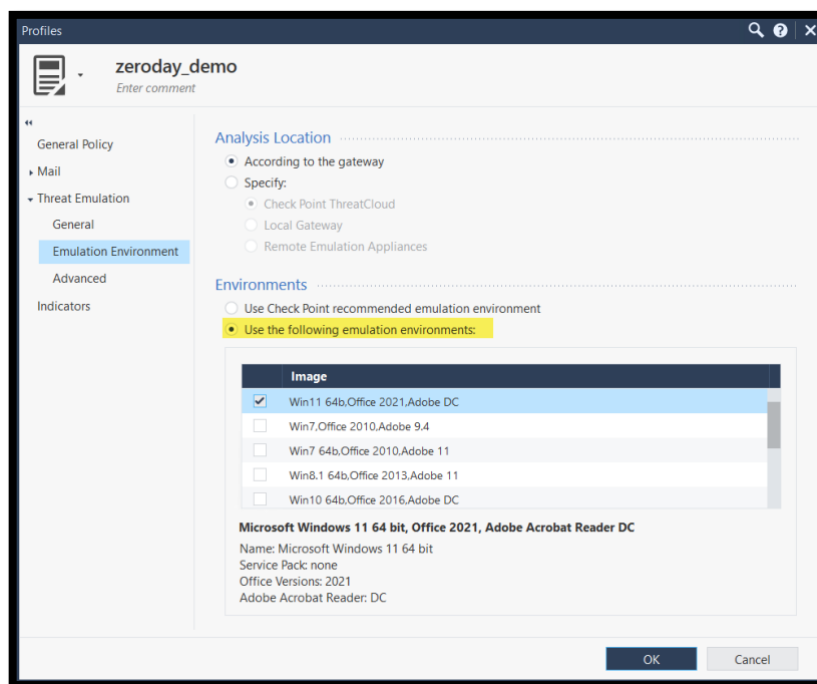


Exercise 3: Threat Emulation Environment

By Default, all files are analyzed on the recommended images, Windows XP and Windows 7 with Adobe 11 and MS Office 2013 installed. Those two OS versions are less secure than the more recent versions and more malicious activities might be recorded. The only exception to this rule is the executable file where they can only be scanned on 64-bit operating systems.

However, in some cases, we would like to change the analysis to be done on specific images. In this exercise, we will change the emulation to be done only on Windows 11 images.

1. Edit the profile and change the emulation environment to Windows 11 only. Notice that the Log will only show a report from Windows 11. Install the **Threat Prevention** policy.



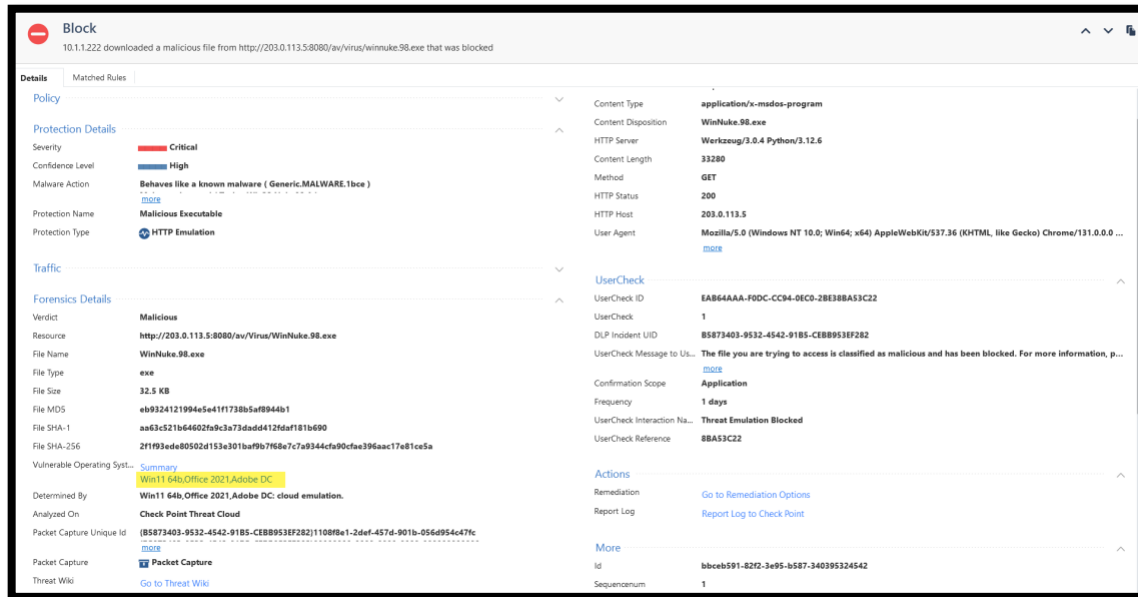
2. Try to download a **malicious file** from the demo server. Notice that while the file can be blocked instantly, the full report will be available once the analysis is complete. Monitor the progress of the file analysis using the command:

o **tecli sh em que**

```
Last login: Thu Nov 28 13:44:23 2024 from 10.1.1.200
[Expert@GW:0]# tecli sh e q
```

File ID (SHA1)	File Name	Emulation Required	Status	External Key / Internal Key
aa63c521b64602fa9c3a73dadd412fdaf181b690 9809e8f0a21/3195dcb4e98ae60599edc6dfa2e695e9b5d064cf	WinNuke.98...	Win11 64b, Office 2021, Ado...	In Progress	b68c34831d505d38d550adb764e90

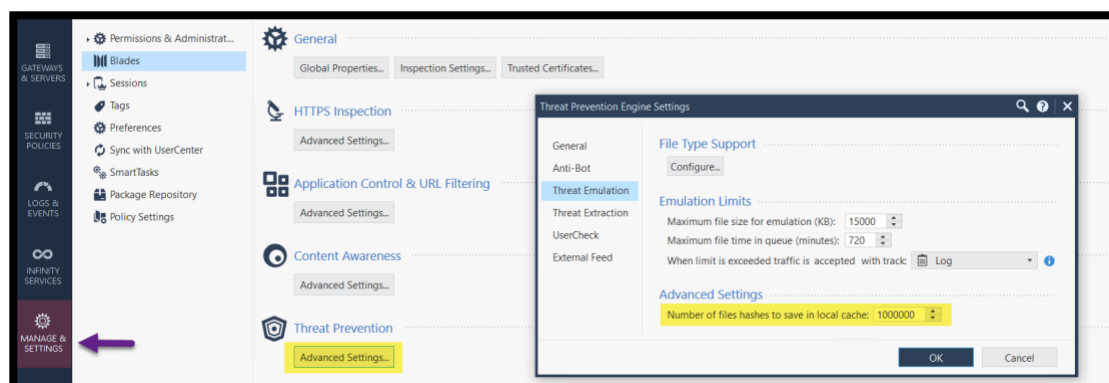
- Once the Emulation is done and the queue is empty, review the logs and notice that OS and the report is showing windows 11 as expected.



Exercise 4: Threat Emulation Advanced Settings

Multiple settings can be modified globally to all Threat Emulation enabled Gateways. Those settings include, the maximum file size scanned by TE, the time files wait in queue, cache size and the file type support. We will navigate through the settings in this exercise.

- Navigate to the Threat Prevention advanced settings. Notice that the Maximum file size scanned by default is 15 MB. The size of cache is 1M entries.



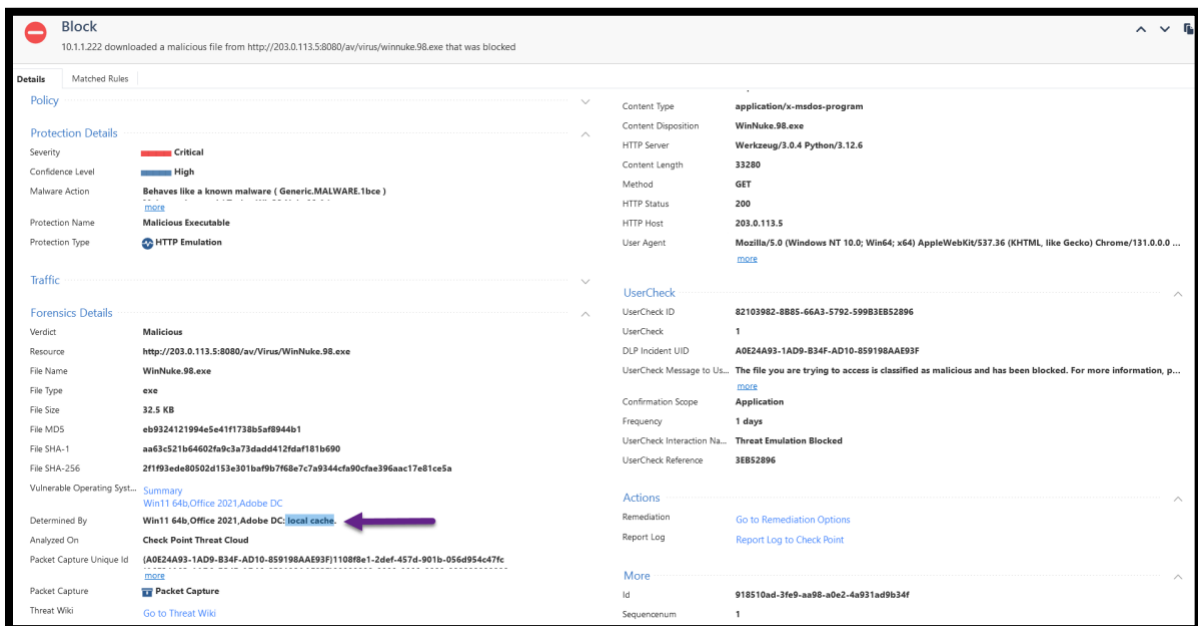
2. Login to the GW over SSH and review the content of the local cache. Use the command **tecli** **cache dump all** to see the content of the cache.

```
[Expert@GW:0]# tecli cache dump all

Images Uid List
=====
Image UID: 1108f8e1-2def-457d-901b-056d954c47fc, Image: Win11 64b,Office 2021,Adobe DC

|sha1|file type|image|verdict|confidence|severity|date|hits|ttl|comment|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|e686139d5ed8528117ba6ca68fe415e4fb02f2be|exe|Win7,Office 2013,Adobe 11|malicious|High|Critical|11-28-2024|1|12-6-2024|dlpu_te
|e686139d5ed8528117ba6ca68fe415e4fb02f2be|exe|WinXP,Office 2003/7,Adobe 9|malicious|High|Critical|11-28-2024|1|12-6-2024|dlpu_te
|747070c74d0400cffe28fba17b64297f14cfbd|exe|Win7,Office 2013,Adobe 11|malicious|High|Critical|11-28-2024|1|12-6-2024|dlpu_te
```

3. Files that are handled already, have entries in the local cache. In case a file verdict is already known and saved in the cache, the decision will be forced without having to rescan the file. Try to download a file twice and notice that the second attempt is blocked based on the decision from the local cache.



Block
 10.1.1.222 downloaded a malicious file from http://203.0.113.5:8080/av/virus/winnuke.98.exe that was blocked

Details | Matched Rules

Policy

Protection Details

Severity: **Critical**

Confidence Level: **High**

Malware Action: **Behaves like a known malware (Generic.MALWARE.1bce)**

Protection Name: **Malicious Executable**

Protection Type: **HTTP Emulation**

Traffic

Forensics Details

Verdict: **Malicious**

Resource: **http://203.0.113.5:8080/av/virus/winnuke.98.exe**

File Name: **WinNuke.98.exe**

File Type: **exe**

File Size: **32.5 KB**

File MD5: **eb9324121994e5e41f1738b5af8944b1**

File SHA-1: **aa63c521b6402fa9c3a73dad412daf181b690**

File SHA-256: **2f1f93ede80502d153e301ba9b768e7c7a9344cfa90cfae396aac17e81ce5a**

Vulnerable Operating Syst...: **Summary**

Determined By: **Win11 64b,Office 2021,Adobe DC**

Analyzed On: **Check Point Threat Cloud**

Packet Capture Unique Id: **(A0E24A93-1AD9-B34F-AD10-859198AAE93F)1108f8e1-2def-457d-901b-056d954c47fc**

Packet Capture: **more**

Threat Wiki: **Go to Threat Wiki**

UserCheck

UserCheck ID: **82103982-8885-66A3-5792-59983EB52896**

UserCheck: **1**

DLP Incident UID: **A0E24A93-1AD9-B34F-AD10-859198AAE93F**

UserCheck Message to Us...: **The file you are trying to access is classified as malicious and has been blocked. For more information, p...**

Confirmation Scope: **Application**

Frequency: **1 days**

UserCheck Interaction Na...: **Threat Emulation Blocked**

UserCheck Reference: **3EB52896**

Actions

Remediation: **Go to Remediation Options**

Report Log: **Report Log to Check Point**

More

Id: **918510ad-3fe9-aa98-a0e2-4a931ad9b34f**

Sequencium: **1**

4. To clear the cache entries, use the command **tecli cache clean** or **tecli c c**

```
[Expert@GW:0]# tecli c c
[Expert@GW:0]# tecli c d a

Images Uid List
=====
Image UID: 1108f8e1-2def-457d-901b-056d954c47fc, Image: Win11 64b,Office 2021,Adobe DC

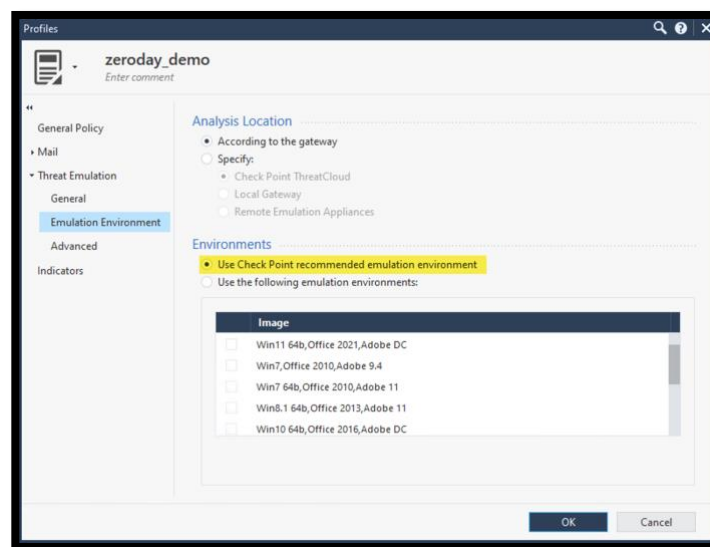
|sha1|file type|image|verdict|confidence|severity|date|hits|ttl|comment|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
```

- Attempt to download a file and notice that all files are now go through analysis since the cache is empty.

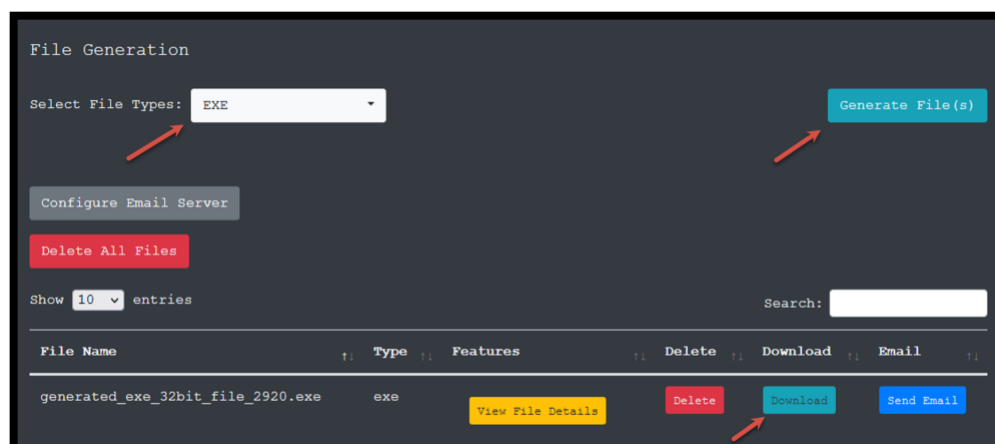
```
[Expert@GW:0]# tecli sh em qu
```

File ID (SHA1)	File Name	Emulation Required	Status	External Key / Internal Key
713b4678c05a76dbd22e6f8d738c9ef655e70226fdc6037e	Gnll.exe	Win11 64b,Office 2021,Ado...	In Progress	2a01d30b45c28faa6d7b1fd101900489256476af/505262f1dd0139a9ec38f6bbc66792e5

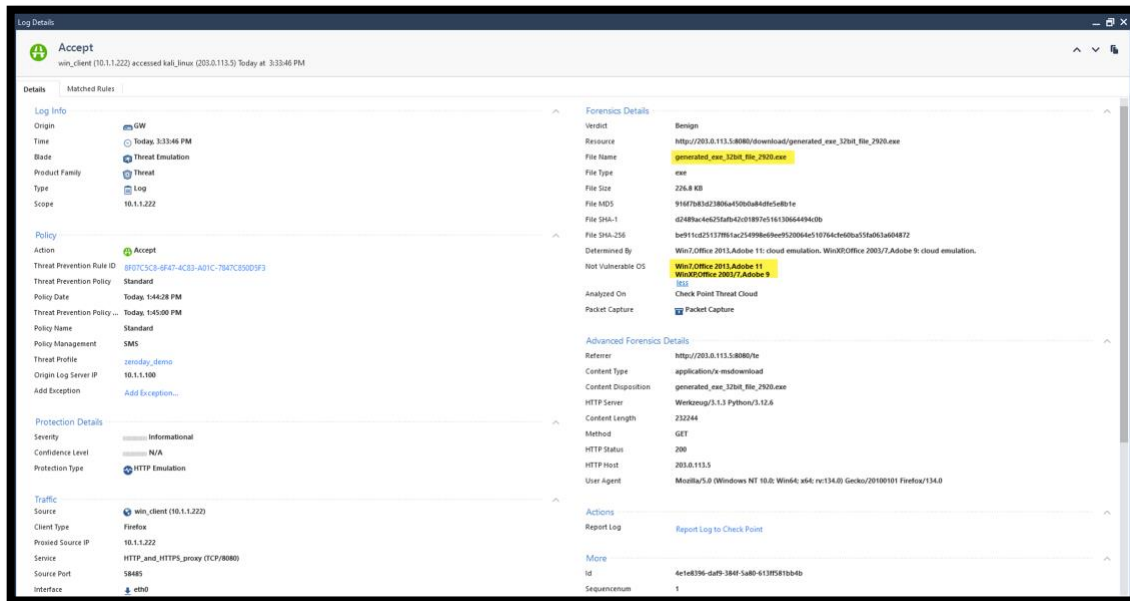
- Edit the profile and revert the environment changes to use the recommended emulation environment.



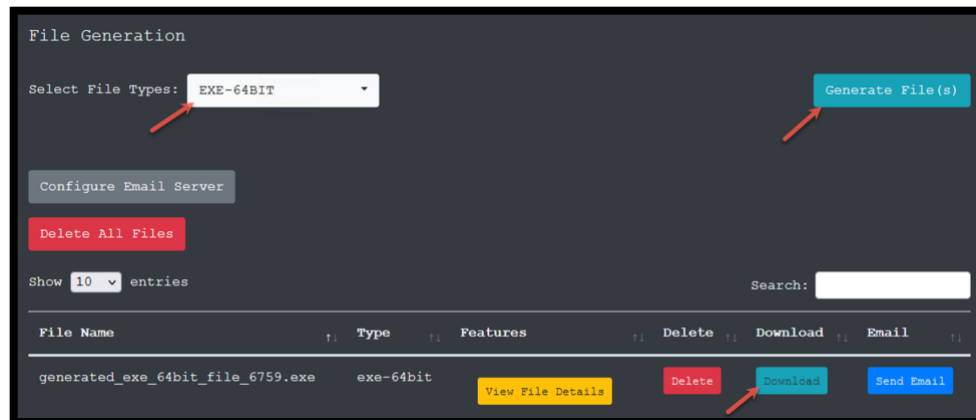
- Install the **Threat Prevention Policy**
- Back from the win_client, use the demo server to generate and download a new executable **EXE** file. This represents a 32-bit executable.



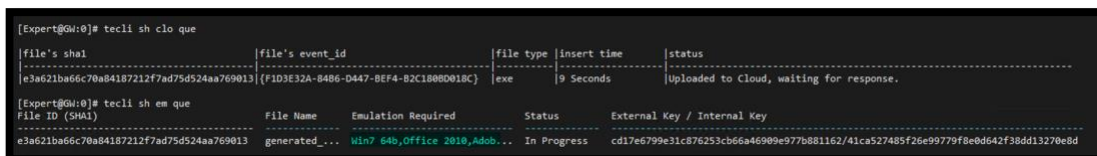
9. Review the log and confirm that the recommended images were used to scan the file.



10. Generate a 64-bit executable file and try to download it.



11. Check the Threat Emulation Queue and notice that only one image was used to scan the file.



- This is expected. Only 64b images are capable of running/scanning 64-bit file.

End of Lab 8