[Firewalls vs Malware]

Key Contributors: Jimmy Aragon, Joshua Ibarra, Joe Perez

Date: April 21, 2022

This project and the preparation of this report through an agreement with the University of the Incarnate Word.
Cyber Security Systems and the University of the Incarnate Word

TABLE OF CONTENTS

EXECUTIVE SUMMARY

For our project, we have decided to discuss our topic on network security applications. Throughout the project, we planned to show off some types of antivirus that many people use daily within their lives. Then we plan to provide a presentation that will give our classmates a good overall understanding of an antivirus's functions within a VM. In addition to that, this report will overview the processes that we followed to understand the malware that we experienced and see the effects on a VM with the process that different antivirus software follow to protect a system.

	Downloaded	Executed	
McA	2/3	3/3	
WD	1/3	2/3	
BD	0/3	3/3	

Rational

Operating System:

We chose Windows 10 as the operating system for this project because of its easy accessibility and due to it already having the Windows firewall and antivirus installed on the system.

Firewalls:

Windows Defender: It came with the base system and served as a baseline for the typical defenses that would be expected in most firewalls and antiviruses. Those who use Windows OS are expected to rely on this, more so when the majority of people use Windows OS.

McAfee: Although this program doesn't have the best reputation for being able to defend against malware once it gets into the system, it is the antivirus that is installed in every windows system as a free trial, so that must mean that Windows endorses it for one reason or another.

BitDefender: This was a free software that was available for download straight from the internet and therefore served as a defense that anyone could get their hands on for no fee.

Malware:

Email Roulette (Trojan): The Email scenario was used as a great example of how our firewalls are able to determine a malicious file attempting to disguise itself to access a system.

Identifying the EK (Exploitation Kit) and infection chain (Backdoor): This scenario was one of the easiest to function with many of the firewalls in terms of functionality and response to the malware.

So Hot Right Now (RAT): This scenario is used to test the ability of our firewalls to get rid of the malicious files that are accessed and protect the system after it was compromised.

Project Milestones:

1. Choose what kind of OS and malware we would be using in our project
2. Testing and reporting of all of the malwares against the chosen firewalls were completed
3. Updated and completed report with additional details of the project

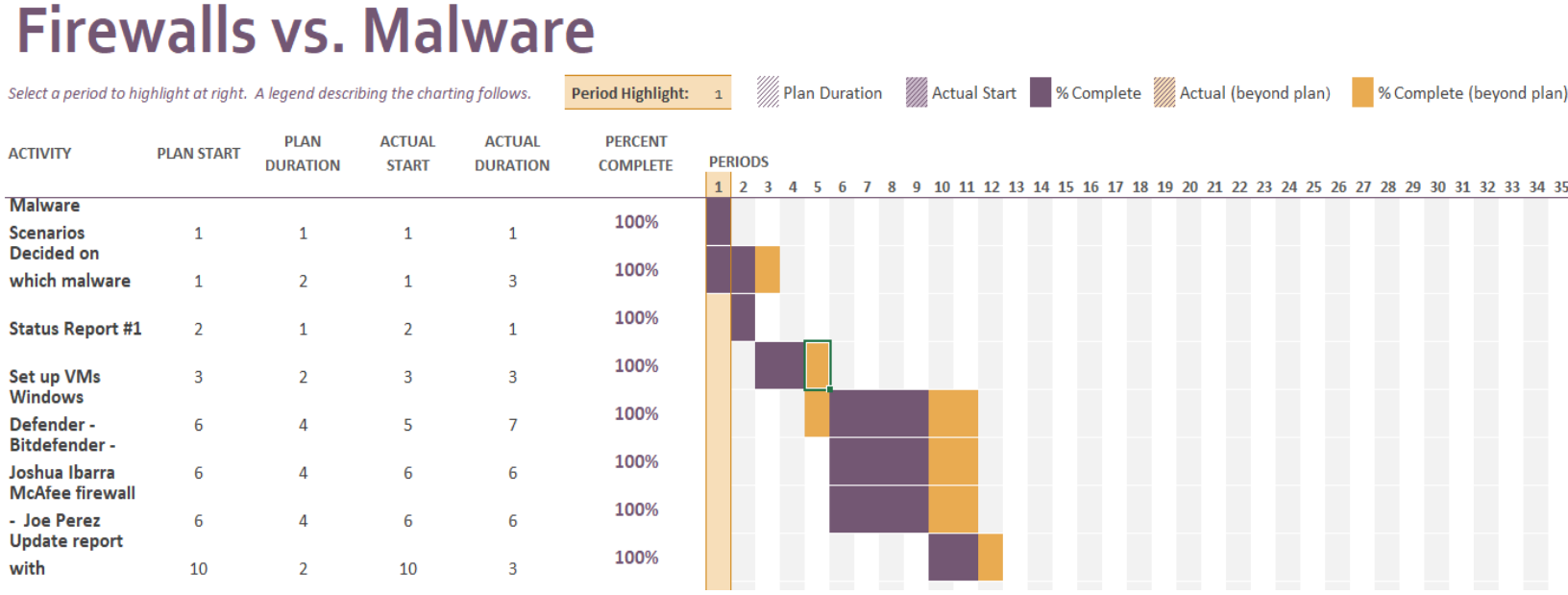
Deliverables:

1. A report of the project and the tests that we have conducted in order to complete it
2. A showcase of the capabilities of the firewalls and antivirus and how they handled different types of malware
3. Help others understand the importance of Antivirus and understand the difference of the services provided from different companies.

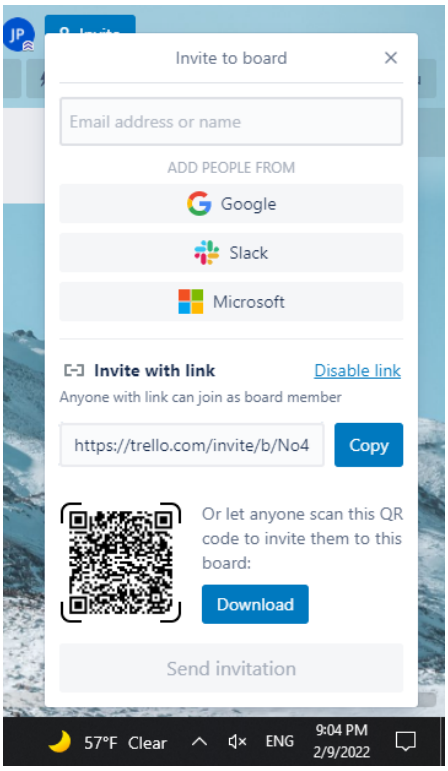
Professional Accomplishments:

1. The ability to analyze and recognize the different events that were going on as the malware executed and the antivirus activated
2. New knowledge of malware and the effects that they could have on the computer systems they infect

PROJECT SCHEDULE MANAGEMENT



Trello QR:



Create a Github Project Repository:

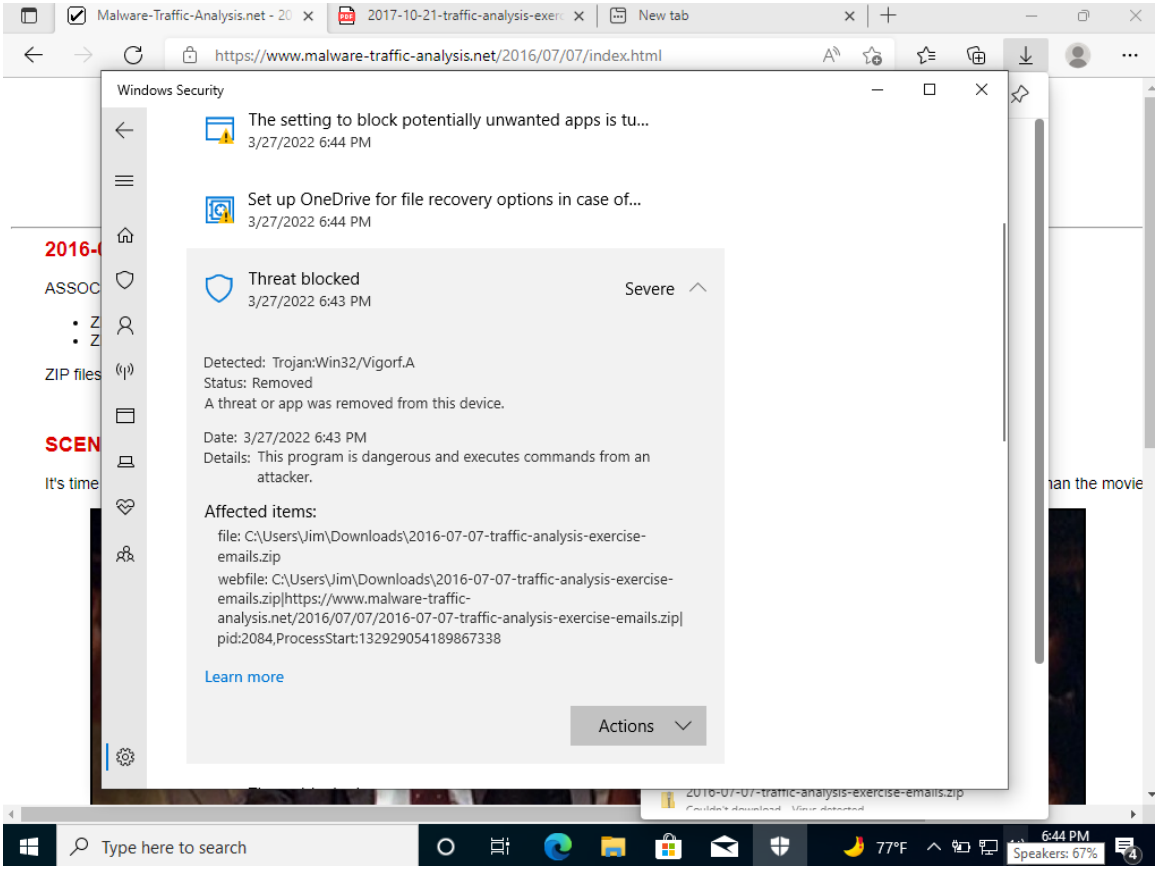
https://github.com/PerezJoe982/CIS-3353_Network_Security_Appliances_Project.git

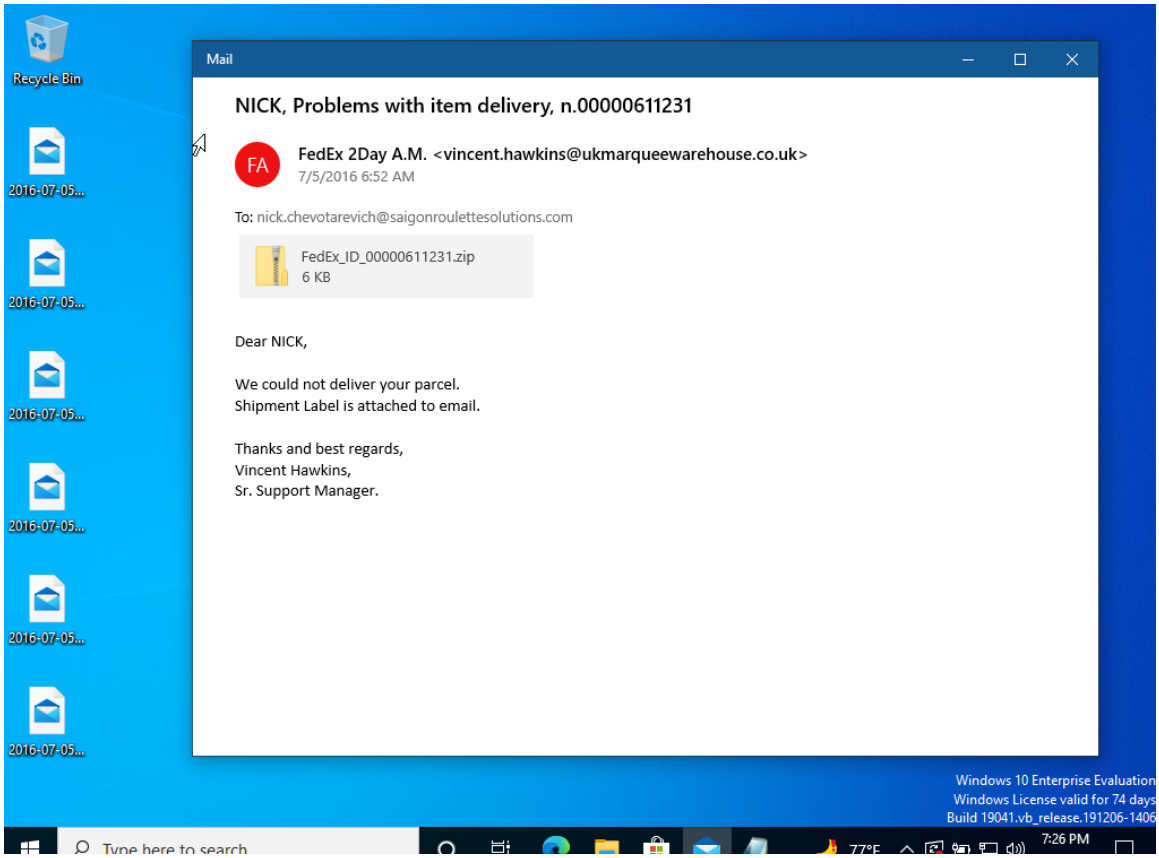
Malware Tests:

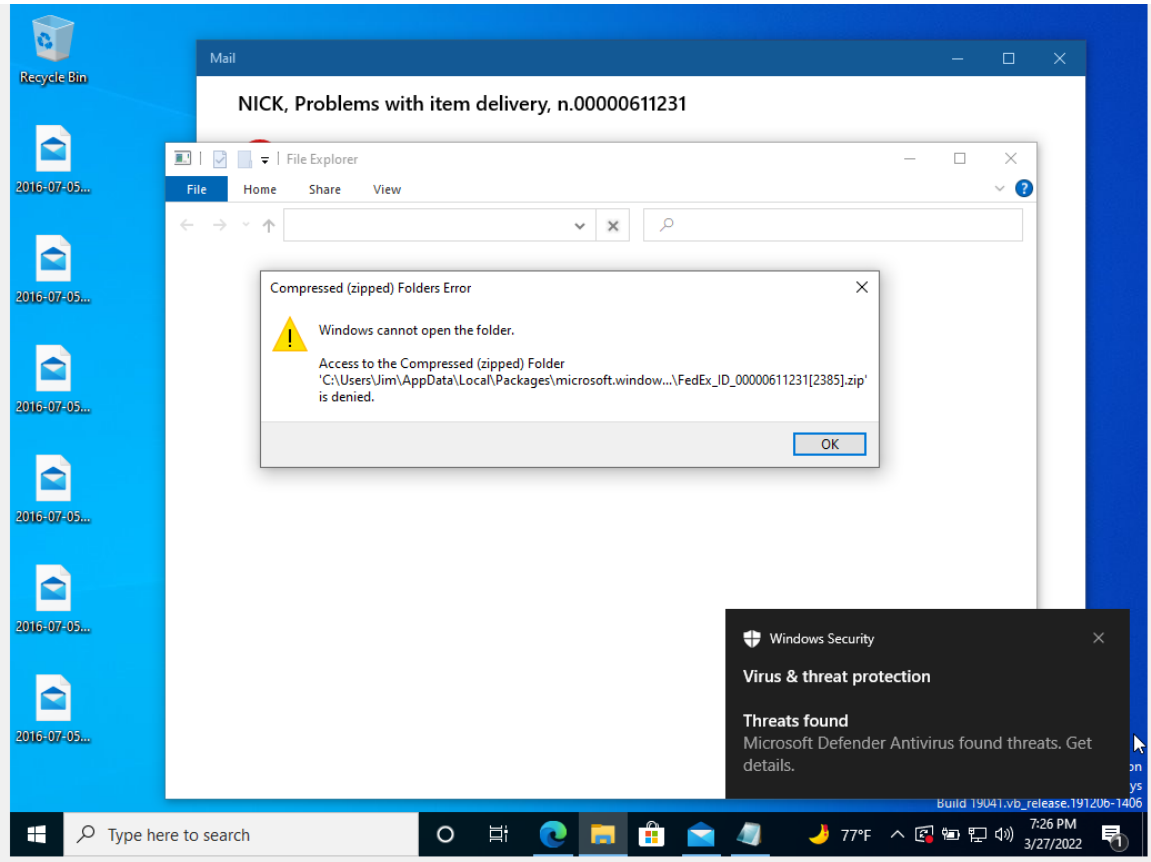
Windows Defender

Exercise 1: In the malware exercise known as 'email roulette' I tested how windows defender would respond to a malicious file hidden behind a link in an email. For starters, I tried to download the EML files in a zip file, from the website in order to view the malicious link. However, windows defender was potent enough to scan the EML zip file while it downloaded and detected that it contained malware. When I clicked the windows notification it listed the threat that it blocked and deleted as a Trojan. As I still needed to test the actual email itself, I clicked on the option to allow the download. Once downloaded, I opened the infected email and proceeded to click on the malicious

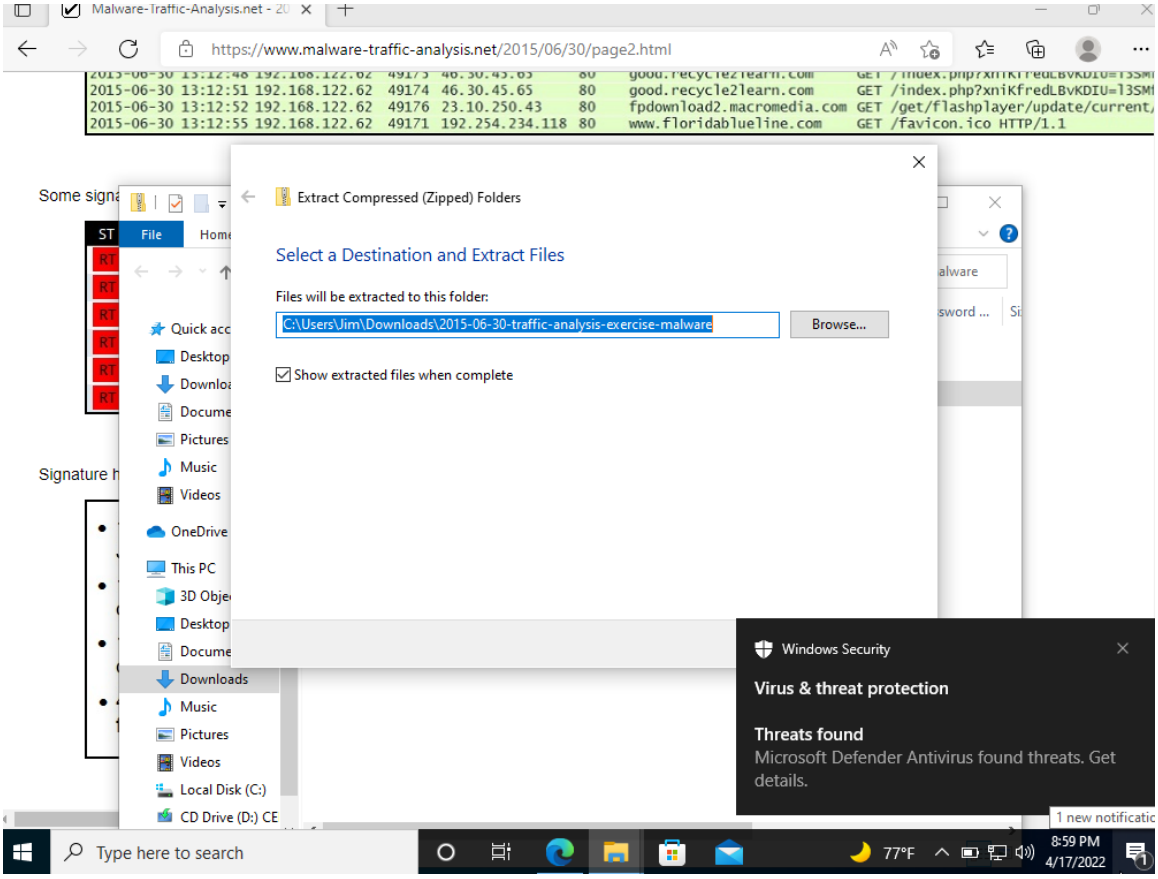
link disguised to be relevant to the actual email itself. After clicking on the link to download it, an error popped up saying that I was denied access to the downloaded contents. Following, a windows defender notification popped up detailing active threats were found. Upon reading through the report, once the file had been downloaded to my computer windows detected it as a malicious file, and then proceeded to ‘quarantine’ the file from the rest of the computer. As windows defender describes it, “Quarantined files are in a restricted area where they can’t harm your device”. It seems that though windows was not able to prevent the file from starting up on my computer, it did prevent it from spreading and executing.

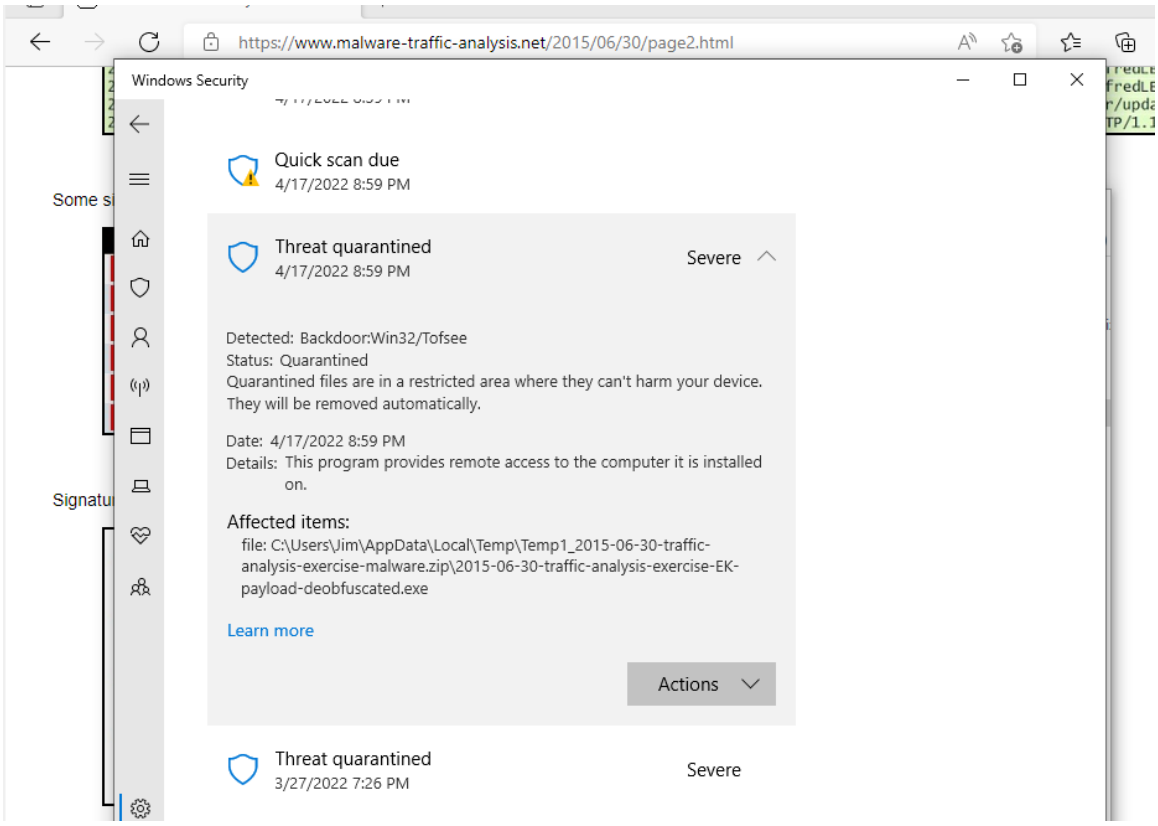

Malware-Traffic-Analysis.net - 20
2017-10-21-traffic-analysis-exerc
New tab
https://www.malware-traffic-analysis.net/2016/07/07/index.html
Windows Security
The setting to block potentially unwanted apps is tu...
3/27/2022 6:44 PM
Set up OneDrive for file recovery options in case of...
3/27/2022 6:44 PM
Threat blocked
3/27/2022 6:43 PM
Severe
Detected: Trojan:Win32/Vigorf.A
Status: Removed
A threat or app was removed from this device.
Date: 3/27/2022 6:43 PM
Details: This program is dangerous and executes commands from an attacker.
Affected items:
file: C:\Users\Jim\Downloads\2016-07-07-traffic-analysis-exercise-emails.zip
webfile: C:\Users\Jim\Downloads\2016-07-07-traffic-analysis-exercise-emails.zip|https://www.malware-traffic-analysis.net/2016/07/07/2016-07-07-traffic-analysis-exercise-emails.zip|pid:2084,ProcessStart:132929054189867338
Learn more
Actions
Type here to search
77°F
6:44 PM
Speakers: 67%

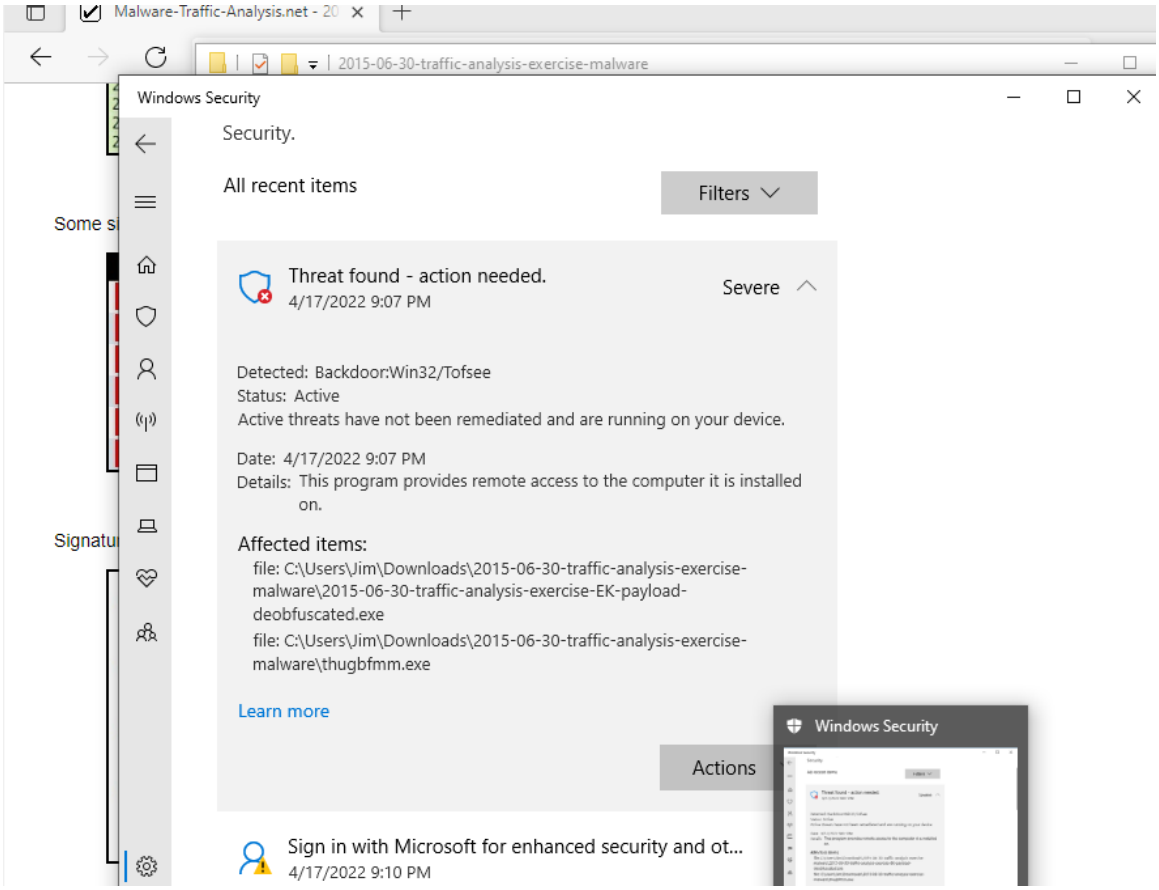

Recycle Bin
Mail
NICK, Problems with item delivery, n.00000611231
FA
FedEx 2Day A.M. <vincent.hawkins@ukmarqueewarehouse.co.uk>
7/5/2016 6:52 AM
To: nick.chevotarevich@saigonroulettesolutions.com
FedEx_ID_00000611231.zip
6 KB
Dear NICK,
We could not deliver your parcel.
Shipment Label is attached to email.
Thanks and best regards,
Vincent Hawkins,
Sr. Support Manager.
Windows 10 Enterprise Evaluation
Windows License valid for 74 days
Build 19041.vb_release.191206-1406
7:26 PM



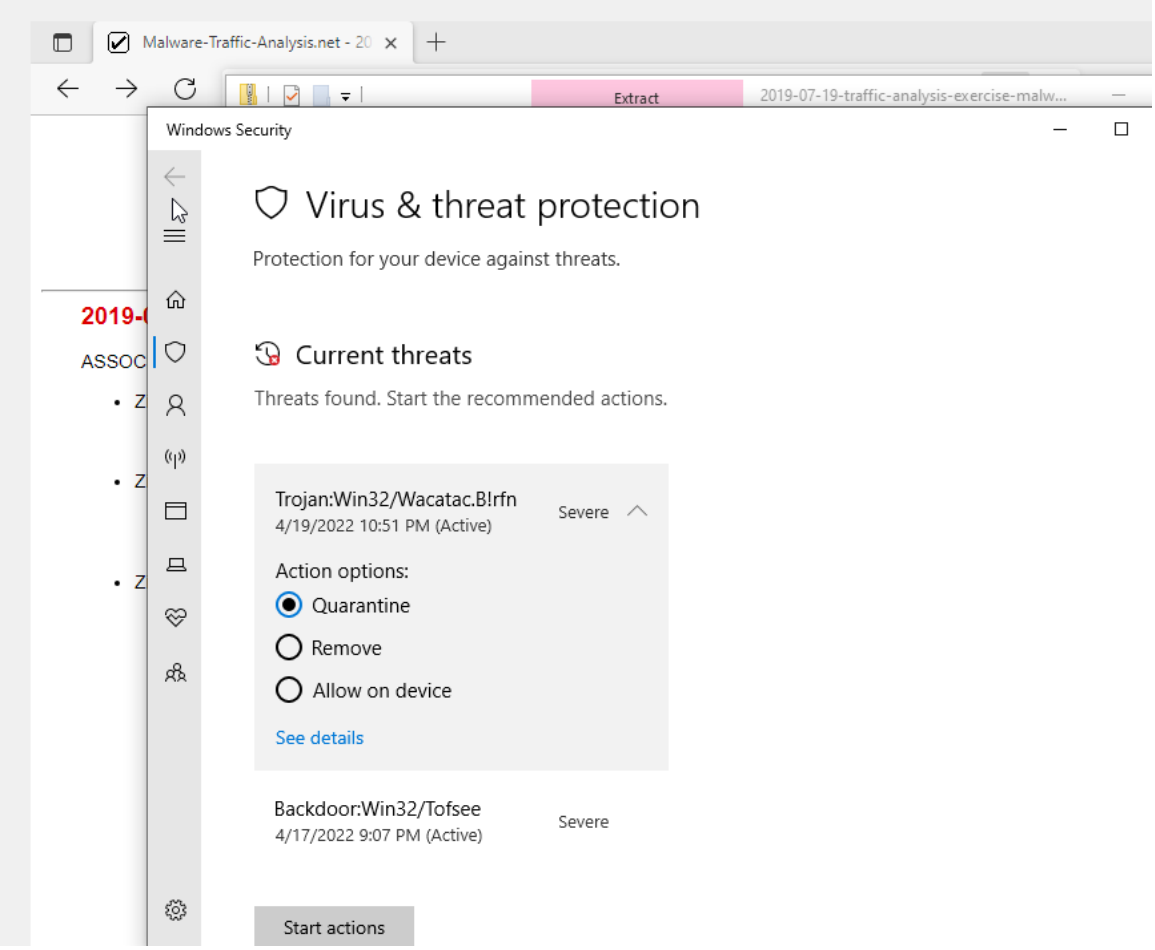
Exercise 2: In the malware exercise known as 'Identifying the EK (Exploitation Kit) and infection chain' I tested how Windows Defender would respond to a compromised website. This time, the download of the zip file itself was not blocked by Windows Defender. When I gained access to the zip, I attempted to launch the executable file, but a Windows pop up detailed "Operation did not complete successfully because the file contains a virus or potentially unwanted software". I checked the action report, and it stated that it prevented the execution, then promptly quarantined the file location that it tried to execute in. Windows also was able to identify the type of malware the file was, a backdoor in this case. What I tried to do next, was extract the executable files from the zip into the downloads folder of my VM. In trying to do so, I was prompted with several Windows Defender notifications, but was not stopped from extracting the files as they did so successfully. After doing so, there was no need for me to try and execute the files manually, as they did so automatically. I clicked the notifications I was getting and saw that Windows Defender identified several instances of the backdoor running on my VM. Upon clicking on them, I was given the option to quarantine, remove, or allow the files. After pressing to remove them, I looked at the action report that Windows provided, and it described the malware as "This program provides remote access to the computer it is installed on". In this case, it seems that Windows was not able to prevent the backdoor from fully operating, but instead notified the user about the operation and needed manual intervention. Even after the manual intervention, it seems that Windows Defender is not able to permanently remove it, as it constantly came back.


Malware-Traffic-Analysis.net
https://www.malware-traffic-analysis.net/2015/06/30/page2.html
2015-06-30 13:12:51 192.168.122.62 49174 46.30.45.65 80 good.recycle2learn.com GET /index.php?xniKfredLBvKDIU=l3SM
2015-06-30 13:12:52 192.168.122.62 49176 23.10.250.43 80 fpdownload2.macromedia.com GET /get/flashplayer/update/current/
2015-06-30 13:12:55 192.168.122.62 49171 192.254.234.118 80 www.floridablueline.com GET /favicon.ico HTTP/1.1
Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\Users\Jim\Downloads\2015-06-30-traffic-analysis-exercise-malware
Browse...
Show extracted files when complete
Windows Security
Virus & threat protection
Threats found
Microsoft Defender Antivirus found threats. Get details.
Type here to search
77°F
8:59 PM
4/17/2022


https://www.malware-traffic-analysis.net/2015/06/30/page2.html
Windows Security
Quick scan due
4/17/2022 8:59 PM
Threat quarantined
4/17/2022 8:59 PM
Severe
Detected: Backdoor:Win32/Tofsee
Status: Quarantined
Quarantined files are in a restricted area where they can't harm your device. They will be removed automatically.
Date: 4/17/2022 8:59 PM
Details: This program provides remote access to the computer it is installed on.
Affected items:
file: C:\Users\Jim\AppData\Local\Temp\Temp1_2015-06-30-traffic-analysis-exercise-malware.zip\2015-06-30-traffic-analysis-exercise-EK-payload-deobfuscated.exe
Learn more
Actions
Threat quarantined
3/27/2022 7:26 PM
Severe



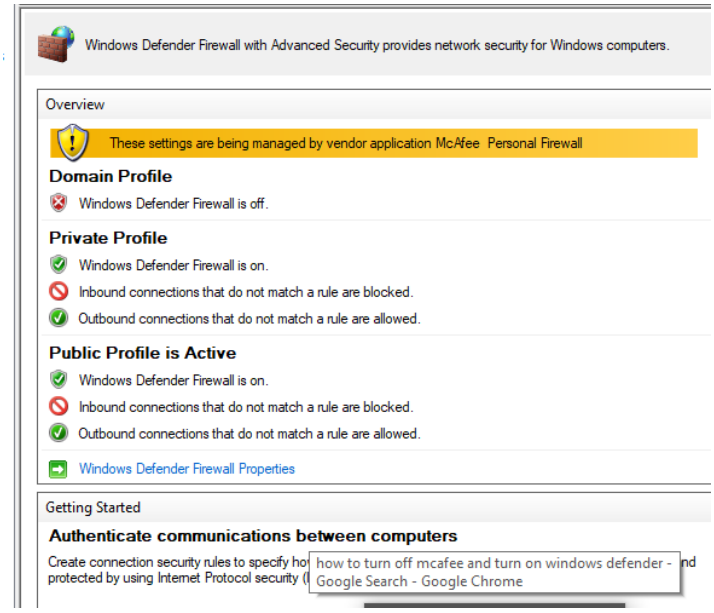
Exercise 3: In the malware exercise known as 'So Hot Right now', Windows Defender did not attempt to intercept the zip containing the malware. When I extracted all the contents of the zip into my downloads folder, Windows Defender immediately picked up the malware and sent out the usual notification followed by quarantining the file. This time though, it was not able to properly identify what the malware does, aside from it being a trojan, it stated "This program is dangerous and executes commands from an attacker". It appears that without the key executable file "Firefox" the RAT was not able to infect my VM at all. After going back and restoring the file, I attempted to allow the malware to infect my computer, but it was not successful. I believe that as the compromised website that the malware uses requires the user to have a google chrome or firefox browser, it is not able to execute properly.

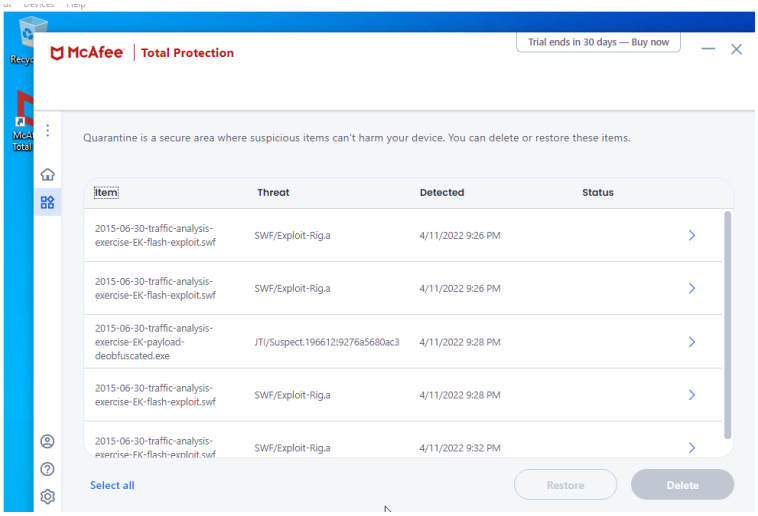


McAfee Firewall

Had to disable Windows Defender in the beginning to get a complete idea of McAfee's Firewall.

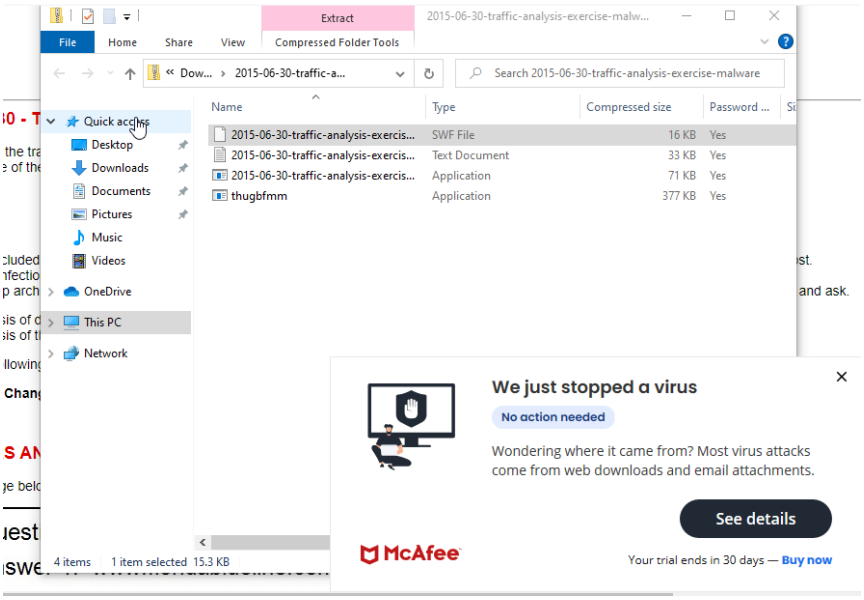
Exercise 1: During my activity of the 'Identifying the EK (Exploit Kit) and infection chain' malware exercise as my malicious source, I wanted to find how McAfee would work as an antivirus software against the malware of an infected host. I started with accessing the files and the link to the false host of 'www.floridablueline.com' as the link. However, McAfee immediately isolated all files regarding the host and even gave me multiple notifications that I almost downloaded malware, which led me to forcing my VM to download and run the files by manually accessing the files and allowing the download. While the files functioned McAfee was not very happy as continued to get notifications against what I was doing, after I accessed all of the links of the site they were all quarantined off within the McAfee site itself as it was re-enabled. Overall, McAfee worked as it's intended purpose and attempted to section off all of the malicious files that I had downloaded initially, in addition to constantly prompting me to the potential dangers of the files and quarantining the files I forced it to run. McAfee works great at its intended function to my surprise considering its "not great" reputation as an antivirus software.



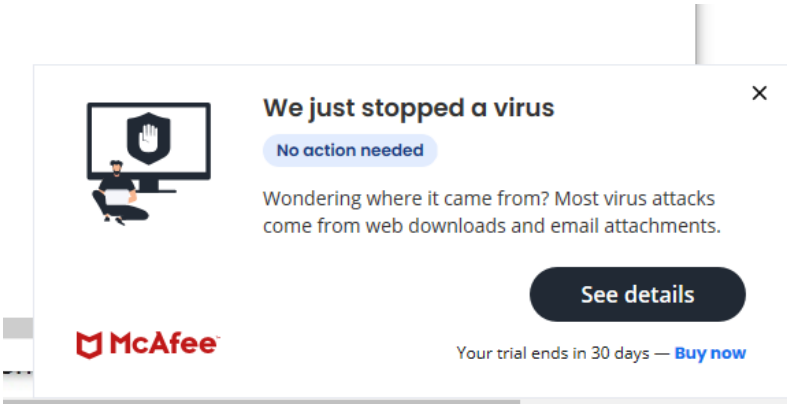


Exercise 2: While Working on the 'Email Roulette' exercise I was tasked with finding the malicious file within one of the links from an email. After accessing the data without the help of McAfee it shows a Trojan gaining access to the system of the VM and having to manually be removed from the files. I then attempted to determine which specific link was malicious through downloading their zip to hopefully proc a response from the antivirus. However, every part of the email links were accessed by my VM without repercussion or notification, so I had to manually cause a scan for McAfee to find any Trojan data within the malicious email link of the email. Curiously I tried the situation again to proc a response before I access the data to no avail, then I attempted to access the data within the malicious link and started the process only for McAfee to finally notify me that they had to stop a virus. With some more time I would have been able to access the files within the link and given access to the VM. McAfee made the situation a little close for comfort as for the longest time it seemed that it was unable to identify the

threat from the link until the end, but allowed me to access the links and download a malicious file in the first place. Overall, making me not very sure of the defense from McAfee and their defense on Trojans, even when one of their major selling points is protection, defense and removal of Trojan viruses in real time.

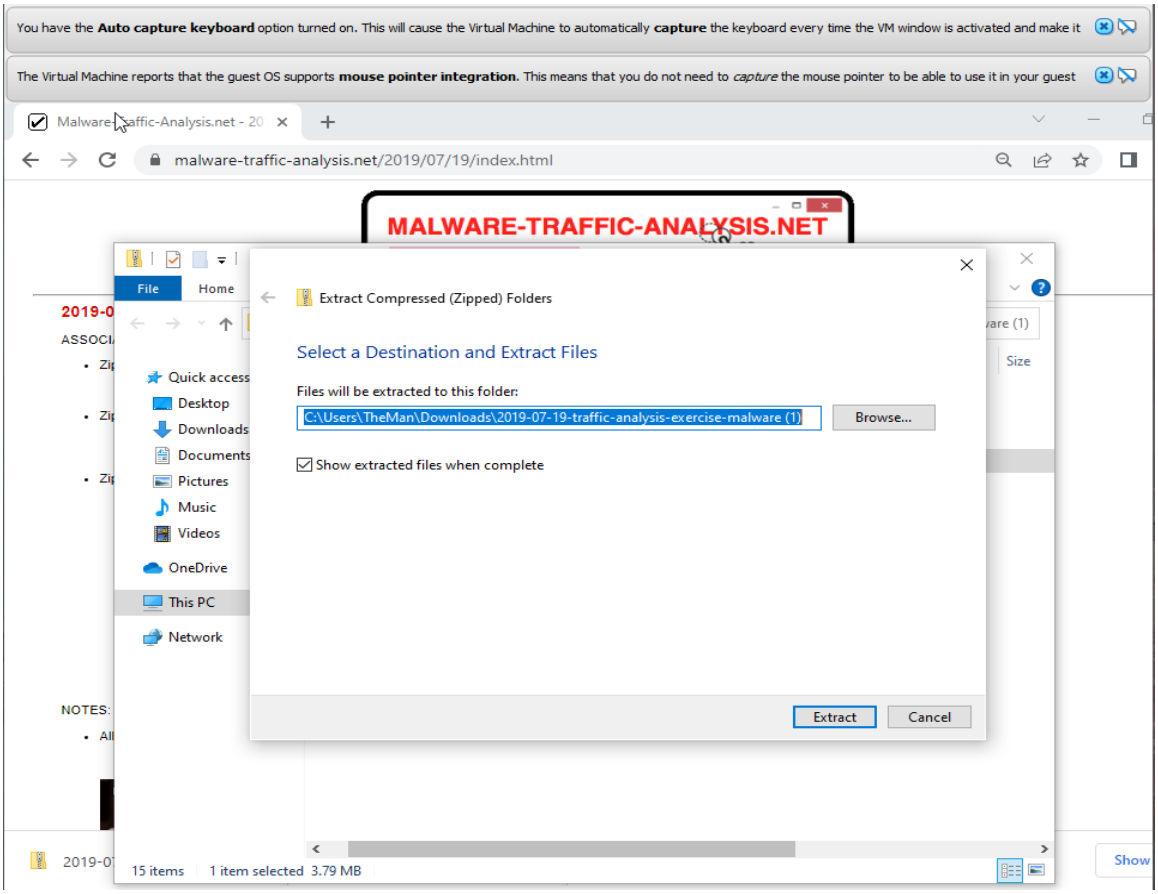


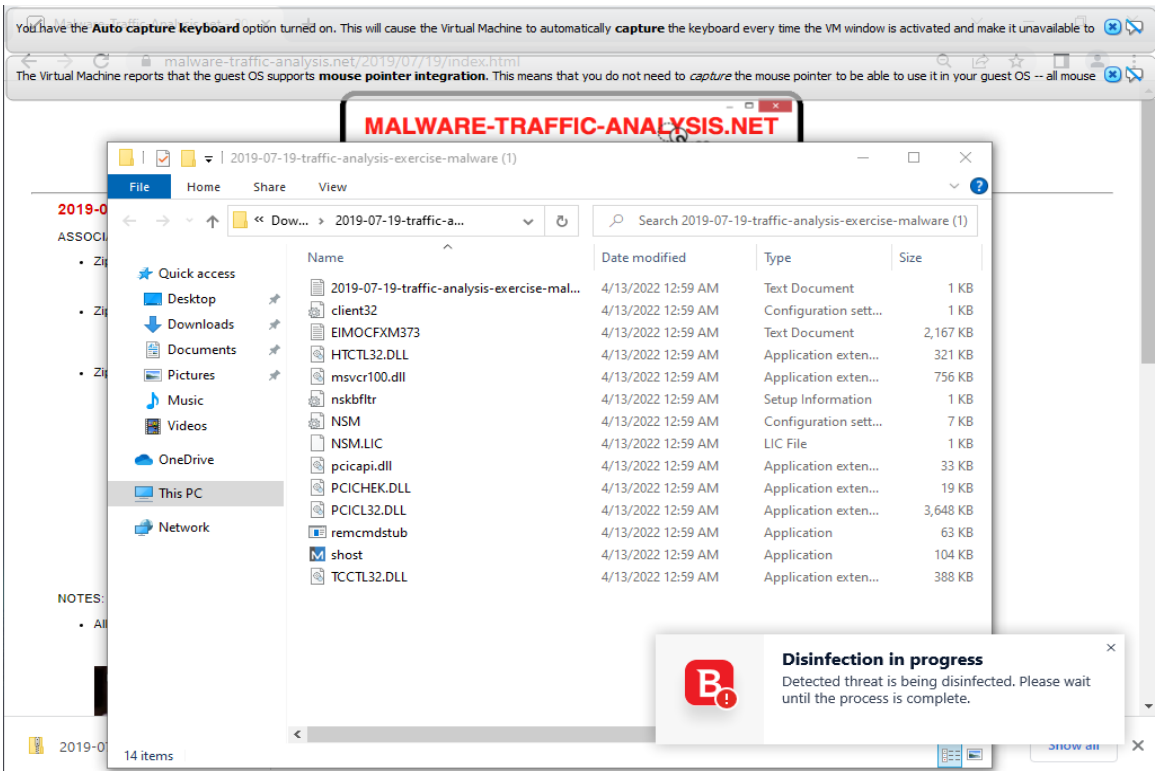
Exercise 3: During a test exercise ‘So Hot Right Now’ the main objective was to understand the function of a RAT (Remote Access Trojans) by accessing the zip archive of infected host files that were able to be downloaded. During the beginning of my testing the files connected to the zip were immediately blocked by McAfee attempting to get rid of the host files, all files are connected to malicious Trojan hosts that were blocked by the antivirus. So of course I had to work around that to download the malicious links, while accessing the links it seems that there is difference in functionality of each link and their response to being downloaded onto the VM, specifically that one may seem fine and will not have a malicious intent, but is connected to another file that has malicious data that infected the VM. Seemingly different to other trojans with the intent to access the data of the computer remotely. With McAfee enabled it stopped the download of the files when I tried again and even stopped all functionality and downloads from the first connecting site to not allow any malicious data to seep into the VM by quarantining the files as a antivirus is supposed to.

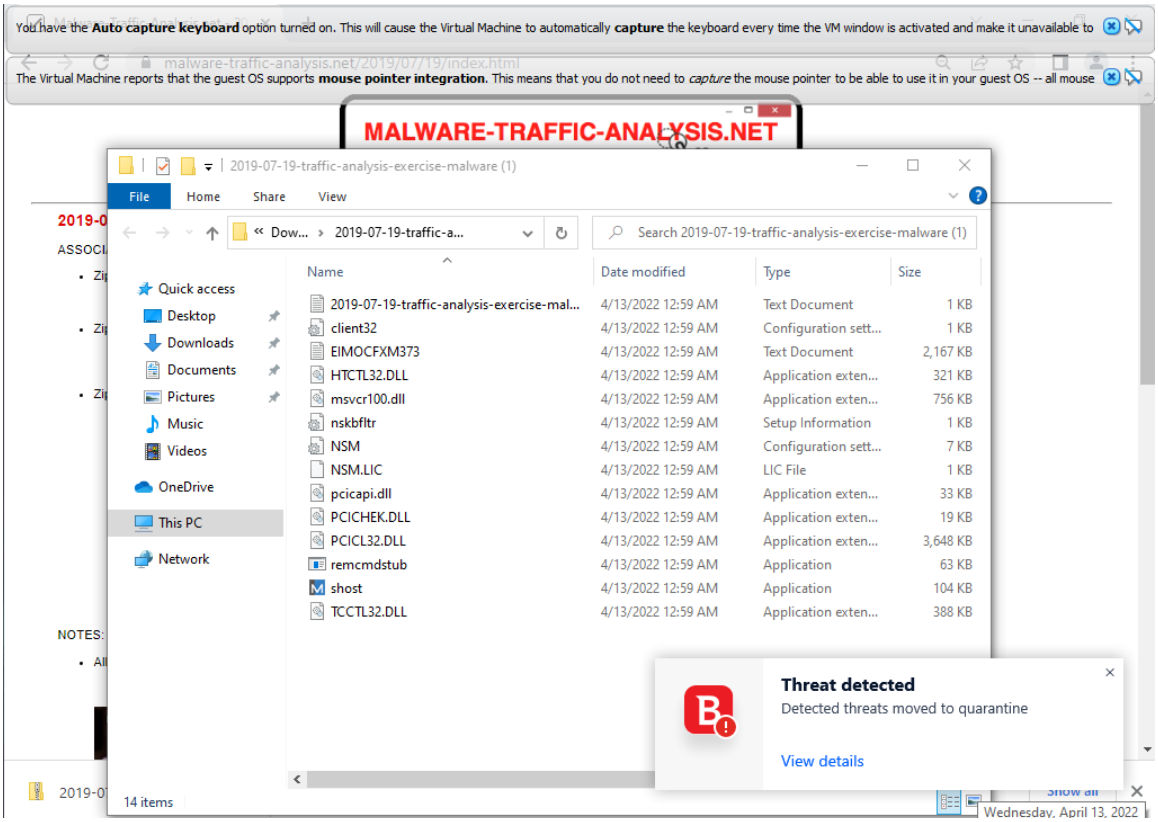


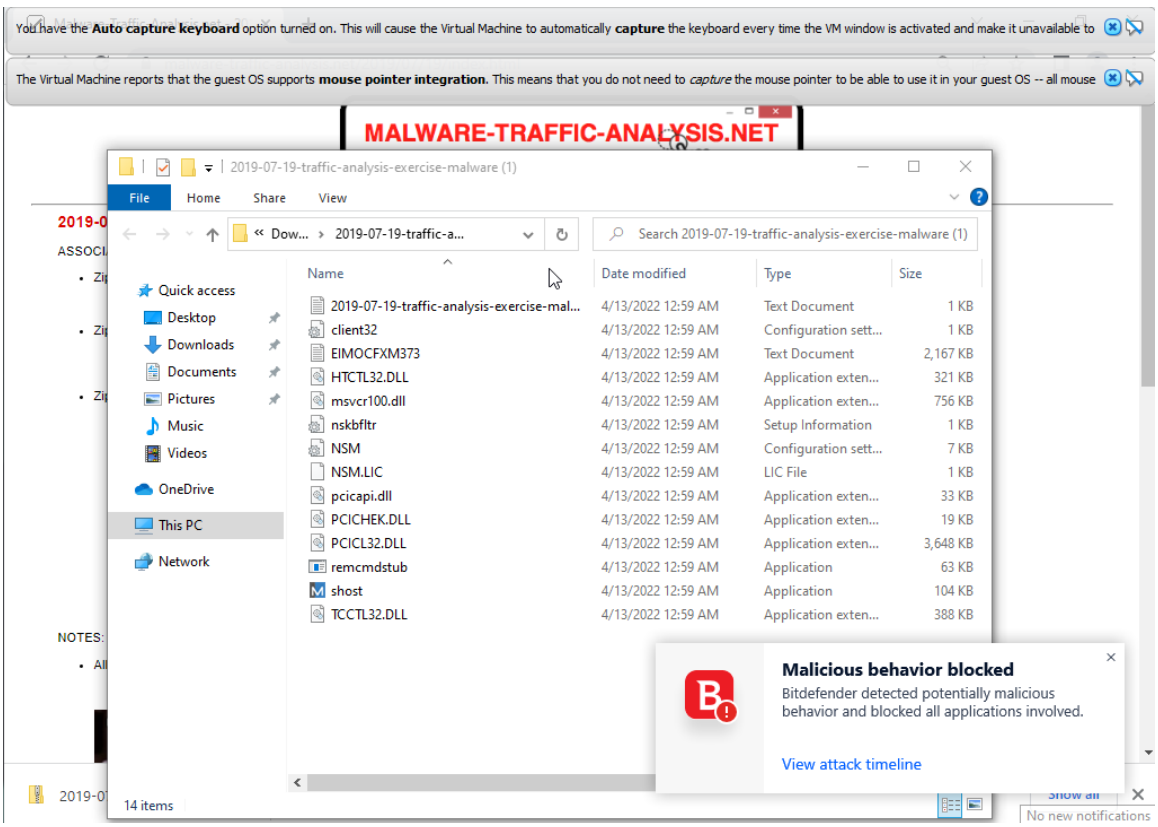
BitDefender

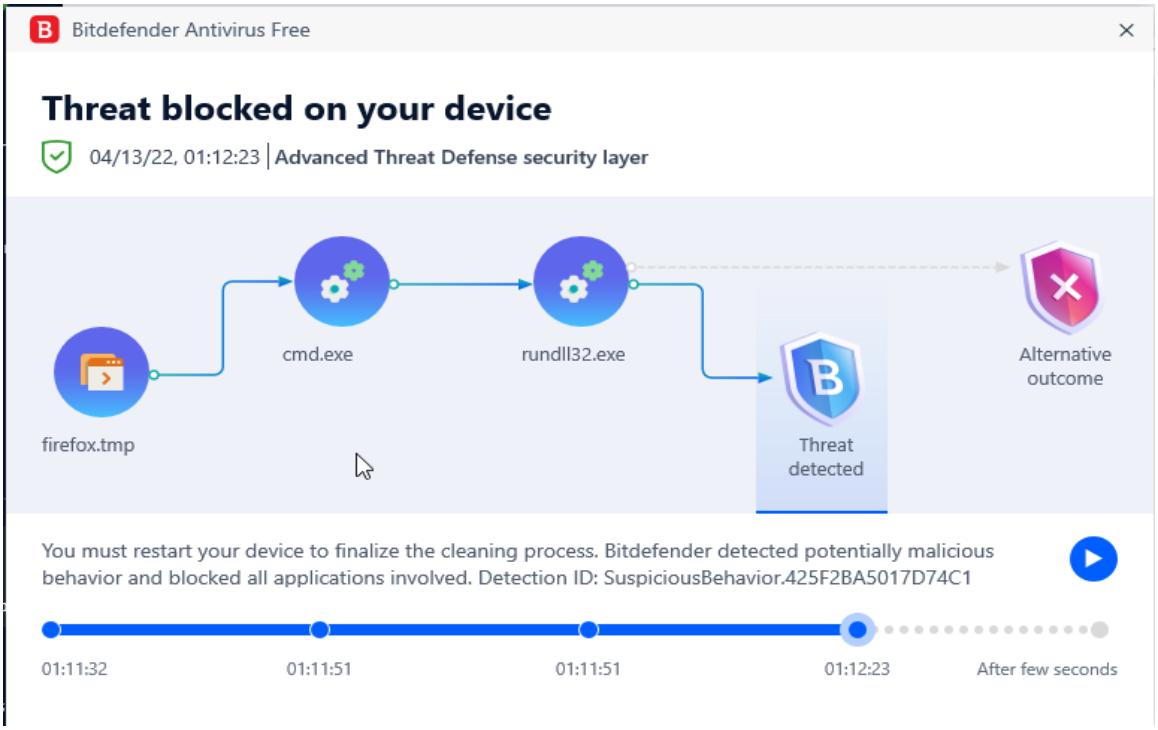
Exercise 1: For this test, I did an analysis on how the BitDefender firewall and antimalware responded to malware involved in a traffic analysis exercise called “So Hot Right Now”. The malware involved was a RAT that initially disguised itself as a compromised website that would inform the user that the web browser they were using was out of date and prompt them to download the newest version of the browser, which was actually a RAT called NetSupport Manager packaged as malware. When I downloaded and tried to load the compromised website, the page immediately executed a file called “cmd.exe” which then ran “rundll32.exe” which was the actual malware that would initiate the RAT. However, BitDefender quickly recognized that there was abnormal behavior that was occurring within the system and moved the infected files to quarantine before blocking all of the applications that were involved, labeling them as potentially malicious. Then, BitDefender advises that the user restart their system to finalize the cleaning process. At the end of this test, BitDefender was able to successfully detect and stop this malware threat through quarantining it and deleting it from the system.


You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it
The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest
malware-traffic-analysis.net/2019/07/19/index.html
MALWARE-TRAFFIC-ANALYSIS.NET
Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\Users\TheMan\Downloads\2019-07-19-traffic-analysis-exercise-malware (1)
Browse...
Show extracted files when complete
Extract
Cancel
15 items
1 item selected 3.79 MB

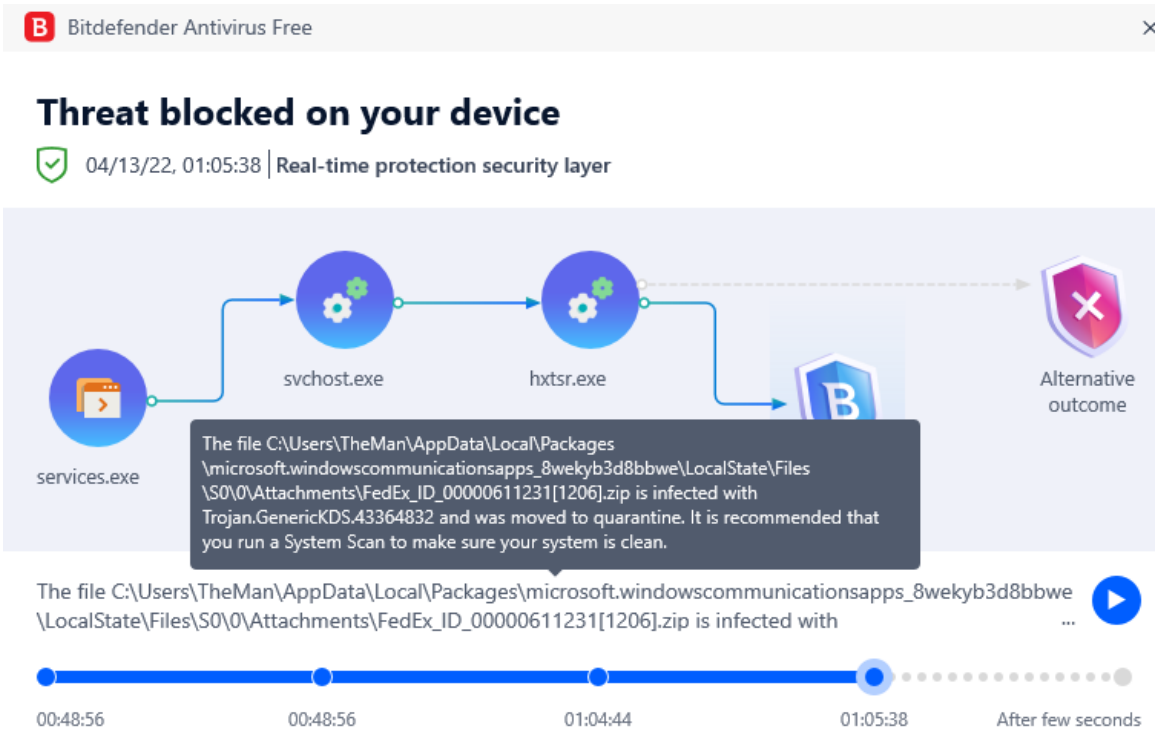

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to
The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse
MALWARE-TRAFFIC-ANALYSIS.NET
2019-07-19-traffic-analysis-exercise-malware (1)
Search 2019-07-19-traffic-analysis-exercise-malware (1)
Name
Date modified
Type
Size
2019-07-19-traffic-analysis-exercise-mal... 4/13/2022 12:59 AM Text Document 1 KB
client32 4/13/2022 12:59 AM Configuration sett... 1 KB
EIMOCFXM373 4/13/2022 12:59 AM Text Document 2,167 KB
HTCTL32.DLL 4/13/2022 12:59 AM Application exten... 321 KB
msvcr100.dll 4/13/2022 12:59 AM Application exten... 756 KB
nskbfltr 4/13/2022 12:59 AM Setup Information 1 KB
NSM 4/13/2022 12:59 AM Configuration sett... 7 KB
NSM.LIC 4/13/2022 12:59 AM LIC File 1 KB
pcicapi.dll 4/13/2022 12:59 AM Application exten... 33 KB
PCICHEK.DLL 4/13/2022 12:59 AM Application exten... 19 KB
PCICL32.DLL 4/13/2022 12:59 AM Application exten... 3,648 KB
remcmdstub 4/13/2022 12:59 AM Application 63 KB
shost 4/13/2022 12:59 AM Application 104 KB
TCCTL32.DLL 4/13/2022 12:59 AM Application exten... 388 KB
Disinfection in progress
Detected threat is being disinfected. Please wait until the process is complete.
14 items


You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make it unavailable to
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse
malware-traffic-analysis.net/2019/07/19/index.html
MALWARE-TRAFFIC-ANALYSIS.NET
2019-07-19-traffic-analysis-exercise-malware (1)
File
Home
Share
View
Dow... › 2019-07-19-traffic-a...
Search 2019-07-19-traffic-analysis-exercise-malware (1)
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
2019-07-19-traffic-analysis-exercise-mal... 4/13/2022 12:59 AM Text Document 1 KB
client32 4/13/2022 12:59 AM Configuration sett... 1 KB
EIMOCFXM373 4/13/2022 12:59 AM Text Document 2,167 KB
HTCTL32.DLL 4/13/2022 12:59 AM Application exten... 321 KB
msvcr100.dll 4/13/2022 12:59 AM Application exten... 756 KB
nskbfltr 4/13/2022 12:59 AM Setup Information 1 KB
NSM 4/13/2022 12:59 AM Configuration sett... 7 KB
NSM.LIC 4/13/2022 12:59 AM LIC File 1 KB
pcicapi.dll 4/13/2022 12:59 AM Application exten... 33 KB
PCICHEK.DLL 4/13/2022 12:59 AM Application exten... 19 KB
PCICL32.DLL 4/13/2022 12:59 AM Application exten... 3,648 KB
remcmdstub 4/13/2022 12:59 AM Application 63 KB
shost 4/13/2022 12:59 AM Application 104 KB
TCCTL32.DLL 4/13/2022 12:59 AM Application exten... 388 KB
14 items
Threat detected
Detected threats moved to quarantine
View details
Wednesday, April 13, 2022

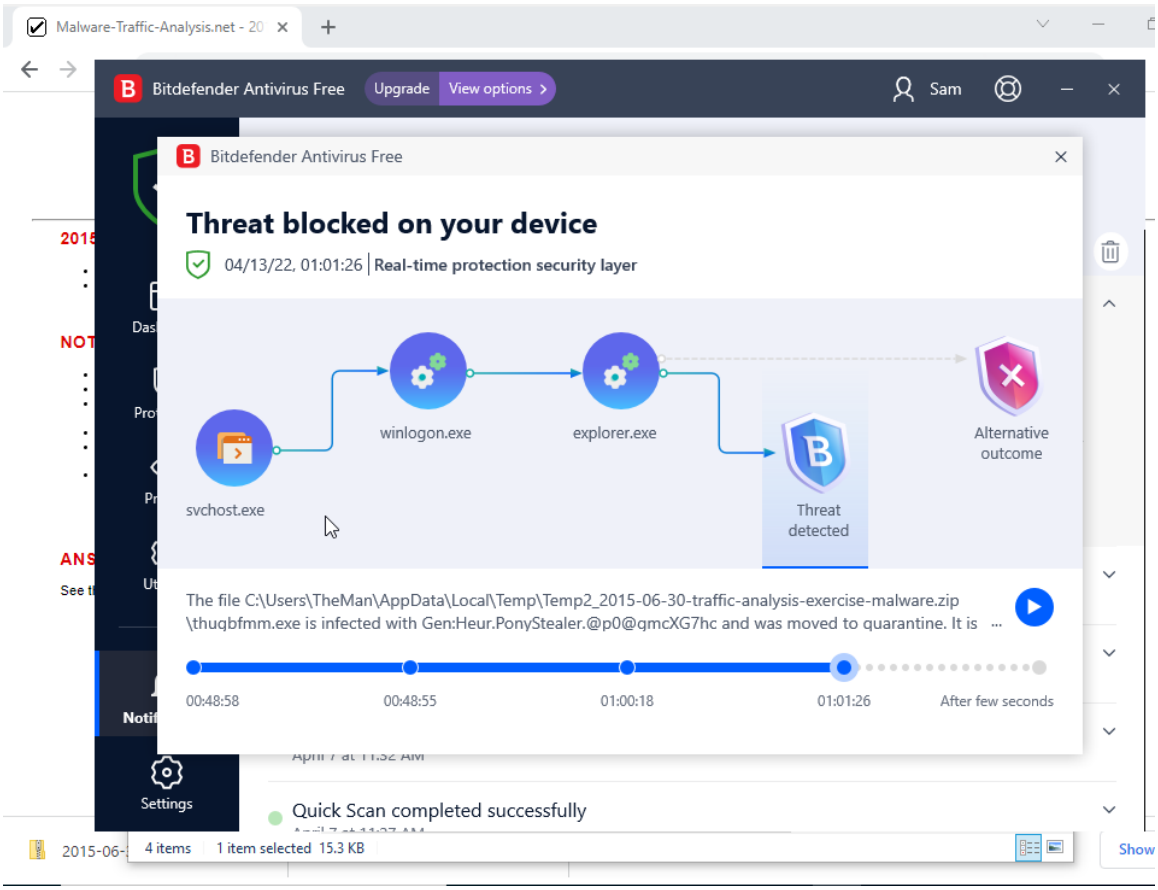

You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make it unavailable to
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse
MALWARE-TRAFFIC-ANALYSIS.NET
2019-07-19-traffic-analysis-exercise-malware (1)
File
Home
Share
View
Dow... › 2019-07-19-traffic-a...
Search 2019-07-19-traffic-analysis-exercise-malware (1)
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
2019-07-19-traffic-analysis-exercise-mal... 4/13/2022 12:59 AM Text Document 1 KB
client32 4/13/2022 12:59 AM Configuration sett... 1 KB
EIMOCFXM373 4/13/2022 12:59 AM Text Document 2,167 KB
HTCTL32.DLL 4/13/2022 12:59 AM Application exten... 321 KB
msvcr100.dll 4/13/2022 12:59 AM Application exten... 756 KB
nskbfltr 4/13/2022 12:59 AM Setup Information 1 KB
NSM 4/13/2022 12:59 AM Configuration sett... 7 KB
NSM.LIC 4/13/2022 12:59 AM LIC File 1 KB
pcicapi.dll 4/13/2022 12:59 AM Application exten... 33 KB
PCICHEK.DLL 4/13/2022 12:59 AM Application exten... 19 KB
PCICL32.DLL 4/13/2022 12:59 AM Application exten... 3,648 KB
remcmdstub 4/13/2022 12:59 AM Application 63 KB
shost 4/13/2022 12:59 AM Application 104 KB
TCCTL32.DLL 4/13/2022 12:59 AM Application exten... 388 KB
14 items
Malicious behavior blocked
Bitdefender detected potentially malicious behavior and blocked all applications involved.
View attack timeline
No new notifications



Exercise 2: In this test, I experimented with malware from a traffic analysis exercise called, “Email Roulette”. The malware involved is a trojan, that is distributed through infected emails that are sent out to unsuspecting users. Though the zip containing the various emails wasn’t blocked, when I downloaded and ran the file that would open the malware-ridden email, BitDefender detected the malware that was in the email as the email application that my system used was booting up. From there, before the email itself finished opening, BitDefender had already moved it into quarantine and prepared it for deletion which it was able to do shortly after. However, in that time, the files that were within the email file were already being executed, which meant that it still took for the executable that would actually initialize the malware to run for the firewall and antivirus to take action towards protecting the system. Also, it was able to identify that it was a trojan in the report of the attack timeline that it provided after taking care of the threat. To summarize this test, the antivirus was able to successfully stop the trojan from executing once the infected file was opened, although it wasn’t able to detect the malware or provide a warning regarding it when I downloaded the original zip file that contained it.



Exercise 3: For the final test that I conducted, I analyzed the response that BitDefender would have on a malware from the traffic exercise called “Identifying the EK (Exploit Kit) and infection chain”. The virus from this particular exercise was , which is a type of malware known as Pony Stealer, which steals passwords on a user's systems in addition to being able to decrypt and unlock them, using a vast variety of different applications to be able to accomplish this. It was distributed through a compromised website called “www.floridablueline.com”. I was able to download the executable with the malware just fine, but when I decided to run it on the system, that is when BitDefender began to recognize that there was malware in the executable that I was running. It then began to quarantine and successfully delete it from the system before it could have done any harm. During the removal of the malware, BitDefender was able to identify it as Pony Stealer, which is a tell tale that the antivirus uses a signature based detection system to be able to quickly recognize harmful programs.


Malware-Traffic-Analysis.net - 20
Bitdefender Antivirus Free
Upgrade
View options
Sam
Bitdefender Antivirus Free
Threat blocked on your device
04/13/22, 01:01:26 | Real-time protection security layer
svchost.exe
winlogon.exe
explorer.exe
Threat detected
Alternative outcome
The file C:\Users\TheMan\AppData\Local\Temp\Temp2_2015-06-30-traffic-analysis-exercise-malware.zip \thuqbfmm.exe is infected with Gen:Heur.PonyStealer.@p0@gmcXG7hc and was moved to quarantine. It is ...
00:48:58
00:48:55
01:00:18
01:01:26
After few seconds
Settings
Quick Scan completed successfully
4 items
1 item selected 15.3 KB

Letter of Transmittal Sample

April 21, 2021

University of The Incarnate Word
Attention: Dr. Gonzalo. D. Parra
4301 Broadway
San Antonio, TX 78209

Dear Dr. Parra:

With this letter, the team Joe Perez, Jimmy Aragon, Joshua Ibarra transmits the following items associated with the **CIS 3353 Final Project**.

SCOPE OF WORK (dated 4/21/2022): "Title of Your Work"

- DELIVERABLES related to the _____ sub-task:

  Aim 1:
  Deliverable 1
  Deliverable 2

  Aim 2:
  Deliverable 1
  Deliverable 2

Please share these with your team as appropriate. If you have any questions, please contact _____ at (210) 458-8618 or by email at _____.

Kindest regards,

Team Lead
Student of Cyber Security Systems at the University of the Incarnate Word