**Malware Analysis Project**

In this project, you will research a specific malware and create report and presentation that covers the following:

- Overview of the Threat

- Technical Expose

- Containment Strategy

- Awareness Training

\*\*Important Due Dates\*\*:

- Projects will be presented in-class on the third day.

- Written reports will be handed in at the end of the following week.

## Malware Analysis

In this project, you and your group will analyze the behavior of a live malware sample running on the Any.Run executable analysis platform.

Access the analyses at the URLs below:

[Adylkuzz]

<https://app.any.run/tasks/79528004-1cb3-4b6e-9c3d-24acd7ea6812>

- [Grand Crab]

<https://app.any.run/tasks/aa782534-ed7f-4879-9998-00c8c18aca29>

[Cryptominer]

<https://app.any.run/tasks/eda9d4a5-9117-4b06-8d2b-7618305c7d26>

-[NotPetya]

<https://app.any.run/tasks/e6357893-f5c8-4301-b82f-7832c9862b53>

- [Satan]

<https://app.any.run/tasks/7557f2f9-62b6-4d7c-858d-c09a4ce90650>

Analyzing Malware with Any.Run

The Any.Run interface is pleasantly intuitive but contains quite a lot of information. In the walkthrough below, you'll learn where all of it lives.

In the Main UI you're first presented with, note the following four panes:

- The top-left contains a view of the VM's desktop, which can be useful for collecting screenshots for your report.

- The bottom-left presents a \*\*Details\*\* pane.

- The top-right contains metadata about the malware.

- The bottom-right contains detailed information about the VM's \*\*Process Environment.\*\*

Refer to the below for additional details on the latter three panes.

Metadata

In the Metadata pane, note the following important buttons:

- \*\*Info\*\* (top-right): Provides information about the file format; hash signatures; required libraries; etc.

- These are important details for hardcore malware analysts, but they're out of scope for this project.

-\*\*Sample\*\*: Downloads a ZIP containing the malware.

- The ZIP is protected by the password: `infected`

- \*\*IOC\*\*: Summarizes TCP connections; DNS requests; and HTTP requests.

- \*\*Text Report\*\*: Contains file information similar to that provided by the Info button.

- \*\*ATT&CK Matrix\*\*: Identifies suspicious activity signatures detected by Any.Run; explains why each signature is significant; and specifies exactly what triggered the alert.

- This is a \*\*VERY USEFUL\*\* pane to refer to.

Details Pane

The bottom-left presents a \*\*Details\*\* pane. Note the four columns it includes:

- \*\*HTTP Requests\*\*: All HTTP requests made by any process running on the VM.

- \*\*Connections\*\*: All connections to/from the VM.

- \*\*DNS Requests\*\*: All DNS requests made by processes running on the VM.

- \*\*Threats\*\*: Any known threats identified by Any.Run.

- Note the three icons on the far left:

- \*\*Network\*\* (top icon) loads the information about HTTP Requests, Connnections, DNS Requests, and Threats that you've already seen.

- \*\*Files\*\* (middle icon) load information on any files changed by processes running on the VM.

- \*\*Debug\*\* (bottom icon) loads Debug Output, which loads information about errors in running processes.

Process Environment

The \*\*Process Environment\*\* pane in the bottom-right contains a list of all processes running on the VM.

On the left half of the UI, note the following:

- Click on a running process and note the \*\*Process Details\*\* pane that appears.

- Click on \*\*More Info\*\* in the Process Details pane.

- Note the following in the resulting UI:

- The top-left presents the name of the process; its location on the VM's filesystem; when it was created/terminated; and any references to any child processes it launched.

- The \*\*Download\*\* button allows you to download the malware in a ZIP file.

- The \*\*Look Up on VT\*\* button opens the results of analyzing the Malware with Virus Total.

- When you click this link, note the following tabs presented by Virus Total:

- \*\*Analysis\*\*: Displays how different Anti-Virus identify the malware.

- \*\*File Detail\*\*: Contains static analysis results about the executable's file format, metadata, etc.

- \*\*Relationships\*\*: Provides information about related files in the Virus Total database.

- \*\*Additional Information\*\*: Presents information such as the file type; hash digests; etc.

- \*\*Comments\*\*: Community commentary on the sample.

- \*\*Votes\*\*: Community votes as to "how malicious" the sample is, on a scale from -100 to +100.

- \*\*Behavioral Information\*\*: Summarizes details such as which files the sample opened/read/wrote; which child processes it launched; whether it made HTTP or DNS requests, or opened other TCP or UDP connections; etc.

- For this project, focus on \*\*Behavioral Information\*\* and \*\*Analysis\*\*.

- Below the \*\*Look up on VT\*\* link, note the \*\*Command Line\*\* field.

- This contains the command run by the VM to launch the process.

- Below the \*\*Command Line\*\* field (bottom-left), note the \*\*Indicators of Suspicious Behavior\*\* pane.

- This summarizes data any suspicious actions the process performs, such as communicating with a foreign host on the network; modifying the filesystem; updating the registry; etc.

On the right half of the UI, note the following columns:

- \*\*Modified Files\*\*: Details on any files changed by the process.

- \*\*Registry Changes\*\*: Registry entries made/altered by the process.

- \*\*HTTP Requests\*\*: HTTP requests made by the process, including the target URL; request method; the reputation of the target server; and the country in which that server is located.

- \*\*Connections\*\*: Details of any TCP/UDP connections opened by the process.

- Note that you can click the \*\*Show Network Stream\*\* link in the bottom-right of any entry in the Connections column to see the raw data sent over the connection.

Click the arrow button to the right of \*\*Connections\*\*, and note the following three columns:

- \*\*Network Threats\*\*: If the process's network activity exhibits any known threat signatures, they'll be documented here.

- \*\*Modules\*\*: Lists all system libraries loaded by the process.

- \*\*Debug\*\*: In the event the process fails to execute successfully, this column will contain debug information produced by the OS.

Click the `X` in the top-right corner to return to the main UI.

Writing the Report

Your report must meet the following \*\*requirements\*\*:

- At least 4-5 pages, double-spaced.

- Include at least one diagram.

- Report should cover the same theme as your presentation.

- Include works cited at the end of the report.

Writing the Overview of the Threat

In this section, you will research, source and cite relevant articles and materials. Then, you will answer the required questions.

Writing the Technical Expose Section

Use the [Technical Expose Template]

https://docs.google.com/document/d/1-V77cM1akgVRu5JXuUJZXklKcQayxgSipkUeW\_XRfF0/edit) to guide you with this section of the report

- Click \*\*File\*\*, then \*\*Make Copy\*\*. Select \*\*Yes\*\* when prompted to copy comments and suggestions.

Writing the Containment Strategy and Awareness Training Sections:

Use the [Containment Strategy and Awareness Training Template]

https://docs.google.com/document/d/1mX3p3fo1lDUilX3w3g1Xuqw2Bq\_BVyNRm3x89wlmSH0/edit) to guide you with these sections of the report

- Click \*\*File\*\*, then \*\*Make Copy\*\*. Select \*\*Yes\*\* when prompted to copy comments and suggestions.

Creating the Presentation

Your presentation must meet the following requirements:

- Presentations will be given in-class, on the third day of the Malware Analysis Unit.

- Presentations will last 10-12 minutes each.

- Each person in the group must contribute in presenting the project. (Each person should speak for at least 2 minutes each.)

- Be prepared to answer follow-up questions.

Keep in mind the following criteria and tips when creating your presentation:

- Focus on developing clean slides with technical accuracy and depth

- Be as engaging as possible. (This presentation is an opportunity to practice your oral communication skills.)

- Consider what in your 4-5-page report is most relevant to include in your 10-12-minute presentation.

RESOURCES

*Example Reports:*

<https://www.us-cert.gov/ncas/analysis-reports/AR18-221A>

<https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/>

<https://www.sentinelone.com/blog/trickbot-technical-analysis-banking-trojan-malware/>

<https://www.vmray.com/cyber-security-blog/vmray-malware-analysis-report-recap-october-17/>

<https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf>

<https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf>

*Research URLs:*

<https://app.any.run/submissions/>

<https://www.vicheck.ca/hashquery.php>

[https://mxtoolbox.com](https://mxtoolbox.com/)