

Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
Leandro Delgado	114416241	As Posted	8%

Name	In-Class Lab: Malware sandbox analysis
Main Goal	Case Investigation
Instructions	<ul style="list-style-type: none"> <li>It is an Individual assignment. Put your name + Student ID in the empty spaces above.</li> <li>Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.</li> <li>Show me genuine signs of your work is done on your machine. This includes: <ul style="list-style-type: none"> <li>Screenshots that show your desktop background with Date/Time.</li> </ul> </li> </ul>
Case Brief	In this scenario, you have uploaded a malware sample to Joe Sandbox and will analyze the results.
Students Work required for this activity	<ul style="list-style-type: none"> <li>Go to <a href="https://www.joesandbox.com/analysispaged/0">https://www.joesandbox.com/analysispaged/0</a></li> <li>Choose a malicious file (one with an Antivirus value greater than 80%) that has been uploaded to the sandbox</li> <li>Click the left-most button to view the HTML report of the sandbox analysis</li> <li>Use the details from the report to analyze what the malicious file is doing. Please use caution to NOT download/execute the uploaded file. Downloading or executing the malicious file is against Seneca policy and there will be consequences.</li> <li>Your report should include:</li> </ul>

← ↻ 🏠 <https://www.joesandbox.com/analysis/search?q=threatnames:Redline> A ☆ ⚙️ ⌵

Import favorites For quick access, place your favorites here on the favorites bar. [Manage favorites now](#)

**JOESandbox Cloud BASIC** threatnames.Redline Analyze Results [Register](#) [Login](#)

Deep Malware Analysis

[AgentTesla](#) [Redline](#) [Njrat](#) [LummaC](#) [Formbook](#) [Amadey](#) [Snake Keylogger](#) [Xworm](#) [Vidar](#) [RisePro](#) [Remcos](#)

Not found what you are looking for? Try: [Advanced Search](#)

### 20 search results for "threatnames:Redline"

(limited to max. 20 search results)

Detection	Sample Info	Download Report	Classification & Info	Graph
<b>MALICIOUS</b> RedLine AV: 36%	49b35e.msi 2025-04-01 14:38:09 +02:00	Full Report Management Report IOC Report	Info Class	
<b>MALICIOUS</b> RedLine AV: 67%	Payment_Advice.exe 2025-03-28 14:57:24 +01:00	Full Report Management Report IOC Report	Info Class	
<b>MALICIOUS</b> AgentTesla, PureLo... AV: 96%	swift_copy_MTC87365-PN... 2025-03-28 02:50:38 +01:00	Full Report Management Report IOC Report	Info Class	
<b>MALICIOUS</b> AgentTesla, PureLo... AV: 96%	RFQ-B2M8938-MATERIAL... 2025-03-27 12:55:27 +01:00	Full Report Management Report IOC Report	Info Class	
<b>MALICIOUS</b> RedLine, XWorm AV: 83%	RFQ-ON736672-MATERIA... 2025-03-25 18:19:08 +01:00	Full Report Management Report IOC Report	Info Class	
<b>MALICIOUS</b> DarkTortilla, RedLine AV: 0%	"powershell.exe" -c "iwr h... 2025-03-25 15:58:52 +01:00	Full Report Management Report IOC Report	Info Class	
<b>MALICIOUS</b> RedLine AV: 69%	OUvDZlu1tw.exe 2025-03-24 18:50:21 +01:00	Full Report Management Report IOC Report	Info Class	
<b>MALICIOUS</b> AgentTesla, PureLo... AV: 83%	POP_Swift_Copy_MTC78... 2025-03-24 13:30:35 +01:00	Full Report Management Report IOC Report	Info Class	
<b>MALICIOUS</b> RedLine AV: 78%	CxDfBJ42IP.exe 2025-03-24 08:57:43 +01:00	Full Report Management Report IOC Report	Info Class	

Leandro Delgado  
student number: 114416241

Ln 2, Col 25 41 characters 100% Window UTF-8

This screenshot shows a search on Joe Sandbox Cloud for malware samples related to **Redline**, a known infostealer. The page displays a list of detected malicious files, including their names, detection rates, analysis reports, and classification details. One sample, titled **RFQ-B2M8938-MATERIALS**, is highlighted, indicating a possible focus for further analysis. The interface also provides access to full, management, and IOC reports, along with behavior graphs for deeper investigation.

- The file name

Import favorites | For quick access, place your favorites here on the favorites bar. [Manage favorites now](#)

# JOeSandbox Cloud BASIC

Overview Signatures Process

## Windows Analysis Report

**RFQ-B2M8938-MATERIALS&SPECIFICATIONS-PO893873.exe**

### Overview

#### General Information

Sample name:	RFQ-B2M8938-MATERIALS&SPECIFICATIONS-PO893873.exe
Analysis ID:	1650068
MD5:	91521adf3bb37d62cc85...
SHA1:	fc3788e6ceaf1c5bbeeb...
SHA256:	24d9992ff5374362ef6cf...
Tags:	exe user-TeamDreier
Infos:	

#### Detection

**MALICIOUS**

SUSPICIOUS

CLEAN

UNKNOWN

#### Signatures


- Antivirus detection for
- Found malware config
- Malicious sample dete
- Multi AV Scanner dete
- Multi AV Scanner dete
- Sigma detected: Drops
- Suricata IDS alerts for
- Yara detected AgentTe

This screenshot displays a **Windows Analysis Report** from Joe Sandbox Cloud for a suspicious file named "**RFQ-B2M8938-MATERIALS&SPECIFICATIONS-PO893873.exe**". The sample has been flagged as **MALICIOUS**, as shown in the detection panel. Under the "General Information" section, the file's hashes (MD5, SHA1, SHA256), tags, and related analysis ID are listed. This report provides a high-level overview of the file's behavior and classification, confirming it as a threat likely related to a known malware family such as **Redline** or **AgentTesla**, based on previous context.

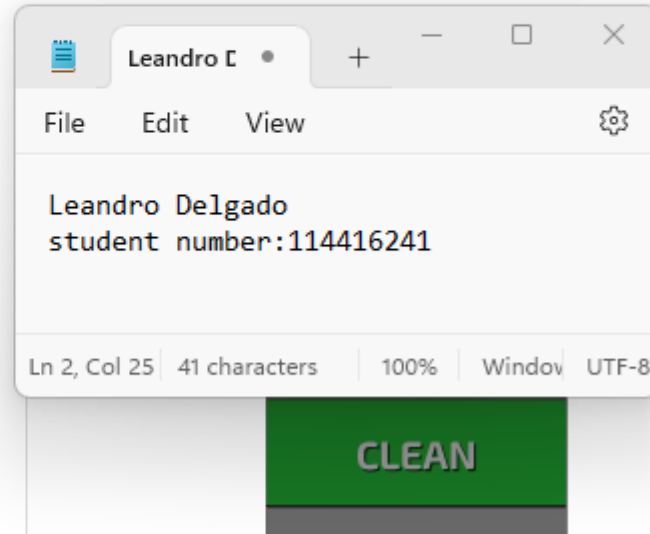
- MD5 and SHA256 hashes

## Overview

### General Information

Sample name:	RFQ-B2M8938-MATERIALS&SPECIFICATIONS-PO893873.exe
Analysis ID:	1650068
MD5:	91521adf3bb37d62cc85...
SHA1:	fc3788e6ceaf1c5bbeeb...
SHA256:	24d9992ff5374362ef6cf...
Tags:	exe user-TeamDreier
Infos:	

### Detection

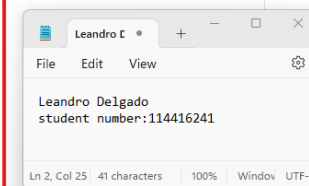
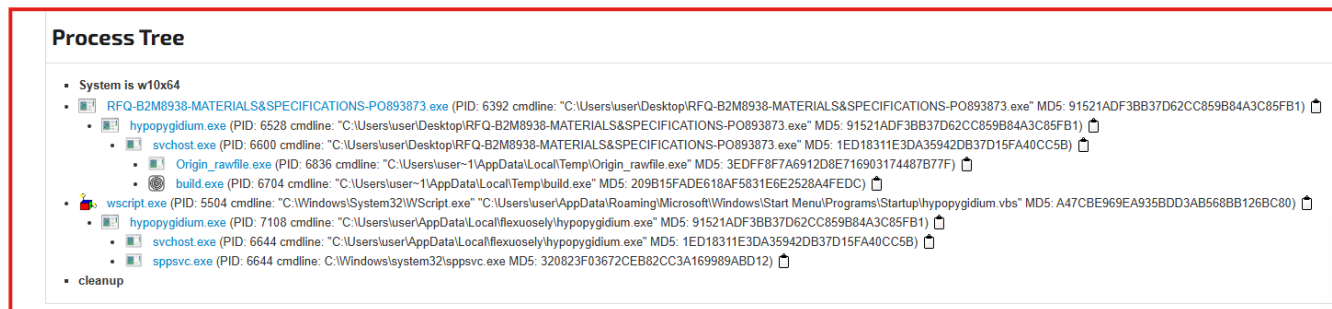


This screenshot focuses on the **General Information** section of a malware analysis report from Joe Sandbox Cloud. It shows a file named "**RFQ-B2M8938-MATERIALS&SPECIFICATIONS-PO893873.exe**", along with its unique hash identifiers:

- **MD5:** 91521adf3bb37d62cc85...
- **SHA256:** 24d9992ff5374362ef6cf...

These cryptographic hashes help identify and track the exact sample across other databases or reports. This type of information is critical in threat intelligence and malware research, allowing analysts to verify file integrity and determine if a file has been seen before in other attacks.

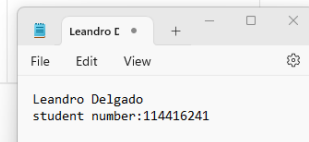
## Process tree



This screenshot shows the **process tree** of a malware sample executed on a Windows 10 system. The file RFQ-B2M8938-MATERIALS&SPECIFICATIONS-PO893873.exe spawns several suspicious processes, including svchost.exe, wscript.exe, and hypopygidium.exe, indicating malicious activity. One script is placed in the startup folder, suggesting an attempt to establish persistence. This visual helps trace the malware's behavior and impact on the system.

## Malware threat intel (if available)

Malware Threat Intel				
Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based information stealer readily available to actors due to leaked build. The malware is able to log keystrokes, can access the host's clipboard and crawls the disk for credentials or other valuable information. It has the capability to send information back to its C&C via HTTP(S), SMTP, FTP, or towards a Telegram channel.	• SWEED	<ul style="list-style-type: none"><li><a href="http://blog.nsfocus.net/sweed-611/">http://blog.nsfocus.net/sweed-611/</a></li><li><a href="http://1v1ngc0d3.wordpress.com/2021/11/...">http://1v1ngc0d3.wordpress.com/2021/11/...</a></li><li><a href="http://ropgadget.com/posts/originlogger.html">http://ropgadget.com/posts/originlogger.html</a></li><li><a href="http://www.secureworks.com/research/thre...">http://www.secureworks.com/research/thre...</a></li><li><a href="https://0xnmrmagnezi.github.io/malware%2...">https://0xnmrmagnezi.github.io/malware%2...</a></li></ul>	<a href="https://malpedia.caad.fkie.fraunhofer.de/det...">https://malpedia.caad.fkie.fraunhofer.de/det...</a>
Name	Description	Attribution	Blogpost URLs	Link
RedLine Stealer	RedLine Stealer is a malware available on underground forums for sale apparently as a standalone (\$100/\$150 depending on the version) or also on a subscription basis (\$100/month). This malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of RedLine added the ability to steal cryptocurrency. FTP and IM clients are also apparently targeted by this family, and this malware has the ability to upload and download files, execute commands, and periodically send back information about the infected computer.	No Attribution	<ul style="list-style-type: none"><li><a href="https://any.run/cybersecurity-blog/crackedc...">https://any.run/cybersecurity-blog/crackedc...</a></li><li><a href="https://apophis133.medium.com/redline-te...">https://apophis133.medium.com/redline-te...</a></li><li><a href="https://asec.ahnlab.com/en/30445/">https://asec.ahnlab.com/en/30445/</a></li><li><a href="https://asec.ahnlab.com/en/35981/">https://asec.ahnlab.com/en/35981/</a></li><li><a href="https://asec.ahnlab.com/ko/25837/">https://asec.ahnlab.com/ko/25837/</a></li></ul>	<a href="https://malpedia.caad.fkie.fraunhofer.de/det...">https://malpedia.caad.fkie.fraunhofer.de/det...</a>



The “Malware Threat Intel” section highlights two dangerous info-stealing malware families: **Agent Tesla** and **RedLine Stealer**. Agent Tesla is a .NET-based malware capable of logging keystrokes, accessing clipboard contents, and scanning the disk for sensitive information such as credentials. It can send the stolen data to its command-and-control server via various channels including HTTP(S), SMTP, FTP, and Telegram. This malware is attributed to the group SWEED and is frequently used due to leaked builders available online. On the other hand, RedLine Stealer is a widely available commercial malware sold on underground forums for a flat fee or monthly subscription. It is designed to harvest browser credentials, autocomplete data, credit card information, and system details like user info, location, and installed software. More advanced variants can also steal cryptocurrency and target FTP and instant messaging clients. RedLine can upload/download files, execute remote commands, and periodically report back to its operators. Unlike Agent Tesla, RedLine has no specific attribution, indicating broad use across different threat actors. Both malware types are extensively documented through blog articles and Malpedia entries, offering valuable insight for security researchers and analysts.

- Yara Signatures

Yara Signatures

PCAP (Network Traffic)					
Source	Rule	Description	Author	Strings	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security		
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security		

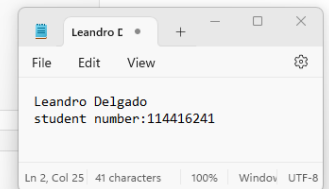
Dropped Files

Source	Rule	Description	Author	Strings	
C:\Users\user\AppData\Local\Temp\build.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security		
C:\Users\user\AppData\Local\Temp\build.exe	infostealer_win_redline_strings	Finds Redline samples based on characteristic strings	Sekoia.io	<div><div><div>0x24cc3.\$gen01: ChromeGetRoamingName</div><div>0x24cc8.\$gen02: ChromeGetLocalName</div><div>0x242db.\$gen03: get_UserDomainName</div><div>0x28bc4.\$gen04: get_encrypted_key</div><div>0x27943.\$gen05: browserPaths</div><div>0x27c19.\$gen06: GetBrowsers</div><div>0x27501.\$gen07: get_installedInputLanguages</div><div>0x238cc.\$gen08: BCRYPT_INIT_AUTH_MODE_INFO_VERSION</div><div>0x3018.\$spe1: [AString-ZaString-zt0][2String4]\[String-w-][String0]\[wString-][2String7]</div><div>0x29006.\$spe7: OFInfoFileInfora GFileInfoX StabFileInfora</div><div>0x290a4.\$spe8: ApGenerierDaGenerisRGenericoamGenering0</div><div>0x296c5.\$spe9: "wait4"</div><div>0x219ea.\$typ02: F413CEA9BAA458730567FE47F57CC3C94DDF83C0</div><div>0x21f14.\$typ03: A937C89924769689556595B3BD09607749A2042</div><div>0x21fc1.\$typ04: D07333042BFFC20116BF01BC556566EC76C0F7E2</div><div>0x21998.\$typ07: 77A9683FAF2EC9EC3DABC09D33C3BD04E8897D80</div><div>0x219c1.\$typ08: A8F9B42190DF0856920D5ED70E2B0F0C96A25280</div><div>0x21592.\$typ10: 2FBDC61103D91C142CC969071EABATD3D10FF6301</div><div>0x21c65.\$typ11: 2A16BF07D33718198219588A968782C51711B52</div><div>0x220d4.\$typ13: 04EC6BA0FC7D98BA259684F330C28AADCAB91F13</div></div></div>	
C:\Users\user\AppData\Local\Temp\Origin_rawfile.exe	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security		
C:\Users\user\AppData\Local\Temp\Origin_rawfile.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security		
C:\Users\user\AppData\Local\Temp\Origin_rawfile.exe	INDICATOR_SUSPICIOUS_EXE_VaultSchemaGUID	Detects executables referencing Windows vault credential objects. Observed in infostealers	dtexShen	<div><div><div>0x34ad5.\$s1: 2F1A5040A-0641-44CF-8B95-3812D985F2E5</div><div>0x34b47.\$s2: 3CCD5499-87A8-4B10-A215-008888D03B55</div><div>0x34bd1.\$s3: 154E23D0-C644-4E6F-8CE6-5009272F990F</div><div>0x34a63.\$s4: 4BF4C442-9B8A-41A0-B380-DD4A704DDB28</div><div>0x34a6c.\$s5: 77BC862B-F0A8-4E16-4650-9173889F2629</div><div>0x34a3f3.\$s6: E60D7838-91B5-4F09-89C6-2304D4C4C29C</div><div>0x34ad5.\$s7: 3EDE35BE-1B77-43E7-B873-AED901B0275B</div><div>0x34ae5.\$s8: 3CB80FF3-2609-4AA2-ABF8-3F8759A77548</div></div></div>	

File Explorer

Leandro student

Ln 2, Col 25



The YARA Signatures section confirms the detection of **RedLine Stealer**, **Agent Tesla**, and a **credential stealer** through specific rules applied to both **network traffic (PCAP files)** and **dropped executables**. Files like `build.exe` and `Origin_rawfile.exe` were flagged using rules from **Joe Security**, **Sekoia.io**, and **ditekSHen**, which identified known malware traits such as Chrome data theft, user domain access, and references to credential vaults. The matched strings include paths to browsers, encryption keys, and wallet indicators, validating the presence of infostealer malware and revealing its focus on harvesting sensitive user data.

- **Dropped files (if applicable) – Do NOT download the malicious file – Only add screenshots and file name and hash**

Dropped Files				
Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\build.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\build.exe	infostealer_win_redline_strings	Finds Redline samples based on characteristic strings	Sekoia.io	<ul style="list-style-type: none"><li>0x24cc3:\$gen01: ChromeGetRoamingName</li><li>0x24cc8:\$gen02: ChromeGetLocalName</li><li>0x24d2b:\$gen03: get_UserDomainName</li><li>0x28bc4:\$gen04: get_encrypted_key</li><li>0x27d43:\$gen05: browserPaths</li><li>0x27c19:\$gen06: GetBrowsers</li><li>0x27501:\$gen07: get_installedInputLanguages</li><li>0x238cc:\$gen08: BCrypt_Init_Auth_Mode_Info_Version</li><li>0x3018:\$spe1: [AString-ZaString-zid][2String4j].[String8].[twString][2String7]</li><li>0x29006:\$spe7: OFileinfoFileinfo GFileinfoX StabFileinfo</li><li>0x290a4:\$spe8: ApGeneropDaGenerotaRGeneroamGenerongl</li><li>0x296c6:\$spe9: "wallet"</li><li>0x219ea:\$typ02: F413CEA98AA458730567FE47F57CC3C94DDF63C0</li><li>0x211f4:\$typ03: A937C86924706B655555B5E3BD09607F49A2042</li><li>0x21fc1:\$typ04: D6733042BFFC20110BF01BC555555EC76C8F7E2</li><li>0x21968:\$typ07: 77A9683FAF2EC9EC3DABCC09D33C3BD04E8897D00</li><li>0x219c1:\$typ08: A8F6B62160DF085B926D5ED70E2B0F6C96A25280</li><li>0x219c2:\$typ10: 2FB0C611D3D61C142C69071EA8A7D3D10FF6301</li><li>0x219e5:\$typ11: 2A19BFD7333718195216558A896752C51711B02</li><li>0x22044:\$typ13: 04EC8A0FC7D9B8A255684F330C28A4DCAB91F13</li></ul>
C:\Users\user\AppData\Local\Temp\Origin_rawfile.exe	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\Origin_rawfile.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\Origin_rawfile.exe	INDICATOR_SUSPICIOUS_EXE_VaultSchemaGUID	Detects executables referencing Windows vault credential objects. Observed in infostealers	ditekSHen	<ul style="list-style-type: none"><li>0x34ad5:\$s1: 2F1A5504-0641-44CF-8BB5-3612D865F2E5</li><li>0x34b47:\$s2: 3CCD5490-87A8-4B10-A215-00888D03B55</li><li>0x34bd1:\$s3: 154E23D0-C644-4E6F-8CE8-5069272F966F</li><li>0x34bd3:\$s4: 4BF4C442-9B5A-41A0-8330-0D4A704D0628</li><li>0x34bd4:\$s5: 77BC582B-F0A8-4E15-4E8D-61736B6F3829</li><li>0x34bd3f:\$s6: E69D7838-91B5-4FC9-89D5-230D4D4CC2BC</li><li>0x34dd5:\$s7: 3E0E35BE-1B77-43E7-8B73-AED901B6275B</li><li>0x34e05:\$s8: 3C886FF3-2660-4AA2-ABFB-3F6756A77548</li></ul>

This screenshot displays the Dropped Files section, an important part in understanding what potentially malicious components were unpacked or created by the main malware sample during runtime. Repeated by multiple YARA rules as belonging to known malware families, persistent files dropped into the AppData\Local\Temp directory, such as `build.exe` and `Origin_rawfile.exe`, were also tested against these same rules.

In instances of detecting strings relevant to browser data theft, `build.exe` was represented by RedLine Stealer matching rules and was deemed to execute theft of Chrome credentials, domain names, and encryption keys, including crypto wallets.

`Origin_rawfile.exe` was detected to be Agent Tesla and credential stealers, which meant its purpose was to harvest sensitive data like passwords stored in the Windows vault.

These detections by Joe Security, Sekoia.io, and ditekSHen show a modular multi-layer target; the dropped files represent the payload phase of the attack, in which credential theft, persistence, and exfiltration do actual damage. Deleted files are valuable sources of evidence for analyzing malware behavior, threat actor tactics, and possible indicators of compromise (IOCs).

o Networking details (i.e. associated domains or IP addresses)

JoeSandbox Cloud BASIC

OverviewSignaturesProcess TreeDomains / IPsDroppedStaticNetworkStatsBehaviorDisassembly

Download Network PCAP: filtered - full

Domains and IPs

Download Network PCAP: filtered - full

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
xma0.com	51.195.65.154	true	true		unknown
ip-api.com	208.95.112.1	true	false		high
mail.xma0.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
204.10.161.147:7082	true	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

World Map of Contacted IPs

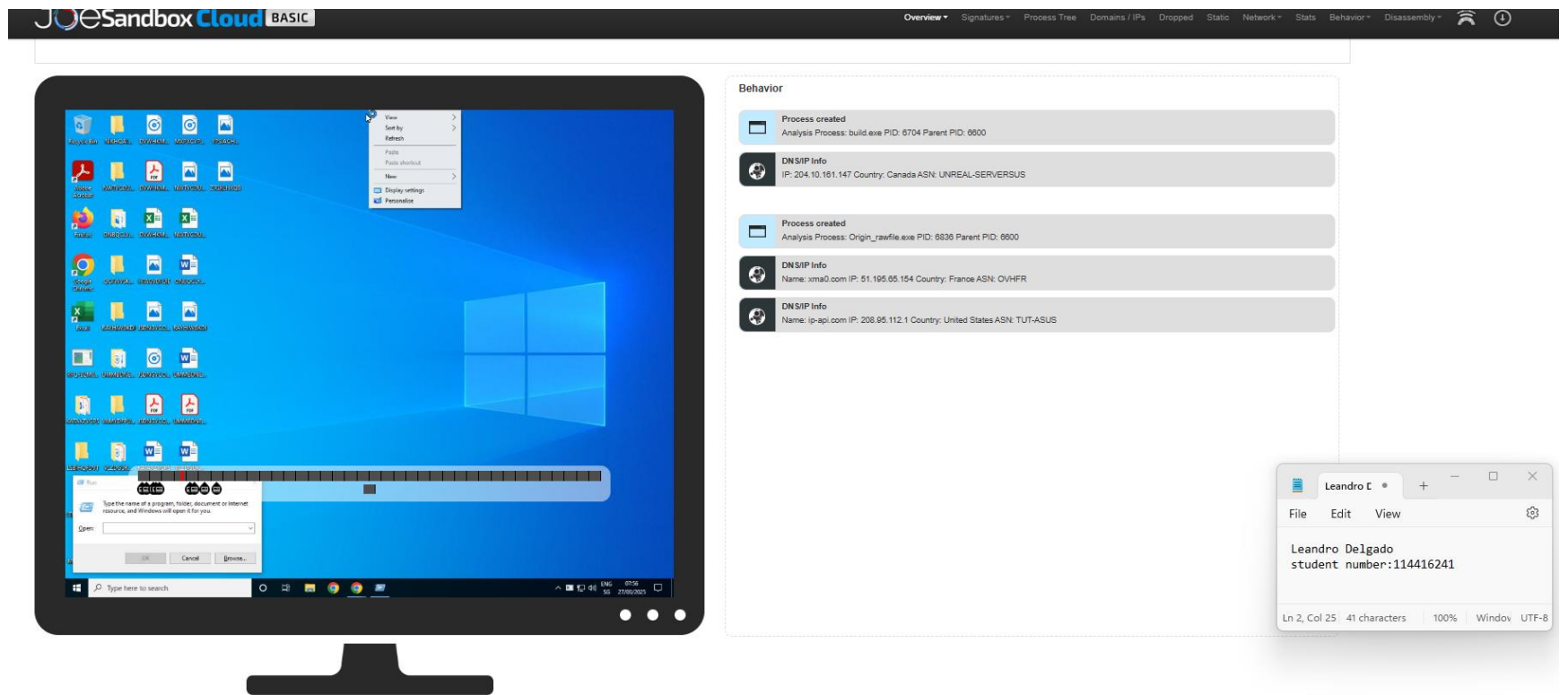
Leandro Delgado  
student number:114416241

Ln 2, Col 25 | 41 characters | 100% | Window | UTF-8

This screenshot shows the **Domains and IPs** section from a malware analysis report in Joe Sandbox Cloud. It reveals that the malware attempted to communicate with multiple domains, including **xma0.com**, **ip-api.com**, and **mail.xma0.com**. Of these, **xma0.com** was flagged as **malicious**, while **ip-api.com** was active but not marked as malicious. One URL, **204.10.161.147:7082**, was contacted and classified as malicious, although Avira's URL cloud rated it as "safe", highlighting potential detection inconsistency. A **world map** at the bottom visualizes the global distribution of contacted IPs, underscoring the malware's outreach and potential command-and-control infrastructure. This section is critical for identifying external connections and possible data exfiltration or control servers used by the malware.

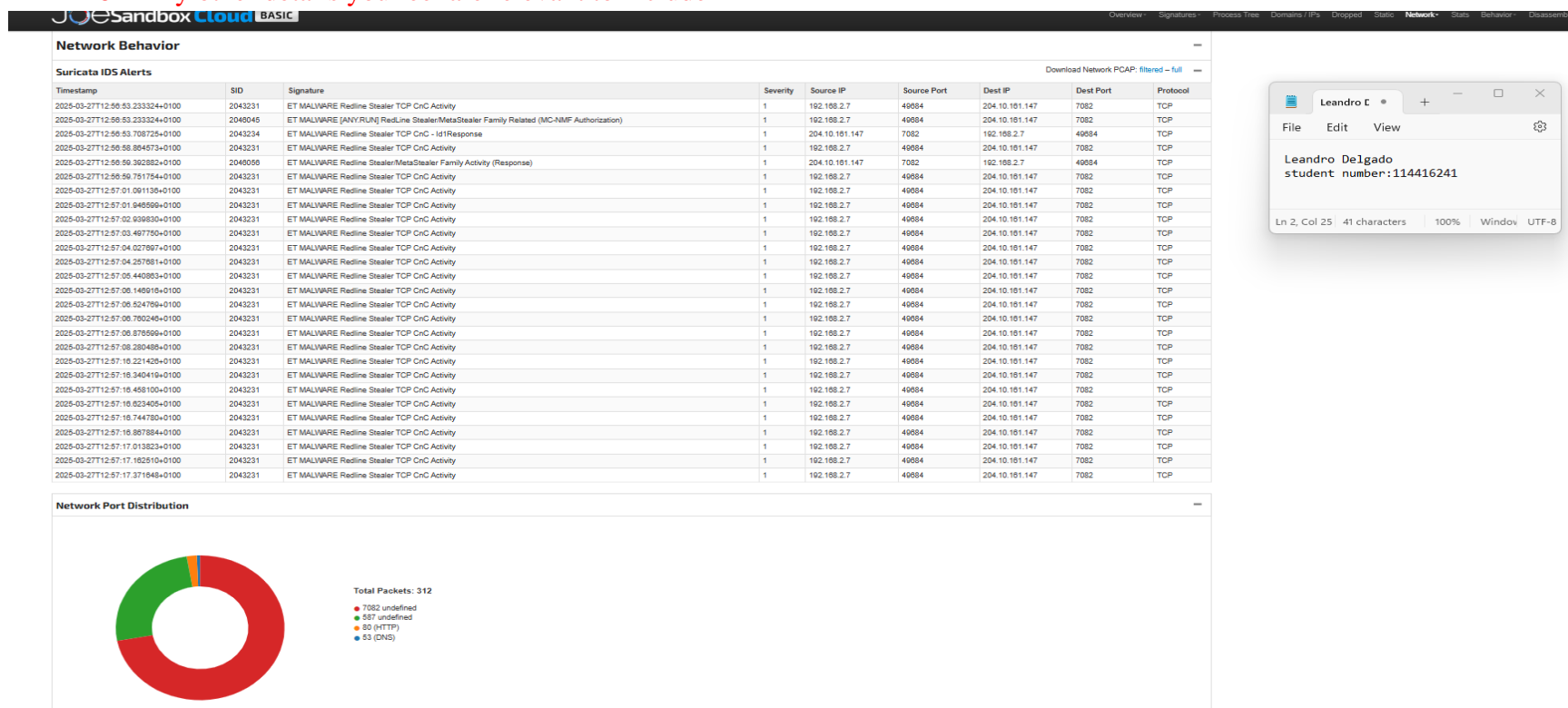


- Screenshots of the malware executing in the sandbox

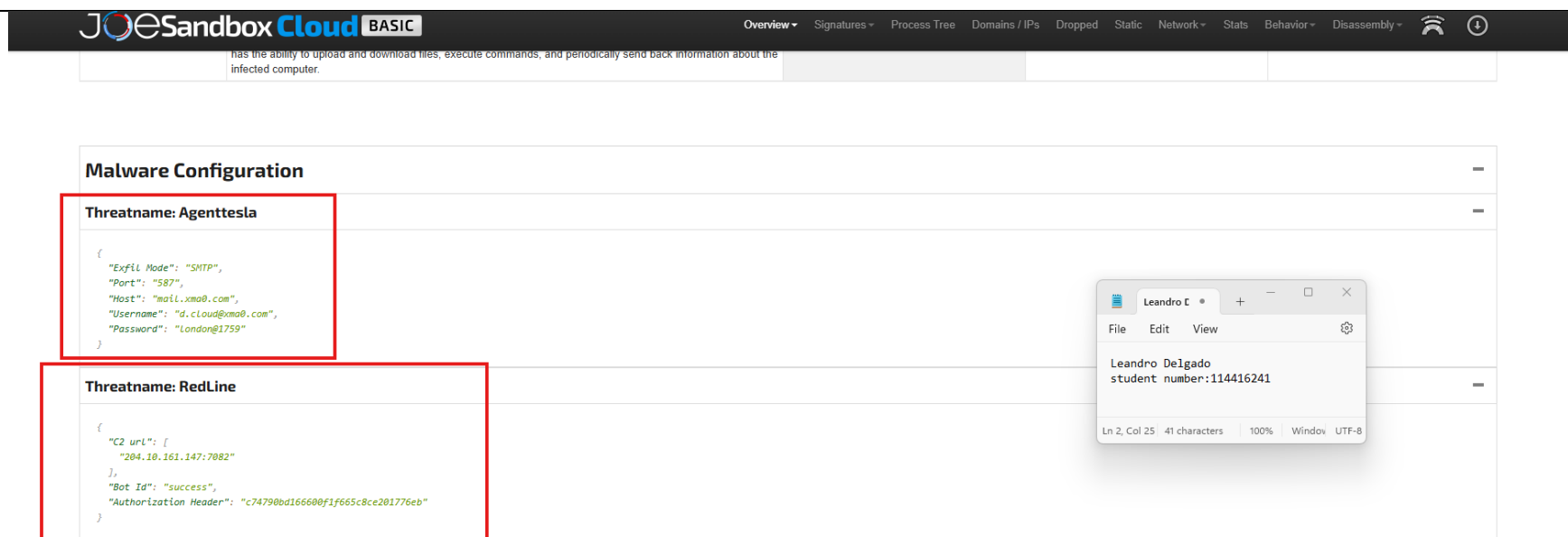


This screenshot shows a behavioral analysis simulation of a malware sample running in a virtual Windows 10 environment using Joe Sandbox Cloud. The desktop displays the execution of the suspicious file, while the behavior log on the right confirms the creation of two processes, `build.exe` and `Origin_rawfile.exe`, indicating payload execution. The malware also contacted several external IPs and domains, including `xma0.com` and `204.10.161.147`, both flagged as malicious, as well as `ip-api.com`, commonly used to collect geolocation and system details. These actions suggest the malware is initiating command-and-control communication and performing victim profiling shortly after execution.

○ Any other details you feel are relevant to include



This screenshot displays the **Network Behavior** section from Joe Sandbox, specifically focusing on **Suricata IDS Alerts**, which monitor suspicious or malicious network activity. The alerts show consistent detection of **RedLine Stealer TCP Command-and-Control (C2) traffic**, targeting the IP address **204.10.161.147** over port **7082**. All alerts originate from the internal IP **192.168.2.7**, indicating the infected machine attempting to communicate externally. The repeated alerts confirm active malware behavior and persistent C2 communication attempts. At the bottom, a **Network Port Distribution** chart provides a visual breakdown of the types of packets observed. Out of **312 total packets**, most were directed to port **7082**, confirming it as the primary channel for RedLine's malicious activity. Smaller portions went to ports **80 (HTTP)** and **53 (DNS)**, which may reflect supporting network behavior like host resolution or legitimate-looking traffic to mask malicious connections.



The screenshot shows the Malware Configuration part of the analysis report, which held other important information on how the malware is programmed to operate. There are two malware families: AgentTesla and RedLine, with respective configurations for each.

In the case of AgentTesla, its exfiltration mode is SMTP, meaning the malware sends compromised information through electronic mail. The malware connects to mail.xma0.com at port 587 using a hardcoded password with the email username d.cloud@xma0.com. Such an approach validates how they weaponize credentials and emails for data theft.

RedLine configuration is fed with C2 URL details pointing to 204.10.161.147:7082. Other headers include "Bot Id": "Success" and unique authorization token. These fields confirm how the attacked machine identifies itself and accesses the infrastructure of the attacker. This section is critical to understanding how it works and to somewhat hard-coded values that allow defenders to create their IOCs for detection and response.

JOE Sandbox Cloud BASIC

Overview
Signatures
Process Tree
Domains / IPs
Dropped
Static
Network
Stats
Behavior
Disassembly

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 28, 2025 02:57:39.404344678 CET	192.168.2.6	1.1.1.1	0xe1e5	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)	false
Mar 28, 2025 02:57:39.148128033 CET	192.168.2.6	1.1.1.1	0x7e46	Standard query (0)	mail.xma0.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 28, 2025 02:57:39.547272621 CET	1.1.1.1	192.168.2.6	0xe1e5	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)	false
Mar 28, 2025 02:57:39.470052004 CET	1.1.1.1	192.168.2.6	0x7e46	No error (0)	mail.xma0.com	xma0.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 28, 2025 02:57:39.470052004 CET	1.1.1.1	192.168.2.6	0x7e46	No error (0)	xma0.com		51.195.65.154	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- ip-api.com

HTTP Packets

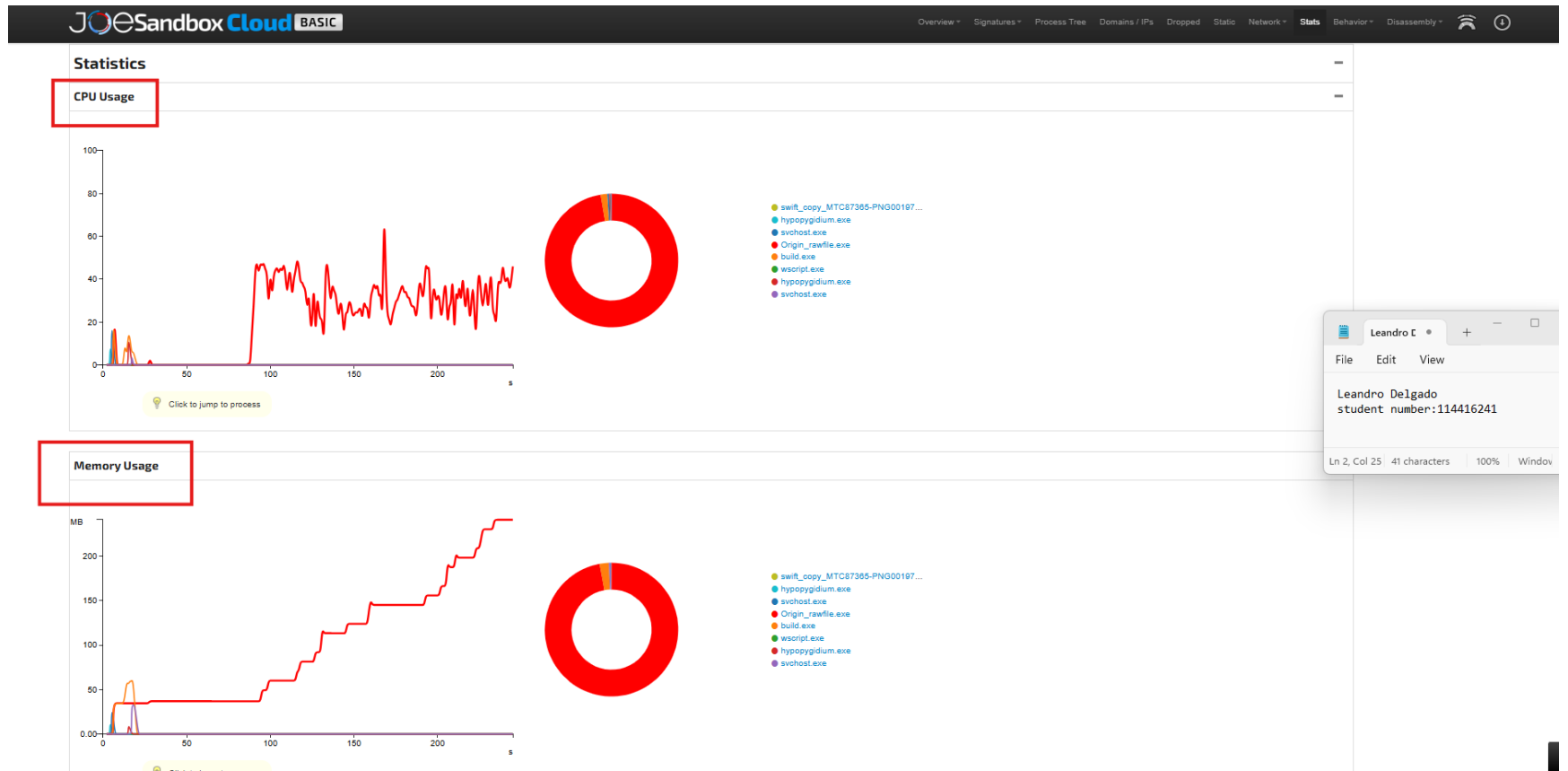
Session ID	Source IP	Source Port	Destination IP	Destination Port	PID	Process
0	192.168.2.6	49505	208.95.112.1	80	7519	C:\Users\User\AppData\Local\Temp\Origin_rawfile.exe

Timestamp	Bytes transferred	Direction	Data
Mar 28, 2025 02:57:39.643387079 CET	80	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: keep-alive
Mar 28, 2025 02:57:39.733124018 CET	175	IN	HTTP/1.1 200 OK Date: Fri, 28 Mar 2025 01:57:36 GMT Content-type: text/plain; charset=utf-8 Content-Length: 6 Access-Control-Allow-Origin: * X-TTL: 60 X-RI: 44 Data Raw: 66 61 6c 73 65 0a Data Ascii: false

This screenshot provides detailed look at the **network-level behavior** of the malware, specifically DNS queries and HTTP communication. The infected host (IP 192.168.2.6) performed DNS lookups for **ip-api.com** and **mail.xma0.com**, both previously linked to malicious activity in this analysis. The DNS answers confirm successful resolution of those domains to **208.95.112.1** and **51.195.65.154** respectively.

In the **HTTP Packets** section, the malware process `Origin_rawfile.exe` is seen making a request to `ip-api.com` using a **GET** method to query system-level information, specifically requesting the `hosting` field. The HTTP response confirms communication with a **200 OK** status and a small data payload. This behavior shows the malware actively gathering system environment information, a typical step during profiling or pre-exfiltration stages.

This network trace highlights the malware's use of standard DNS and HTTP protocols (not encrypted), which makes it easier to detect in unsecured environments and shows its attempt to blend in with normal traffic while communicating with its command infrastructure.



	<p>This screenshot presents the <b>system resource usage statistics</b> recorded during the malware analysis in Joe Sandbox. It includes two main charts: <b>CPU Usage</b> and <b>Memory Usage</b>, each showing a timeline and corresponding donut charts for visual distribution among processes.</p> <p>In the <b>CPU Usage</b> section, the red line represents the activity of <code>build.exe</code>, which is responsible for a sustained and fluctuating load on the system, often hovering between 20% and 50%. This high CPU consumption indicates that the process was actively performing background tasks, likely related to malware behavior such as data collection, encryption, or communication.</p> <p>The <b>Memory Usage</b> chart shows a steady and continuous increase in memory consumption by the same <code>build.exe</code> process. The red line sharply climbs over time, exceeding 200MB of RAM usage, which further confirms ongoing malicious operations such as loading modules, storing stolen data in memory, or interacting with other components. The donut charts reinforce that <b>build.exe dominated both CPU and memory resources</b>, highlighting it as the core payload responsible for executing the main malicious routines. This behavior is typical of advanced info-stealers or malware with persistence and active exfiltration logic.</p> <p>Summary</p> <p>This malware analysis produced many key lessons. First, it highlighted a modular approach to modern threats like RedLine and AgentTesla, which work in stages to execute payloads, steal data, and maintain persistence. The bad actors even hardcode SMTP credentials and C2 URLs into their malware configuration; this is an indication that attackers would include critical bits of infrastructure directly into their code so that they could be easily extracted as indicators of compromise. Behavioural analysis became paramount; for instance, the spikes in CPU and Memory on <code>build.exe</code> were clear indicators of active malicious activities beyond what would have been otherwise evident by static detection methods. After this, DNS queries and HTTP traffic showed further proof of these profiling services and malicious domain contacts. Suricata IDS with alerts gave hard facts about the command-and-control communication assumption further strengthening the call for strong network monitoring. All these clearly indicate the concerted need for static, dynamic, and network approaches to better understand and to defend against sophisticated malware.</p>
Students reports	<ul style="list-style-type: none"> <li>• Submit your report that contains your analysis.</li> <li>• Your report should include the relevant <b>screenshots</b> of your analysis.</li> <li>• Write a paragraph or more about your personal learning experience.</li> </ul>
Grading= 8 Marks	<ul style="list-style-type: none"> <li>• 1 Mark/Analysis and learning experience</li> </ul>