



Security Assessment Detailed Report

REPORT:

ANTI-VIRUS TEST REPORT

ASSESSMENT:

ANTI-VIRUS TEST

Report Generated on

02/28/2024 - 11:41 am (UTC)

Report Generated by:

username: Abdulazeez Mohammad

email:

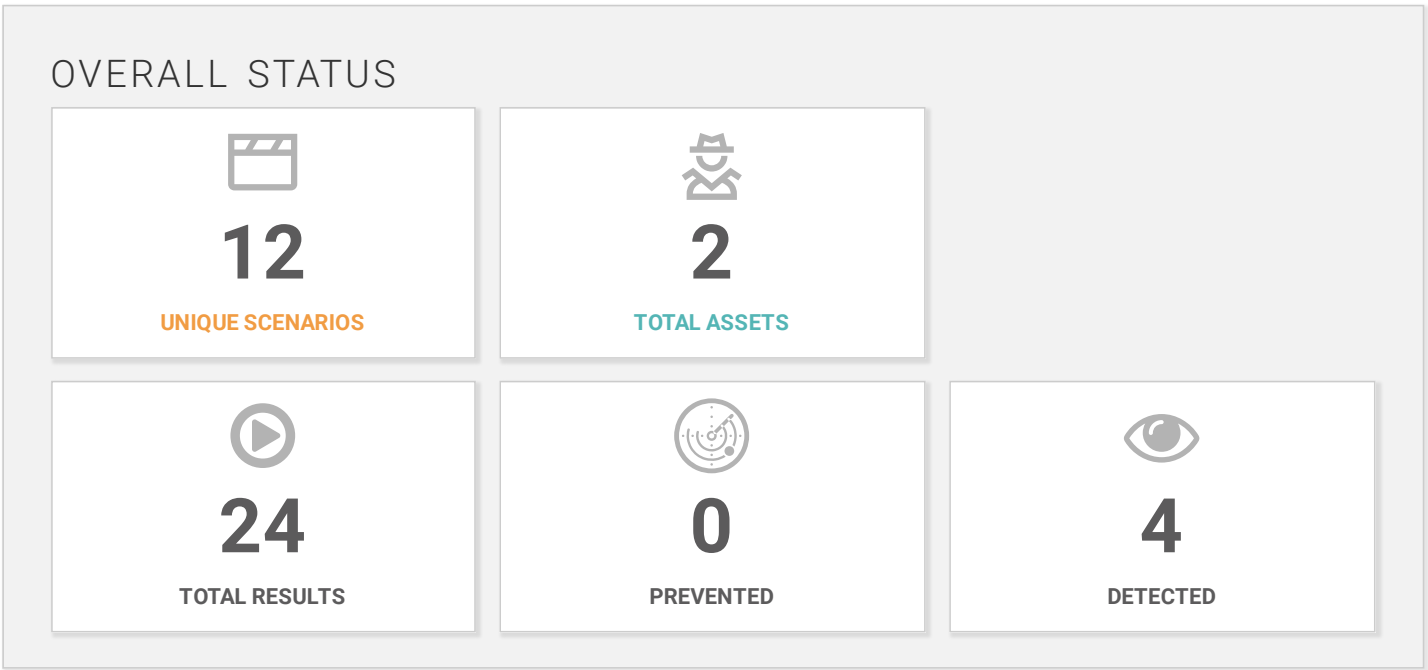
mohammad.abdulazeez@virtuallytestingfoundation.org

EXECUTIVE SUMMARY

This is a general assessment report containing results from an assessment. The information starts at an executive summary level with overall scenario pass rates and then progresses to increasingly detailed information about individual scenarios, assets, and mitigation recommendations.


DEFINITIONS

- Scenario:** a Scenario is a package of scripted behaviors to mimic attack activity or validate security controls.
- Asset:** a machine or device in your network on which the AttackIQ agent is installed. AttackIQ agents execute scenarios on their machines or devices.
- Result:** an instance of a scenario executed on a particular asset.
- Prevented:** when the execution of the intended behavior carried out by a Scenario is unsuccessful. This result is determined by the AttackIQ Agent and Scenario execution.
- Detected:** when an attack carried out by a Scenario has been observed in the logs of a Vendor Product / Security Control in the customer environment. This result is determined by the Integrations Manager and the integrations that have been configured.



TEST OVERVIEW

Total tests (3)

TESTS	SCENARIOS	USER PRIVILEGES*	ASSETS	TECHNOLOGIES	PREVENTION	DETECTION
EICAR	4	SYSTEM	2	No detections	<div><div></div></div> 100%	<div><div></div></div> 100%
Ransomware Memory	4	SYSTEM	2	No detections	<div><div></div></div> 100%	<div><div></div></div> 100%
Ransomware Disk	4	SYSTEM	2		<div><div></div></div> 100%	<div><div></div><div></div></div> 50% 50%

* User Privileges are SYSTEM for Linux and MacOS assets

THREAT ASSESSMENT (AMONG ALL ASSETS EXERCISED)



EICAR
100% not blocked (8)



Ransomware Memory
100% not blocked (8)



Ransomware Disk
100% not blocked (8)

** Percentages are truncated*

TOP MITIGATION RECOMMENDATIONS

Mitigation	Occurrences	Scenarios
Content Filter Best Practices	16	Download Robinhood's ransomware STEEL application killer to Memory, Download TXT EICAR file to Memory, Download Robinhood's ransomware RBNL malicious driver to Memory, Download Double Zipped EICAR file to Memory, Download EICAR file to Memory, Download Zip EICAR file to Memory, Download Maze Ransomware Sample to Memory, Download Coverton Ransomware to Memory
Malware Protection Best Practices	8	Save Robinhood's ransomware RBNL malicious driver to File System, Save Robinhood's ransomware ROBNR driver installer to File System, Save Robinhood's ransomware STEEL application killer to File System, Save Maze Ransomware Sample to File System

SCENARIOS OVERVIEW

Based upon the pass rate of assets tested, these are scenarios you may want to watch closely.

Scenario Name	Pass Rate
Download Robinhood's ransomware STEEL application killer to Memory	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Download Coverton Ransomware to Memory	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Download EICAR file to Memory	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Download Robinhood's ransomware RBNL malicious driver to Memory	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Save Robinhood's ransomware ROBNR driver installer to File System	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Save Maze Ransomware Sample to File System	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Save Robinhood's ransomware STEEL application killer to File System	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Download Double Zipped EICAR file to Memory	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Download Maze Ransomware Sample to Memory	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Download TXT EICAR file to Memory	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Save Robinhood's ransomware RBNL malicious driver to File System	0% PASSED, 100% FAILED, 0% OTHER <div></div>
Download Zip EICAR file to Memory	0% PASSED, 100% FAILED, 0% OTHER <div></div>

ASSETS OVERVIEW

Based upon the pass rate of assets tested, there are assets you may want to watch closely.

Asset Name	Pass Rate
acad2815-un	0% PASSED, 100% FAILED, 0% OTHER <div></div>
acad6969-prot	0% PASSED, 100% FAILED, 0% OTHER <div></div>

SCENARIO DETAILS

The following pages contain details and results for each scenario that was run as part of this project.

DOWNLOAD ROBINHOOD'S RANSOMWARE STEEL APPLICATION KILLER TO MEMORY SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

DOWNLOAD ROBINHOOD'S RANSOMWARE STEEL APPLICATION KILLER TO MEMORY

One of the most common actions for malware is to drop files to the filesystem. This scenario mimics part of that behavior by downloading a file and storing it in memory. The file SHA256 hash will be validated against the parameter provided hash in order to validate that the file was not modified in-transit.

This scenario has many parameters already configured to achieve its intent, which can be checked in the scenario template description for this scenario ("Download File to Memory"). The only parameters that could be modified without altering the scenario intent are the HTTP proxy-related parameters. The "HTTP Proxy" parameter allows selecting between using the default environment HTTP proxy settings, and manually specifying the HTTP proxy settings to be used for the file download. The "Proxy Address" and "Proxy Authentication Method" allow setting the HTTP proxy configuration to be used for the file download. These options only appear if "HTTP Proxy" is set to "Manual settings".

Although this scenario is not really complex, it lets you efficiently and easily test your network security controls by downloading the latest malware samples.

The scenario outcome will be Not Prevented if the file can be downloaded to memory and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:10 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:10 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

DOWNLOAD COVERTON RANSOMWARE TO MEMORY SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

DOWNLOAD COVERTON RANSOMWARE TO MEMORY

One of the most common actions for malware is to drop files to the filesystem. This scenario mimics part of that behavior by downloading a file and storing it in memory. The file SHA256 hash will be validated against the parameter provided hash in order to validate that the file was not modified in-transit.

This scenario has many parameters already configured to achieve its intent, which can be checked in the scenario template description for this scenario ("Download File to Memory"). The only parameters that could be modified without altering the scenario intent are the HTTP proxy-related parameters. The "HTTP Proxy" parameter allows selecting between using the default environment HTTP proxy settings, and manually specifying the HTTP proxy settings to be used for the file download. The "Proxy Address" and "Proxy Authentication Method" allow setting the HTTP proxy configuration to be used for the file download. These options only appear if "HTTP Proxy" is set to "Manual settings".

Although this scenario is not really complex, it lets you efficiently and easily test your network security controls by downloading the latest malware samples.

The scenario outcome will be Not Prevented if the file can be downloaded to memory and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:09 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:10 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

DOWNLOAD EICAR FILE TO MEMORY SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

DOWNLOAD EICAR FILE TO MEMORY

One of the most common actions for malware is to drop files to the filesystem. This scenario mimics part of that behavior by downloading a file and storing it in memory. The file SHA256 hash will be validated against the parameter provided hash in order to validate that the file was not modified in-transit.

This scenario has many parameters already configured to achieve its intent, which can be checked in the scenario template description for this scenario ("Download File to Memory"). The only parameters that could be modified without altering the scenario intent are the HTTP proxy-related parameters. The "HTTP Proxy" parameter allows selecting between using the default environment HTTP proxy settings, and manually specifying the HTTP proxy settings to be used for the file download. The "Proxy Address" and "Proxy Authentication Method" allow setting the HTTP proxy configuration to be used for the file download. These options only appear if "HTTP Proxy" is set to "Manual settings".

Although this scenario is not really complex, it lets you efficiently and easily test your network security controls by downloading the latest malware samples.

The scenario outcome will be Not Prevented if the file can be downloaded to memory and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:09 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:09 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Download File	<div>Failed</div>	<ul style="list-style-type: none">Content Filter Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Download File	<div>Failed</div>	<ul style="list-style-type: none">Content Filter Best Practices

DOWNLOAD ROBINHOOD'S RANSOMWARE RBNL MALICIOUS DRIVER TO MEMORY SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

DOWNLOAD ROBINHOOD'S RANSOMWARE RBNL MALICIOUS DRIVER TO MEMORY

One of the most common actions for malware is to drop files to the filesystem. This scenario mimics part of that behavior by downloading a file and storing it in memory. The file SHA256 hash will be validated against the parameter provided hash in order to validate that the file was not modified in-transit.

This scenario has many parameters already configured to achieve its intent, which can be checked in the scenario template description for this scenario ("Download File to Memory"). The only parameters that could be modified without altering the scenario intent are the HTTP proxy-related parameters. The "HTTP Proxy" parameter allows selecting between using the default environment HTTP proxy settings, and manually specifying the HTTP proxy settings to be used for the file download. The "Proxy Address" and "Proxy Authentication Method" allow setting the HTTP proxy configuration to be used for the file download. These options only appear if "HTTP Proxy" is set to "Manual settings".

Although this scenario is not really complex, it lets you efficiently and easily test your network security controls by downloading the latest malware samples.

The scenario outcome will be Not Prevented if the file can be downloaded to memory and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:10 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:10 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

SAVE ROBINHOOD'S RANSOMWARE ROBNR DRIVER INSTALLER TO FILE SYSTEM SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

SAVE ROBINHOOD'S RANSOMWARE ROBNR DRIVER INSTALLER TO FILE SYSTEM

This scenario takes a Robinhood's ransomware ROBNR driver installer and save it to the file system.

The file content is provided AES encrypted to the scenario. The scenario will decrypt the content and save it to the disk, then make a copy of it. Finally, both files are checked against the expected hash of the original file.

The file is copied to make sure that it hasn't been quarantined / deleted by any security control. The same applies for the hash calculation.

The scenario has two parameters:

- A delay in seconds to apply between each operation to give the security controls time to react. The default is 3 seconds.
- The path where the files are created. By default, a folder in the OS TEMP folder is used (the user's TEMP folder when running under user privileges).

The scenario outcome will be Not Prevented if the file can be saved and copied to the file system and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:12 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:13 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Save File To Disk And Copy It	<div>Failed</div>	<ul style="list-style-type: none">Malware Protection Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Save File To Disk And Copy It	<div>Failed</div>	<ul style="list-style-type: none">Malware Protection Best Practices

SAVE MAZE RANSOMWARE SAMPLE TO FILE SYSTEM SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

SAVE MAZE RANSOMWARE SAMPLE TO FILE SYSTEM

This scenario takes a Maze Ransomware Sample and save it to the file system.

The file content is provided AES encrypted to the scenario. The scenario will decrypt the content and save it to the disk, then make a copy of it. Finally, both files are checked against the expected hash of the original file.

The file is copied to make sure that it hasn't been quarantined / deleted by any security control. The same applies for the hash calculation.

The scenario has two parameters:

- A delay in seconds to apply between each operation to give the security controls time to react. The default is 3 seconds.
- The path where the files are created. By default, a folder in the OS TEMP folder is used (the user's TEMP folder when running under user privileges).

The scenario outcome will be Not Prevented if the file can be saved and copied to the file system and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:15 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:15 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Save File To Disk And Copy It	Failed	<ul style="list-style-type: none">Malware Protection Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Save File To Disk And Copy It	Failed	<ul style="list-style-type: none">Malware Protection Best Practices

SAVE ROBINHOOD'S RANSOMWARE STEEL APPLICATION KILLER TO FILE SYSTEM SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

SAVE ROBINHOOD'S RANSOMWARE STEEL APPLICATION KILLER TO FILE SYSTEM

This scenario takes a Robinhood's ransomware STEEL application killer and save it to the file system.

The file content is provided AES encrypted to the scenario. The scenario will decrypt the content and save it to the disk, then make a copy of it. Finally, both files are checked against the expected hash of the original file.

The file is copied to make sure that it hasn't been quarantined / deleted by any security control. The same applies for the hash calculation.

The scenario has two parameters:

- A delay in seconds to apply between each operation to give the security controls time to react. The default is 3 seconds.
- The path where the files are created. By default, a folder in the OS TEMP folder is used (the user's TEMP folder when running under user privileges).

The scenario outcome will be Not Prevented if the file can be saved and copied to the file system and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:14 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:14 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Save File To Disk And Copy It	<div>Failed</div>	<ul style="list-style-type: none">Malware Protection Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Save File To Disk And Copy It	<div>Failed</div>	<ul style="list-style-type: none">Malware Protection Best Practices

DOWNLOAD DOUBLE ZIPPED EICAR FILE TO MEMORY SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

DOWNLOAD DOUBLE ZIPPED EICAR FILE TO MEMORY

One of the most common actions for malware is to drop files to the filesystem. This scenario mimics part of that behavior by downloading a file and storing it in memory. The file SHA256 hash will be validated against the parameter provided hash in order to validate that the file was not modified in-transit.

This scenario has many parameters already configured to achieve its intent, which can be checked in the scenario template description for this scenario ("Download File to Memory"). The only parameters that could be modified without altering the scenario intent are the HTTP proxy-related parameters. The "HTTP Proxy" parameter allows selecting between using the default environment HTTP proxy settings, and manually specifying the HTTP proxy settings to be used for the file download. The "Proxy Address" and "Proxy Authentication Method" allow setting the HTTP proxy configuration to be used for the file download. These options only appear if "HTTP Proxy" is set to "Manual settings".

Although this scenario is not really complex, it lets you efficiently and easily test your network security controls by downloading the latest malware samples.

The scenario outcome will be Not Prevented if the file can be downloaded to memory and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:09 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:09 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

DOWNLOAD MAZE RANSOMWARE SAMPLE TO MEMORY SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

DOWNLOAD MAZE RANSOMWARE SAMPLE TO MEMORY

One of the most common actions for malware is to drop files to the filesystem. This scenario mimics part of that behavior by downloading a file and storing it in memory. The file SHA256 hash will be validated against the parameter provided hash in order to validate that the file was not modified in-transit.

This scenario has many parameters already configured to achieve its intent, which can be checked in the scenario template description for this scenario ("Download File to Memory"). The only parameters that could be modified without altering the scenario intent are the HTTP proxy-related parameters. The "HTTP Proxy" parameter allows selecting between using the default environment HTTP proxy settings, and manually specifying the HTTP proxy settings to be used for the file download. The "Proxy Address" and "Proxy Authentication Method" allow setting the HTTP proxy configuration to be used for the file download. These options only appear if "HTTP Proxy" is set to "Manual settings".

Although this scenario is not really complex, it lets you efficiently and easily test your network security controls by downloading the latest malware samples.

The scenario outcome will be Not Prevented if the file can be downloaded to memory and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:09 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:09 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

DOWNLOAD TXT EICAR FILE TO MEMORY SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

DOWNLOAD TXT EICAR FILE TO MEMORY

One of the most common actions for malware is to drop files to the filesystem. This scenario mimics part of that behavior by downloading a file and storing it in memory. The file SHA256 hash will be validated against the parameter provided hash in order to validate that the file was not modified in-transit.

This scenario has many parameters already configured to achieve its intent, which can be checked in the scenario template description for this scenario ("Download File to Memory"). The only parameters that could be modified without altering the scenario intent are the HTTP proxy-related parameters. The "HTTP Proxy" parameter allows selecting between using the default environment HTTP proxy settings, and manually specifying the HTTP proxy settings to be used for the file download. The "Proxy Address" and "Proxy Authentication Method" allow setting the HTTP proxy configuration to be used for the file download. These options only appear if "HTTP Proxy" is set to "Manual settings".

Although this scenario is not really complex, it lets you efficiently and easily test your network security controls by downloading the latest malware samples.

The scenario outcome will be Not Prevented if the file can be downloaded to memory and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:09 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:09 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

SAVE ROBINHOOD'S RANSOMWARE RBNL MALICIOUS DRIVER TO FILE SYSTEM SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

SAVE ROBINHOOD'S RANSOMWARE RBNL MALICIOUS DRIVER TO FILE SYSTEM

This scenario takes a Robinhood's ransomware RBNL malicious driver and save it to the file system.

The file content is provided AES encrypted to the scenario. The scenario will decrypt the content and save it to the disk, then make a copy of it. Finally, both files are checked against the expected hash of the original file.

The file is copied to make sure that it hasn't been quarantined / deleted by any security control. The same applies for the hash calculation.

The scenario has two parameters:

- A delay in seconds to apply between each operation to give the security controls time to react. The default is 3 seconds.
- The path where the files are created. By default, a folder in the OS TEMP folder is used (the user's TEMP folder when running under user privileges).

The scenario outcome will be Not Prevented if the file can be saved and copied to the file system and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:11 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:11 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Save File To Disk And Copy It	<div>Failed</div>	<ul style="list-style-type: none">Malware Protection Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Save File To Disk And Copy It	<div>Failed</div>	<ul style="list-style-type: none">Malware Protection Best Practices

DOWNLOAD ZIP EICAR FILE TO MEMORY SCENARIO RESULTS

Detailed description, results and mitigation recommendations for this scenario.

DESCRIPTION

DOWNLOAD ZIP EICAR FILE TO MEMORY

One of the most common actions for malware is to drop files to the filesystem. This scenario mimics part of that behavior by downloading a file and storing it in memory. The file SHA256 hash will be validated against the parameter provided hash in order to validate that the file was not modified in-transit.

This scenario has many parameters already configured to achieve its intent, which can be checked in the scenario template description for this scenario ("Download File to Memory"). The only parameters that could be modified without altering the scenario intent are the HTTP proxy-related parameters. The "HTTP Proxy" parameter allows selecting between using the default environment HTTP proxy settings, and manually specifying the HTTP proxy settings to be used for the file download. The "Proxy Address" and "Proxy Authentication Method" allow setting the HTTP proxy configuration to be used for the file download. These options only appear if "HTTP Proxy" is set to "Manual settings".

Although this scenario is not really complex, it lets you efficiently and easily test your network security controls by downloading the latest malware samples.

The scenario outcome will be Not Prevented if the file can be downloaded to memory and the resulting hash matches the expected one. Otherwise, the scenario execution will appear as Prevented.

SCENARIO RESULTS BY ASSET (LAST RUN)

	USER PRIVILEGES	HOSTNAME	IP ADDRESS	OS	GROUP	LAST RUN
✖	SYSTEM	acad2815-un	172.16.15.171	Microsoft Windows 10 Pro N		02/28/2024 09:08 am
✖	SYSTEM	acad6969-prot	172.16.14.107	Microsoft Windows 10 Pro N		02/28/2024 09:08 am

PHASE RESULTS BY SCENARIO RUN

02/28/2024 09:08 amOn asset: acad2815-un (172.16.15.171)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

02/28/2024 09:08 amOn asset: acad6969-prot (172.16.14.107)		
Phase	Outcome	Mitigation Recommendations
Download File	Failed	<ul style="list-style-type: none">Content Filter Best Practices

Appendix-A **Phases**

PHASE	DESCRIPTION
Download File	Download file
Save File To Disk And Copy It	This phase saves a file and moves it within the same directory.

MITIGATION	DESCRIPTION
Content Filter Best Practices	<p data-bbox="523 78 1492 190">When configuring a content filter, there are several best practices to follow to ensure it is properly configured to meet your organization's needs. Here are the key steps to configure a content filter effectively:</p> <ul data-bbox="563 286 1492 2168" style="list-style-type: none"> <li data-bbox="563 286 1492 481">• Understand your organization's requirements: Assess and understand your organization's specific content filtering needs. Consider factors such as acceptable internet usage, compliance regulations, and the types of content you want to filter (e.g., explicit material, social media, gaming sites, etc.). <li data-bbox="563 577 1492 772">• Define content filtering policies: Clearly define the content filtering policies that align with your organization's objectives and requirements. Determine what types of content should be allowed, blocked, or monitored. Consider creating different policies for different user groups or departments based on their roles and responsibilities. <li data-bbox="563 869 1492 1064">• Categorize content and set filtering levels: Categorize content into different levels of filtering based on the desired level of restriction or appropriateness. For example, you may have stricter filtering for explicit content while allowing access to educational or work-related websites. Configure filtering levels accordingly. <li data-bbox="563 1160 1492 1355">• Customize filtering profiles: Create and configure filtering profiles that can be applied to different user groups or departments. Tailor the profiles to enforce appropriate content control while allowing flexibility when necessary. Consider any exceptions or specific requirements for certain user groups. <li data-bbox="563 1451 1492 1646">• Regularly update content filter databases: Ensure that your content filter's databases are regularly updated with the latest information about websites, URLs, categories, and emerging threats. Regular updates help keep the filter accurate in identifying and blocking inappropriate or malicious content. <li data-bbox="563 1742 1492 1937">• Enable HTTPS/SSL inspection: Enable HTTPS/SSL inspection capabilities in your content filter. This allows the filter to analyze encrypted web traffic, providing better visibility into potential threats or policy violations. <li data-bbox="563 2033 1492 2168">• Customize whitelist and blacklist: Maintain a whitelist of trusted websites that should always be accessible and a blacklist of known malicious or inappropriate sites that should be blocked. Regularly review and update these lists to ensure they remain accurate and up-to-date.

MITIGATION	DESCRIPTION
	<ul style="list-style-type: none"> • Monitor and log content filter activity: Enable logging and monitoring features to track user activity and filter actions. Regularly review logs to identify policy violations, security threats, and potential areas for improvement. Monitoring helps ensure compliance and allows for proactive response to emerging risks. • Educate users about content filtering policies: Provide clear guidelines and communicate content filtering policies to your users. Educate them about the purpose of content filtering, potential risks associated with certain online activities, and the importance of responsible internet usage. <p>Remember to periodically review and update your content filter configuration to adapt to changing needs, emerging threats, and new content categories. Combine content filtering with other security measures, employee training, and user awareness to create a comprehensive approach to content security within your organization.</p>
Malware Protection Best Practices	<p>Configuring your antivirus software properly is important to ensure that it provides effective protection against malware. Here are some best practices for configuring your antivirus software:</p> <ul style="list-style-type: none"> • Update antivirus definitions regularly: Antivirus software relies on virus definitions to identify and detect malware. Make sure to regularly update your antivirus software to ensure it has the latest virus definitions, so it can effectively detect and remove the latest malware threats. • Enable real-time scanning: Enable real-time or on-access scanning, which scans files and programs as they are accessed or executed in real-time. This helps to detect and block malware before it can infect your system. • Schedule regular scans: Set up scheduled scans on your devices to run regular full system scans. This helps to detect and remove any dormant or hidden malware that may have evaded real-time scanning. • Configure automatic updates: Configure your antivirus software to automatically download and install updates, including virus definitions and software patches. This ensures that your antivirus software stays up-to-date with the latest security features and bug fixes.

MITIGATION	DESCRIPTION
	<ul style="list-style-type: none"><li data-bbox="560 69 1481 219">• Enable heuristic scanning: Enable heuristic scanning, which uses behavioral and pattern-based techniques to detect previously unknown malware. This helps to catch new and emerging malware threats that may not yet have a known signature in the virus definitions.<li data-bbox="560 320 1481 510">• Customize scan settings: Review and customize the scan settings according to your needs. For example, you may want to specify certain folders or file types to be excluded from scanning if you know they are safe. Customizing scan settings can help optimize performance and reduce false positives.<li data-bbox="560 611 1497 757">• Enable email and web protection: If your antivirus software provides email and web protection features, make sure to enable them. These features help detect and block malware that may be transmitted through email attachments, links, or malicious websites.<li data-bbox="560 857 1497 1003">• Set up quarantine or vault: Configure your antivirus software to automatically quarantine or isolate infected files instead of deleting them outright. This allows you to recover potentially false positives or restore mistakenly quarantined files if needed.<li data-bbox="560 1104 1497 1294">• Enable automatic scans for removable media: Configure your antivirus software to automatically scan removable media, such as USB drives or external hard drives, when they are connected to your system. This helps to detect and remove any malware that may be present on these devices.<li data-bbox="560 1395 1497 1541">• Keep backups: Always maintain regular backups of your important data and files. In case of a malware infection, having backups ensures that you can recover your data even if it gets encrypted or compromised by malware. <p data-bbox="523 1686 1469 1921">Remember that antivirus software is just one layer of defense against malware, and it's important to follow other best practices for overall cybersecurity, such as being cautious with email attachments, using strong passwords, keeping your software up-to-date, and practicing safe browsing habits. A combination of multiple security measures is the best approach to protect against malware effectively.</p>