Abstract

Malware reverse engineering is an undisputed element of cyber security incident management as it strongly supports detection and response activities. Building and maintaining this capability in-house is challenging in many aspects. This whitepaper provides an overview of how malware reverse engineering as a service offers a solution for this problem.

Problem Statement

Have you ever

- received a question from your users if they can open a specific file that was marked by an email gateway as suspicious although a trusted party sent it, or
- received an alert that a file was blocked as malicious with the confidence rate at 61%, or
- been provided with a multipage malware sandbox report suggesting that a file is a generic malware

and it was your responsibility to decide on the next steps?

Background

Analysis of suspicious code is inevitable at some point in the life of all cyber security teams. Numerous technologies, operating at network and endpoint levels, aid cyber security professionals in performing automated runtime analysis of code to conclude whether the code is benign or malicious.

The issue is caused by a potentially inaccurate verdict or the need to reveal why that decision was made:

- The new generation of malware use highly evasive techniques to bypass automated malware analysis tools; therefore, verification of the verdict might be necessary.
- Legitimate programs might act suspiciously, so understanding the reasons that led to the decision can be essential before overriding it.
- Investigation of malware incidents does not stop at blocking malicious code. Understanding what the code does, enables effective response to the incident, including identifying which assets are impacted and how.

When automated analysis tools have fulfilled their tasks and questions regarding a suspicious file are still open, getting the answers requires in-depth malware analysis. So skilled malware reverse engineers need to take over and drive the analysis for adequate results.

Establishing in-house malware analysis capability is difficult to reach as truly skilled malware reverse engineers are hard to be recruited and retained.

Solution

Malware Reverse Engineering as a Service takes off such burden via providing the malware analysis capability on demand.

Subscuto's Malware Reverse Engineering service offers the human analysis of malware built on decades of experience at high capacity powered by Subscuto's automation-aided triaging pipeline in a purpose-built environment.

Some of the technical advantages:

- the service ensures that there is no need to upload the samples to any public environment; the analysis is performed in a private, purpose-built system,
- as the analysis is completed on real hardware with manual supervision, malware evasion techniques become useless, and
- specific evasion techniques cannot be developed against it, unlike in the case of automated sandbox solutions.

The suggested relevant use cases of malware reverse engineering service include, however not limited to:

- tactical malware analysis to support the response part of incident management,
- analysis of suspicious files, for example, email attachments to increase the accuracy of the detection phase of incident management,
- any other cases when deeper understanding is required on the behavior of a computer code.

Contact

Don't hesitate to contact Péter Szilágyi at peter.szilagyi@subscuto.com for further information on the service, including free trials and technical deep dive.