INTEZER

Leading Telecom Company Implements Genetic Malware Analysis to Accelerate its Incident Response Time

Case Study

Case Study
Case Study

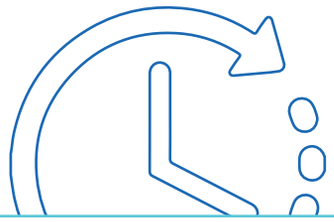
About the company

A leading Israeli cellular provider, providing millions of subscribers with a broad range of services including cellular telephony, roaming services, text and multimedia messaging, advanced cellular content and data services, and other value added services in the areas of music, video and mobile office.

This case study will demonstrate how Genetic Malware Analysis technology, Intezer Analyze, is implemented to enable the telecom company's incident response (IR) team to optimize processes, accelerate time to response, and adopt a proactive approach to threat hunting.

INTEZER

THE CHALLENGE
Shorten Time to Response



This enterprise has been the target of hacktivist groups and nation state sponsored cyber attacks for many years. Albeit endlessly investing in security solutions, its incident response (IR) team was spending a large amount of time and resources on investigation processes, and the time from detection to response remained too long. Shortening the time from detection of malicious files to response was a high priority for the enterprise, in order to lower the risk of attacks residing in the network.

Using IDA (Interactive Disassembler) and manually reverse engineering malware, the telecom's IR team was able to uncover the malware's components and data, yet the process was extremely time-consuming and still did not provide complete context into the malware. Critical information such as where the malware originated from, the attack group behind the file's development, and whether or not the file was a new variant of a known malware, remained uncertain.

The IR team was searching for an automated solution that would substantially shorten the time to response and gain insightful context about suspicious files.

They chose Intezer Analyze to:

- Obtain quick and accurate malware analysis
- Uncover variants of discovered malware in the network
- Reduce false positives by identifying code reuse in suspicious files
- Perform rapid memory analysis

The Challenge	The time from detection to response is too long due to complex investigation and reverse engineering processes.
The Solution	Instantly investigate and classify all alerts and accelerate the time to response. Immunize the organization with code-based vaccines, identifying code reuse in malware.
The Outcome	Reduce the number of false positives and shorten the incident response time from hours to minutes. Take a proactive approach to threat hunting by enabling automatic YARA generation.

THE SOLUTION

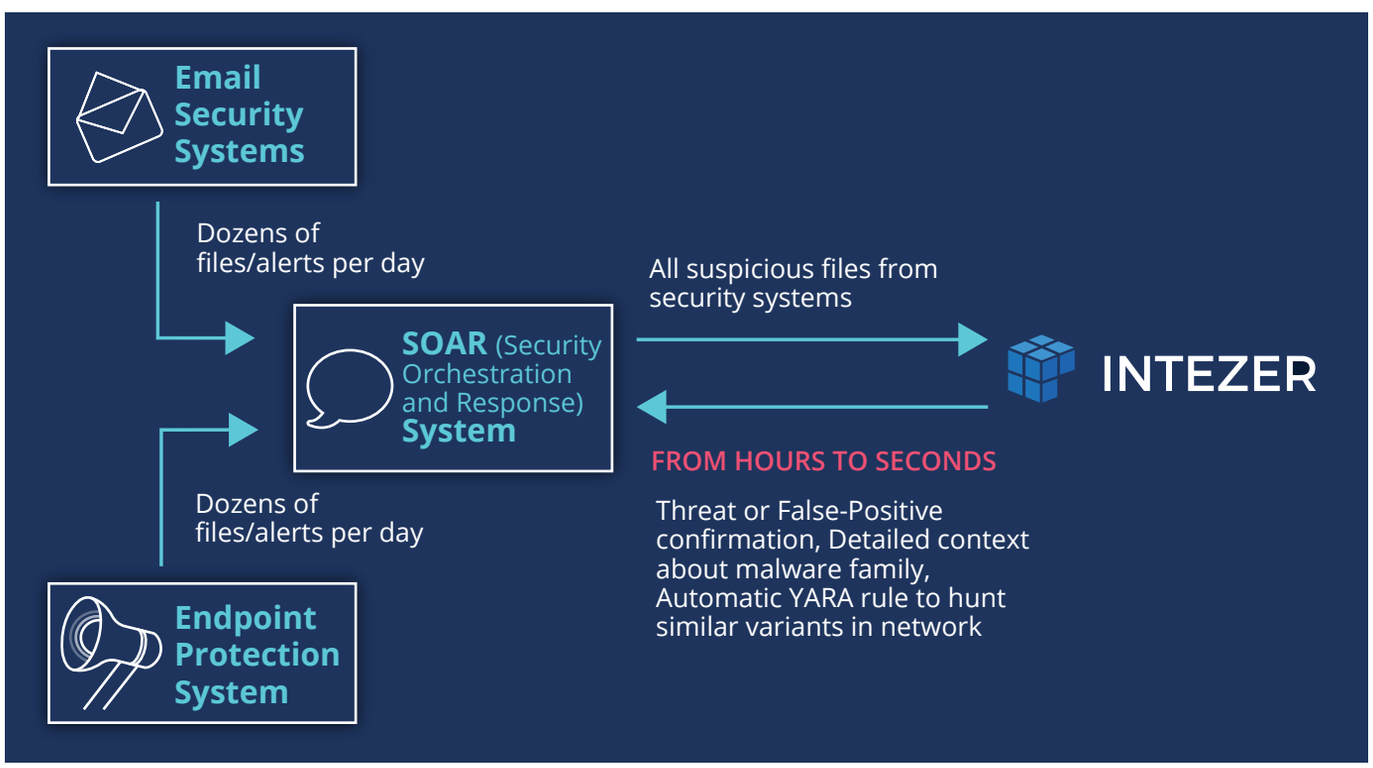
Genetic Malware Analysis

Intezer Analyze was deployed, integrating with manual and automated IR processes, in addition to seamlessly integrating with the enterprise's existing SOAR (Security Orchestration and Response) system.
The main process in the day-to-day security operations is to investigate alerts raised by existing security systems, such as e-mail and endpoint security solutions. Intezer is integrated with the enterprise's SOAR solution, to fully automate the alert investigation process and deliver the IR team the context needed to assess a suspicious file, and efficiently respond to an incident. This automated process enables the IR team to accurately identify threats, classify them according to severity, and provide deep insights into every single alert.

In addition, Intezer Analyze enables the cybersecurity team to perform memory analysis of an endpoint to uncover hidden in-memory attacks and respond in a timely manner.

With Intezer's Genetic Malware Analysis technology, the security team can also demonstrate a proactive approach to threat hunting. Having the ability to create vaccines (in YARA format), enables the IR team to actively look for similar variants of threats, instead of waiting to respond to incidents.

> Intezer's one-of-a kind malware analysis technology based on code reuse detection is exactly what our IR teams needed. Obtaining deep insights into every suspicious file in seconds saves precious time and efforts, enabling the team to focus on prioritizing and remediating attacks.
>
> CISO

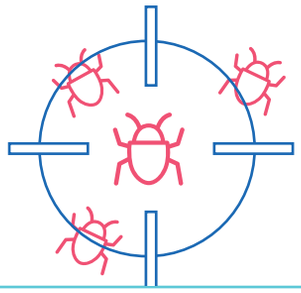


INTEZER

Case Study
Case Study
Case Study

THE OUTCOME

Accelerated Response and Proactive Threat Hunting



The immediate benefit experienced by the telecom company from implementing Intezer Analyze was saving time and resources. They now had the ability to simultaneously validate threats from multiple sources and substantially reduce the number of false positives, enabling the incident response team to focus on prioritizing and remediating attacks.

The automated reverse engineering and delivery of deep insights on suspicious files within seconds, as opposed to hours or even several days, on investigation processes, freed up precious analysts' time as well as in many cases, pointed them in directions they were blind to before, enabling them to hunt threats before they become attacks.
In addition, code-based vaccines are deployed to ensure the enterprise's resilience to future and unknown threats, as malware creators reuse code or create variants of previously written code.

Following the implementation of Intezer Analyze, the IR team reports that in over 90 percent of its cases, processes and memory modules receive concrete and precise information about their nature, whether they share code with trusted software and can be filtered, or share code with a known malware family and are detected and classified accordingly.

SEE IT IN ACTION

Investigate Results within Seconds

The cellular provider became aware of a fraudulent email sent to customers, designed as a legitimate email. The email contained a PDF file attachment that once opened, runs a malware in the background. The IR team uploaded the suspicious file to Intezer Analyze and within seconds identified the file as malicious. The file was a bitcoin miner running on the victims' computers.
Although the attack was not targeting the company's network, it was attacking its customers, and the team was able to quickly and easily remediate it, based on the instant Genetic Malware Analysis and deep insights provided by Intezer Analyze.

About Intezer

Intezer introduces a Genetic Malware Analysis approach, offering enterprises unparalleled and accelerated incident response.
Intezer provides a fast, in-depth understanding of any file by mapping its code DNA at the 'gene' level - offering the most advanced level of malware analysis. By identifying the origins of every piece of code, Intezer is able to detect code reuse from known malware, as well as code that was seen in trusted applications.

www.intezer.com