

**Name:** Hemant Jain

**Lab Progress Report Due Date:** 03/29/2021

**Current Week Since Start Date:** Week 10 (03/31/2021– 04/06/2021)

**Reporting Week:** From Mar 23, 2021 to Mar 29, 2021

**Summary about the TestOut Module-10 Learning:**

From the TestOut LabSim, I learnt about Securing Data and Applications. In this week's module., numerous conventions made within the past were outlined with few to no security controls. An unsecured protocol is one that does not give verification or encryption, or one that employs plaintext for passing authentication data or information. More current conventions with security controls incorporate Secure Attachment Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), HyperText Exchange Convention (HTTP), and HyperText Exchange Convention Secure (HTTPS).

In the later module, discussed in brief about IPsec Facts, Protocols, Modes of Operations, Internet Key Exchange(IKE), IPsec facts. Detailing out each layer of the OSI Model and discussing the two IPsec protocols namely Authentication Header(AH), Encapsulating Security Payload(ESP). The transport and tunnel mode in the IPsec and IKE facts was outlined in summary. Discussed about the Data Loss Prevention (DLP), which is a system that attempts to detect and stop breaches of sensitive data within an organization. Various DLP Implementations namely Network DLP, Endpoint DLP, File-level DLP, Cloud DLP were discussed in the further outliners. The two masking algorithms Dynamic data Masking and Static Data Masking working by replacing the sensitive data with the realistic fictional data.

Tokenization which is an effective tool to avoid the data loss and replaces out the actual data with a randomly generated alphanumeric character set called a token and stores original data on a server, protecting data on its server with authentication and authorization protocols allowing the continued control access to the file. Rights management classified in two types : Digital Rights (DRM) and Information Rights(IRM) was discussed.

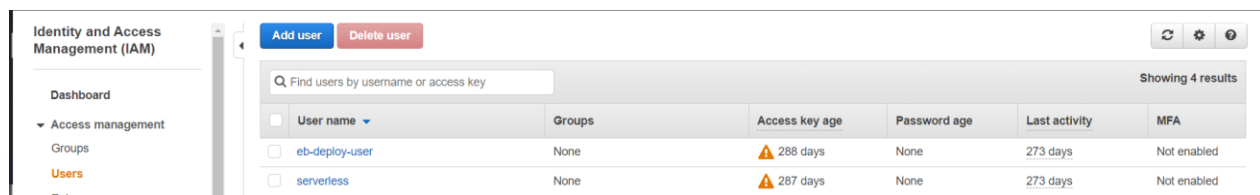
Learnt Techniques for the Enhanced Browser Privacy in the Browser Settings Cookies, Cache, Security, Add-ons, General. In detail description about the various methods attackers use to find the bug/loophole in the web applications and exploit it out namely Privilege Escalation, Pointer

Dereference, Buffer Overflows, Resource Exhaustion, Memory Leaks, Race Conditions, Error Handling, Improper Input Handling, replay attacks, Pass the hash, API attacks, SSL Scripting, Driver Manipulations.

Discussed in summary about the various Life Cycle Models available: Waterfall and agile along the Coding Errors and different types of them with some of Security testing methods like Normalization, Stored Procedures, Code Obfuscation, Code Reuse, Dead Code, Memory Management, Third-party libraries and software development kits(SDKs), Sensitive data exposure, Fuzz testing, Code Signing.

### Class Labs Screenshots:

#### IAM USER GROUP POLICIES:



The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Identity and Access Management (IAM)' at the top, followed by 'Dashboard', 'Access management' (expanded), 'Groups', 'Users' (highlighted), and 'Roles'. The main content area has a top bar with 'Add user' and 'Delete user' buttons, and a search bar labeled 'Find users by username or access key'. Below this is a table with 7 columns: 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. Two users are listed: 'eb-deploy-user' and 'serverless', both with 'None' for groups and '288 days'/'287 days' for access key age. The table indicates 'Showing 4 results'.

User name	Groups	Access key age	Password age	Last activity	MFA
eb-deploy-user	None	288 days	None	273 days	Not enabled
serverless	None	287 days	None	273 days	Not enabled

The image shows two screenshots of the AWS IAM console. The top screenshot displays the 'Roles' page, and the bottom screenshot displays the 'Policies' page.

**Top Screenshot: Roles Page**

The 'Roles' page shows a list of roles. The 'Create role' button is visible at the top. The table below shows 15 results.

Role name	Trusted entities	Last activity
<input type="checkbox"/> aws-quicksight-service-role-v0	AWS service: quicksight	59 days
<input type="checkbox"/> AWSServiceRoleForAutoScaling	AWS service: autoscaling (Service-Linked role)	11 days
<input type="checkbox"/> AWSServiceRoleForAWSCloud9	AWS service: cloud9 (Service-Linked role)	65 days
<input type="checkbox"/> AWSServiceRoleForECS	AWS service: ecs (Service-Linked role)	273 days
<input type="checkbox"/> AWSServiceRoleForElasticLoadBalancing	AWS service: elasticloadbalancing (Service-Linked role)	194 days
<input type="checkbox"/> AWSServiceRoleForOrganizations	AWS service: organizations (Service-Linked role)	None
<input type="checkbox"/> AWSServiceRoleForRDS	AWS service: rds (Service-Linked role)	67 days
<input type="checkbox"/> AWSServiceRoleForRedshift	AWS service: redshift (Service-Linked role)	67 days
<input type="checkbox"/> AWSServiceRoleForSupport	AWS service: support (Service-Linked role)	225 days
<input type="checkbox"/> AWSServiceRoleForTrustedAdvisor	AWS service: trustedadvisor (Service-Linked role)	None
<input type="checkbox"/> DataPipelineDefaultResourceRole	AWS service: ec2	68 days
<input type="checkbox"/> DataPipelineDefaultRole	AWS service: datapipeline and 1 more	68 days
<input type="checkbox"/> masters.cluster.dev.cloudknowledge.in	AWS service: ec2	11 days
<input type="checkbox"/> nodes.cluster.dev.cloudknowledge.in	AWS service: ec2	11 days

**Bottom Screenshot: Policies Page**

The 'Policies' page shows a list of policies. The 'Create policy' button is visible at the top. A green notification banner at the top states: "demo-for-cyber has been created." The table below shows 1 result.

Policy name	Type	Used as	Description
<input type="radio"/> demo-for-cyber	Customer managed	None	demo-for-cyber-policies

**WAF & Shield**

**AWS WAF**

Getting started

Web ACLs

IP sets

Regex pattern sets

Rule groups

AWS Marketplace

Switch to AWS WAF Classic

**AWS Shield**

**AWS Firewall Manager**

# AWS WAF

## Protect your web applications from common web exploits

AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.

**Get started with AWS WAF**

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

[Create web ACL](#)

**Pricing (US)**

- \$5 per web ACL per month (prorated hourly)
- \$1 per rule per month (prorated hourly)
- \$0.6 per million request processed

**What's new**

The migration wizard is now available, giving you a simple way to migrate your existing web ACL from AWS WAF Classic. To get started, please click [here](#) to launch the migration wizard and visit our documentation page [here](#) for more information.

urlscan.io/result/424a8b8e-1e22-4159-8d52-a4beeb06f329/

**jainhemant.herokuapp.com**

3.208.158.124

Submitted URL: <http://jainhemant.herokuapp.com/>

Effective URL: <http://jainhemant.herokuapp.com/index.html>

Submission: On March 29 via manual (March 29th 2021, 12:30:38 am) from US

**Summary**

This website contacted **9 IPs** in **3 countries** across **9 domains** to perform **28 HTTP transactions**. The main IP is **3.208.158.124**, located in **Ashburn, United States** and belongs to **AMAZON-AES, US**. The main domain is **jainhemant.herokuapp.com**.

This is the only time **jainhemant.herokuapp.com** was scanned on urlscan.io!

urlscan.io Verdict: **No classification**

**Live information**

Google Safe Browsing: **No classification for jainhemant.herokuapp.com**

Current DNS A record: **52.6.203.110 (AS14618 - AMAZON-AES, US)**

**Domain & IP information**

IP/ASNs | IP Detail | Domains | Domain Tree | Links | Certs | Frames

**Screenshot**

[Live screenshot](#) [Full image](#)

**Page URL History**

1. <http://jainhemant.herokuapp.com/> <http://jainhemant.herokuapp.com/index.html>

**Project 3-1: Analyze File and URL for File-Based Viruses Using VirusTotal-Part 1**

The screenshot shows the VirusTotal interface for a file analysis. The file is named "VirusTotal.docx" with a SHA-256 hash of 8320c484c2ce631eac4e6d32bab6da4ac9e26de876d9afbfcac443b8bff2a136. It is 11.83 KB in size and was uploaded on 2021-03-28 at 23:09:21 UTC. The file has been scanned by 62 engines, and all have reported it as "Undetected". The community score is 7, indicating a low risk of being a virus. The interface includes tabs for Detection, Details, Relations, and Community. The Detection tab is active, showing a list of scanning engines and their results.

8320c484c2ce631eac4e6d32bab6da4ac9e26de876d9afbfcac443b8bff2a136

0 / 62

No engines detected this file

8320c484c2ce631eac4e6d32bab6da4ac9e26de876d9afbfcac443b8bff2a136  
VirusTotal.docx  
11.83 KB  
Size  
2021-03-28 23:09:21 UTC  
a moment ago  
DOCX

Community Score: 7

DETECTION	DETAILS	RELATIONS	COMMUNITY
Acronis	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Aibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	CAT-QuickHeal	Undetected
ClamAV	Undetected	CMC	Undetected

https://www.virustotal.com/gui/file/8320c484c2ce631eac4e6d32bab6da4ac9e26de876d9afbfcac443b8bff2a136/detection

ESET-NOD32	Undetected	F-Secure	Undetected
FireEye	Undetected	Fortinet	Undetected
GData	Undetected	Gridinsoft	Undetected
Ikarus	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kaspersky	Undetected	Kingsoft	Undetected
Malwarebytes	Undetected	MAX	Undetected
MaxSecure	Undetected	McAfee	Undetected
McAfee-GW-Edition	Undetected	Microsoft	Undetected
NANO-Antivirus	Undetected	Panda	Undetected
Qihoo-360	Undetected	Rising	Undetected
Sangfor Engine Zero	Undetected	SentinelOne (Static ML)	Undetected
Sophos	Undetected	SUPERAntiSpyware	Undetected
Symantec	Undetected	TACHYON	Undetected
Tencent	Undetected	TrendMicro	Undetected
TrendMicro-HouseCall	Undetected	VBA32	Undetected

https://www.virustotal.com/gui/

Week 10 Network Security.pdf x VirusTotal x +

https://www.virustotal.com/gui/file/8320c484c2ce631eac4e6d32bab6da4ac9e26de876d9afbcae443b8bff2a136/detection

8320c484c2ce631eac4e6d32bab6da4ac9e26de876d9afbcae443b8bff2a136

Sangfor Engine Zero	Undetected	SentinelOne (Static ML)	Undetected
Sophos	Undetected	SUPERAntiSpyware	Undetected
Symantec	Undetected	TACHYON	Undetected
Tencent	Undetected	TrendMicro	Undetected
TrendMicro-HouseCall	Undetected	VBA32	Undetected
VIPRE	Undetected	ViRobot	Undetected
Yandex	Undetected	Zillya	Undetected
ZoneAlarm by Check Point	Undetected	Zoner	Undetected
SecureAge APEX	Unable to process file type	BitDefenderFake	Unable to process file type
CrowdStrike Falcon	Unable to process file type	Cybereason	Unable to process file type
Cylance	Unable to process file type	eGambit	Unable to process file type
Elastic	Unable to process file type	Palo Alto Networks	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trapmine	Unable to process file type
Webroot	Unable to process file type	Trustlook	—

Sign in Sign up

**University Website VirusTotal Screenshots:**

The screenshot displays the VirusTotal interface for the URL <http://www.northeastern.edu/>. The page shows a green circle with '0' and '82' indicating the detection status. Below this, a table lists various detection engines and their results. The table is organized into two columns, with the first column listing engines and the second column showing the detection result (Clean or Unrated).

DETECTION	DETAILS	LINKS	COMMUNITY
ADMINUSLabs	✓ Clean	AegisLab WebGuard	✓ Clean
AlienVault	✓ Clean	Anti-AVL	✓ Clean
Armis	✓ Clean	Artists Against 419	✓ Clean
Avira (no cloud)	✓ Clean	BADWARE.INFO	✓ Clean
Baidu-International	✓ Clean	BitDefender	✓ Clean
BlockList	✓ Clean	Blueliv	✓ Clean
Certego	✓ Clean	CINS Army	✓ Clean
CLEAN MX	✓ Clean	CMC Threat Intelligence	✓ Clean
Comodo Valkyrie Verdict	✓ Clean	CRDF	✓ Clean
Quttera	✓ Clean	Rising	✓ Clean
Sangfor Engine Zero	✓ Clean	SCUMWARE.org	✓ Clean
SecureBrain	✓ Clean	securolytics	✓ Clean
Snort IP sample list	✓ Clean	Sophos	✓ Clean
Spam404	✓ Clean	Spamhaus	✓ Clean
StopForumSpam	✓ Clean	Sucuri SiteCheck	✓ Clean
Tencent	✓ Clean	ThreatHive	✓ Clean
Threatsourcing	✓ Clean	Trustwave	✓ Clean
URLhaus	✓ Clean	Virusdie External Site Scan	✓ Clean
VX Vault	✓ Clean	Web Security Guard	✓ Clean
Yandex Safebrowsing	✓ Clean	ZeroCERT	✓ Clean
zvelo	✓ Clean	AutoShun	? Unrated
Cyan	? Unrated	Lumu	? Unrated
Netcraft	? Unrated	NotMining	? Unrated
PhishLabs	? Unrated	StopBadware	? Unrated

Que: How could VirusTotal be useful to users? How could it be useful to security researchers? Could it also be used by attackers to test their own malware before distributing it to ensure that it does not trigger an AV alert? What should be the protections against this?

Ans: VirusTotal inspects items with over 70 antivirus scanners and URL/domain blacklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal. VirusTotal offers several file submission methods, including the primary public web interface, desktop uploaders, browser extensions and a programmatic API. The web interface has the highest scanning priority among the publicly available submission methods. Submissions may be scripted in any programming language using the HTTP-based public API.

As with files, URLs can be submitted via several different means including the VirusTotal webpage, browser extensions and the API.

Upon submitting a file or URL basic results are shared with the submitter, and between the examining partners, who use results to improve their own systems. As a result, by submitting files, URLs, domains, etc. to VirusTotal you are contributing to raise the global IT security level.

This core analysis is also the basis for several other features, including the VirusTotal Community: a network that allows users to comment on files and URLs and share notes with each other. VirusTotal can be useful in detecting malicious content and in identifying false positives -- normal and harmless items detected as malicious by one or more scanners.

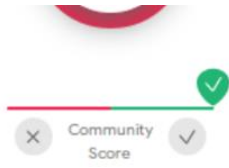
VirusTotal not only tells you whether a given antivirus solution detected a submitted file as malicious, but also displays each engine's detection label (e.g., I-Worm.Allapple.gen). The same is true for URL scanners, most of which will discriminate between malware sites, phishing sites, suspicious sites, etc. Some engines will provide additional information, stating explicitly whether a given URL belongs to a particular botnet, which brand is targeted by a given phishing site, and so on.

### **Project 3-2: Analyze Virus File Using VirusTotal-Part 2**

Was Popped up with the error and was unable to get it inside the Windows Sandbox. But overall, I understood the concept and looks quite like the above practical inside of uploading the VirusTotal.docx file we were uploading the eicar.com file.



Performed the lab on the SEED Ubuntu machine on the VirtualBox:



Community Score

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

eicar.com-52494

attachment text via-tor

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY <span>20+</span>
Ad-Aware	ⓘ EICAR-Test-File (not A Virus)			AegisLab
AhnLab-V3	ⓘ Virus/EICAR_Test_File			Alibaba
ALYac	ⓘ Misc.Eicar-Test-File			Antiy-AVL
SecureAge APEX	ⓘ EICAR Anti-Virus Test File			Arcabit
Avast	ⓘ EICAR Test-NOT Virus!!!			Avast-Mobile
AVG	ⓘ EICAR Test-NOT Virus!!!			Avira (no cloud)
Baidu	ⓘ Win32.Test.Eicar.a			BitDefender
BitDefenderTheta	ⓘ EICAR-Test-File (not A Virus)			Bkav Pro
CAT-QuickHeal	ⓘ EICAR.TestFile			ClamAV
CMC	ⓘ Eicar.test.file			Comodo
Cynet	ⓘ Malicious (score: 85)			Cyren
DrWeb	ⓘ EICAR Test File (NOT A Virus!)			Elastic
Emsisoft	ⓘ EICAR-Test-File (not A Virus) (B)			eScan

### Project 3-3: Explore Ransomware Sites

**Que:** Read through the Prevention Advice. Do you think it is helpful?

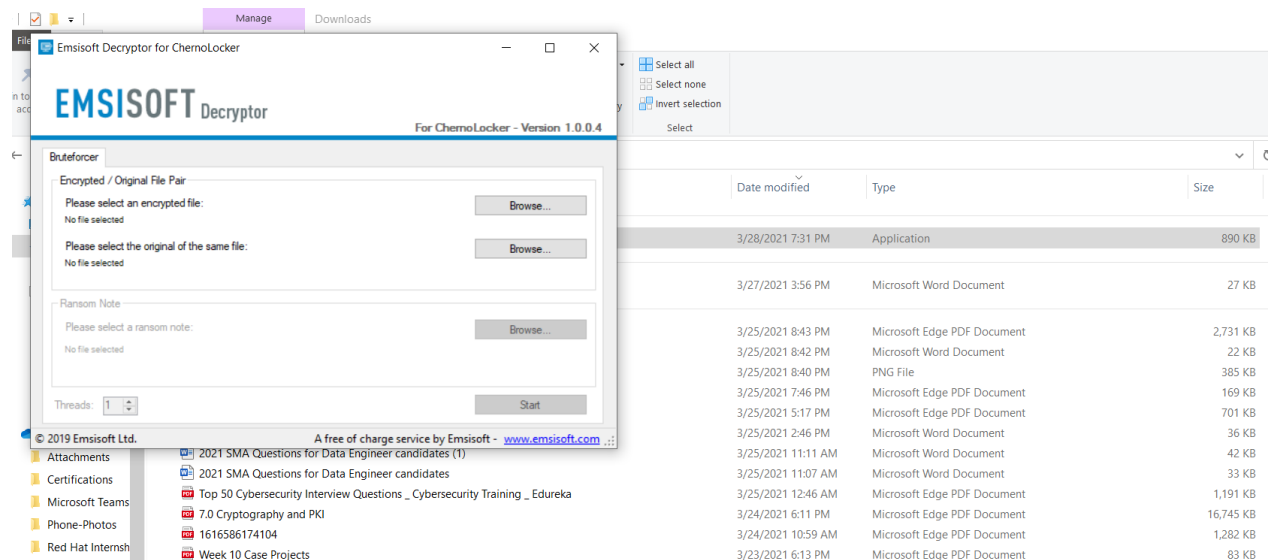
**Ans:** Yes, it was helpful to get some basic information needed to prevent the ransom attacks like creating Back-up, enabling antivirus software, and updating system software etc.

**Que:** Click Crypto Sheriff. How could this be useful to a user who has suffered a ransomware infection?

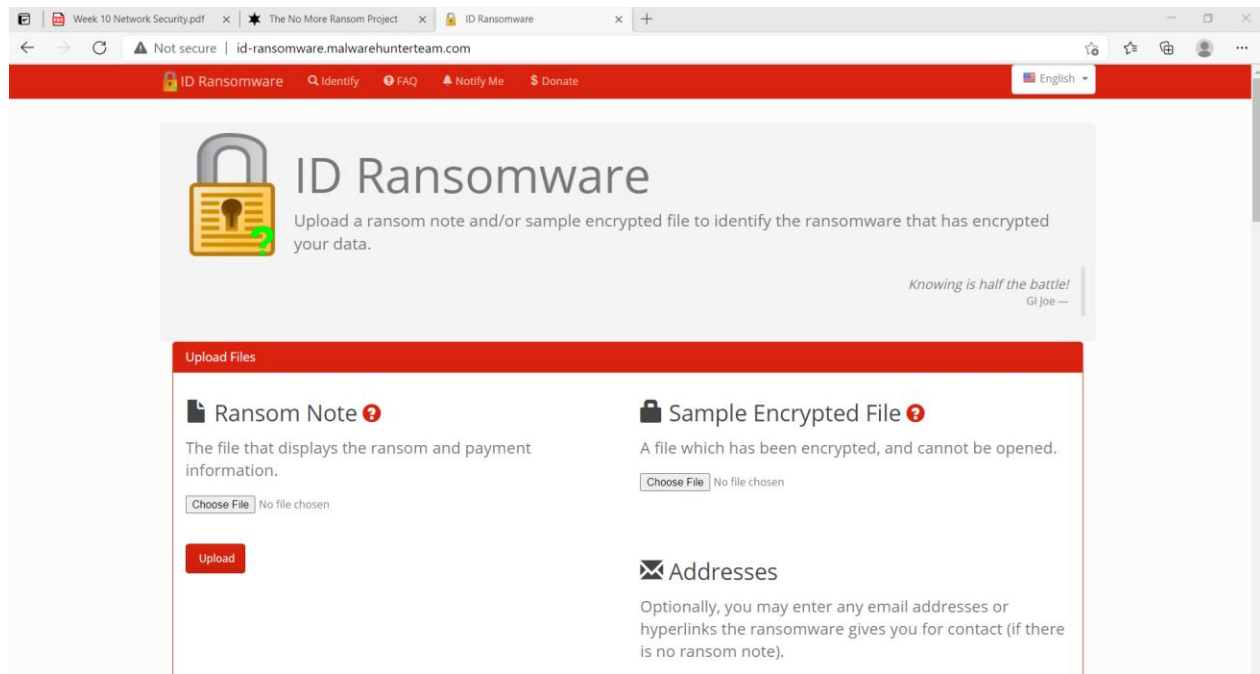
**Ans:** To help us define the type of ransomware affecting your device, please fill in the form below. This will enable us to check whether there is a solution available. If there is, we will provide you with the link to download the decryption solution.

**Que:** Click Ransomware: Q&A. Read through the information. Which statements would you agree with? Which statements would you disagree with?

**Ans:** Agree with all statements.



[ID Ransomware \(malwarehunterteam.com\)](http://malwarehunterteam.com)



**Que:** What features does this site provide?

**Ans:** ID Ransomware is, and always will be, a free service to the public. It is currently a personal project that I have created to help guide victims to reliable information on a ransomware that may have infected their system. Other than direct development and signature additions to the website itself, it is an overall community effort.

**Que:** How could the website like ID Ransomware be useful?

**Ans:** Everyone can be the target of a ransomware attack. It doesn't discriminate whether you are rich or poor, for as long as your computer is not secured, you can be infected by ransomware. Each one must learn how to identify ransomware in order to know what to do in case you encounter an attack.

Ransomware can be dangerous if it is on your computer. Simply because it locks your computer and sometimes it encrypts your data. You will know that you have been infected when there is a ransom message on your screens. Then it demands you to pay a certain amount, typically in the form of cryptocurrency.

ID ransomware behavior is silent but deadly. It has many ways on how it could enter your computer. If you do not know how to identify ransomware and how it acts, it would be difficult for you to make a solution to the problem it created.

**File Encryption**

One simple way on identify ransomware on your computer is when the file got encrypted. Ransomware has the capability of encrypting all kind of files. It includes photos, videos, office documents and many else.

**File Renaming**

When an id ransomware gets into your computer, it renames your data. This is a better way of identifying ransomware on your computer. This is typical behavior of a ransomware to create confusion on which file is affected.

**File Extension Alteration**

To help you on how to identify ransomware, you can check the extension file of your data. If the extensions were altered and became an unknown character, there is a big possibility of a ransomware infection on your computer.

**Ransom Note on the Screen**

Usually, you will never know when a ransomware gets inside to your computer. It will secretly do what it needs to do, and when it is finished, that is the time it will reveal itself. A good way to know identify ransomware is when you see a ransom message flashed to your screen. It demands you to pay a ransom fee for a certain period. If you fail to pay the criminals, all your files will be deleted.

**Turn your Computer into Botnets**

One of the things that may happen to your computer when you have been infected by a ransomware is to become a bot in a botnet. Although it would be difficult for you how to identify ransomware on your computer if it became a botnet. You will just notice that your PC is running slow and keeps on hanging most of the time.

**Spread in the Network**

Another common way on how to identify Ransomware is when your neighboring computers also gets infected. It is because ransomware can spread the infection into your local network. So, if you are infected, all the computer connected to your network will also be infected by the ransomware.

## Data extraction

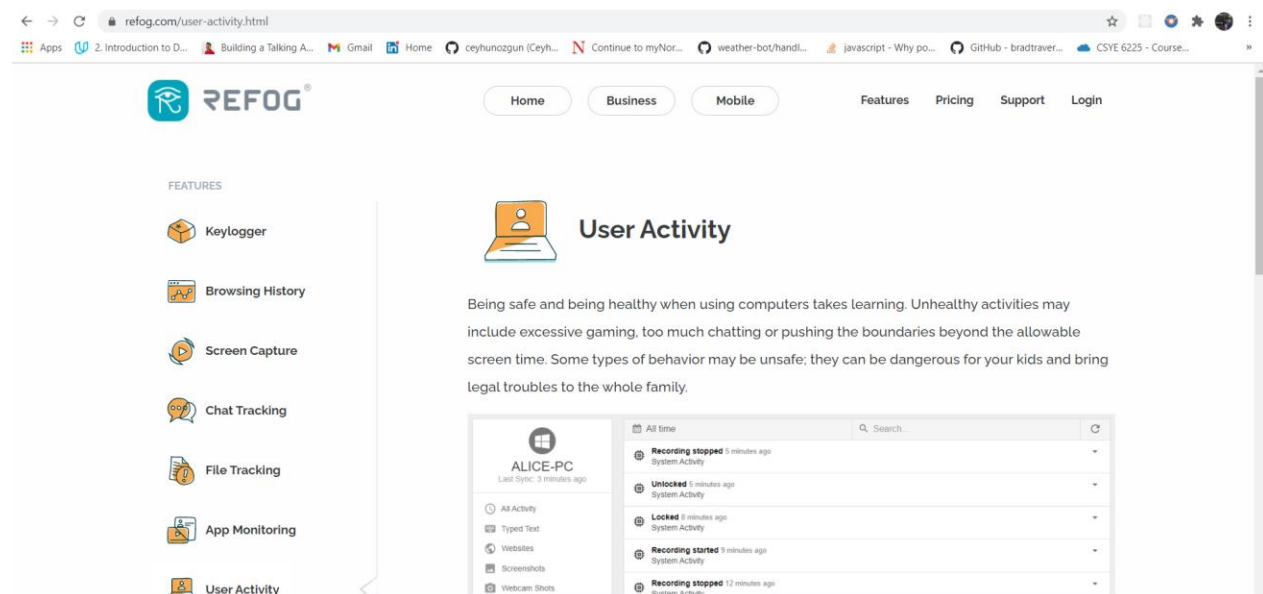
The last option on how to identify ransomware is data extraction. Although this also happens in the background and would be hard to recognize. Once it has extracted your files, you will never know what it will do next. It could upload your file to criminal's server or encrypt them all.

## Sources of Ransomware

There are many sources on how to identify ransomware on your computer. One typical way is when you visited a compromised website. If the website is infected by a ransomware and you accidentally visited the site, the ransomware script could be transferred to your computer.

Another way is via spam emails. When you received an email coming from an unknown sender and you open the email and click any link that is on that email. There is a big chance of getting infected by a ransomware. The spam emails might also include a malicious attachment that could be carrying a script. If you happen to open the attachments, the malicious script may run to your computer and infect yours with the ransomware.

## Project 3-4: Use a Software Keylogger



Performed all the key steps and uninstalled the tool immediately.

**Progress Embedded Image of Progress Report from LabSim:**

Score Sheet: TestOut Security Pro: Jain, Hemant

Product: TestOut Security Pro 7.0

Resources to Show: ☒ Exams ☒ Labs ☐ Lessons ☐ Videos

Date Range: Start: End:

Show scores as points: ☐

Resource	Time In Resource	Newest Score	Highest Score	Lowest Score	Average Score	Points Possible	Attempts
9.8.4 Secure an iPad	11 minutes 12 seconds	100% (3/22/2021 11:5...	100% (3/22/2021 11:5...	0% (3/22/2021 11:49 ...	50%	8	2
9.8.6 Create a Guest ...	6 minutes 13 seconds	100% (3/23/2021 12:0...	100% (3/23/2021 12:0...	0% (3/22/2021 11:59 ...	50%	4	2
9.8.7 Section Quiz	2 minutes 35 seconds	100% (3/22/2021 6:13...	100% (3/22/2021 6:13...	100% (3/22/2021 6:13...	100%	10	1
9.9.6 Section Quiz	1 minute 35 seconds	100% (3/22/2021 5:05...	100% (3/22/2021 5:05...	100% (3/22/2021 5:05...	100%	10	1
10.1.5 Allow SSL Con...	3 minutes 33 seconds	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100%	3	1
10.1.9 Section Quiz	1 minute 44 seconds	100% (3/27/2021 10:5...	100% (3/27/2021 10:5...	100% (3/27/2021 10:5...	100%	10	1
10.2.3 Section Quiz	1 minute 6 seconds	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100%	10	1
10.3.10 Clear the Bro...	55 seconds	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100%	1	1
10.3.15 Perform an S...	3 minutes 54 seconds	100% (3/27/2021 11:1...	100% (3/27/2021 11:1...	100% (3/27/2021 11:1...	100%	2	1
10.3.16 Section Quiz	1 minute 6 seconds	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100%	10	1
10.4.10 Implement Ap...	5 minutes 56 seconds	100% (3/27/2021 11:1...	100% (3/27/2021 11:1...	100% (3/27/2021 11:1...	100%	4	1
10.4.12 Implement D...	3 minutes 48 seconds	100% (3/27/2021 11:2...	100% (3/27/2021 11:2...	100% (3/27/2021 11:2...	100%	3	1
10.4.14 Section Quiz	1 minute 1 second	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100%	10	1
11.1.4 Section Quiz						10	0
11.2.9 Section Quiz						10	0
11.3.5 Implement Intr...						5	0
11.3.6 Section Quiz						10	0
11.4.7 Scan for Wind...						6	0