INTEZER

Orange Cyberdefense

Case Study

Orange Cyberdefense accelerates malware analysis with Intezer Analyze

About Orange Cyberdefense

Orange Cyberdefense is Europe's leading go-to security services provider, supporting businesses globally. The company's 2,500 cybersecurity experts work together to provide a wide array of cybersecurity services including targeted threat intelligence, auditing & penetration testing, red & purple teaming, managed threat detection and response, and incident response & cyber resilience digital forensics. With a success rate of identifying 90% of threats before they have any business impact, Orange Cyberdefense proudly serves and protects clients worldwide including high-tech startups, SMBs, financial institutions and cosmetics giants.

The Orange Cyberdefense team of **forensics investigators** and **incident responders** are the first responders when a client is under attack. Serving clients from all sectors and of all sizes, from startups to enterprise giants, the team is called to contain, mitigate and document different types of threats, on a daily basis.

The Orange Cyberdefense **Forensics and Incident Response team** was looking for ways to accelerate the **malware analysis** process and selected **Intezer Analyze**.

Intezer Analyze detects threats with **automated malware analysis**, recognizing even the slightest amount of code reuse, enabling it to identify the malware's functionalities, quickly contain the risk and speed up remediation.

The team initially used the free version and later upgraded to the full service.

Challenges

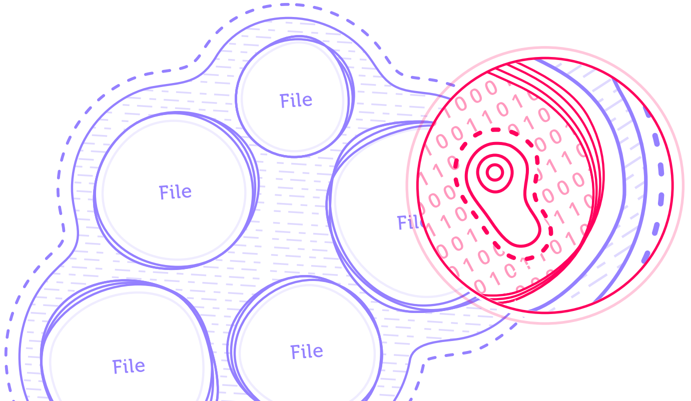
- Malware analysis and reverse engineering are performed manually
- The process is too lengthy and delays mitigation

Solution

- Classify malware in seconds
- Find related samples based on code reuse
- Accelerate memory forensics
- Proactive threat hunting

Benefits

- Optimize analyst/investigator's time and resources
- Get malware functionalities in seconds
- Leverage existing CTI to solve incidents and speed response



Cut Malware Analysis Time from Hours to Seconds

The malware analysis process begins with the identification of the malicious or suspicious file with executable code that the attacker dropped on a compromised system. You may know the file is malicious, but you might not always know what it can do, who is behind it, or what kind of damage it can lead to.

Intezer Analyze provides information about the **malware within 20 seconds**. Using **genetic analysis** and **code similarities to detect malware**, it replaces the manual analysis and reverse engineering processes that can take several hours.

In addition, Intezer Analyze includes an IDA plugin, which enables reverse engineers to accelerate their investigations when they want to run an in-depth analysis of the malware.

✓ Success Story – Automated Malware Analysis Leads to Faster Mitigation

The team was responding to an attack that was classified as **Trojan.Generic** by other solutions. Intezer Analyze provided the binary analysis within seconds, with real evidence and input about the malware, classifying it as **IcedID**. From this analysis the team understood they were dealing with a remote access tool that can dump passwords, and use C&C over https, and were able to prepare for mitigation accurately and at speed. This has also happened with **Qakbot**, another banking Trojan.

> “Intezer Analyze contributes to our incident response and forensics investigations daily. Knowing what we are dealing with in the middle of an attack, in less than 30 seconds, directly impacts our clients’ risk mitigation and recovery time.”
>
> **Robinson Delaugerre,**
> Head of Forensics and Incident Response team

Instead of giving the malware to a reverse engineer, which would take 1-2 hours and delay the investigation and response, Orange Cyberdefense is provided with the answer in seconds.

When other tools classify malware as malicious but provide no additional information about it, Intezer Analyze provides input on what the malware is designed to do, what malware family it belongs to and more. In addition, Intezer Analyze identifies malware that bypasses detection tools, for example, malware that is written in the Golang programming language.

✓ Success story – Threat Intelligence Collaboration Accelerates Malware Identification

Responding to a client's incident, the investigators submitted a malware sample analyzed by Intezer, to the Orange Cyberdefense threat intelligence repository, where they saw a similar sample submitted two days earlier from a different incident with another client. Collaboration between the investigators enabled them to combine what they knew about **IoCs** and **IP addresses**, revealing links between the incidents, which led to the conclusion that they were analyzing two variants of the same malware deployed by the same threat actor on two different victims. Thanks to **Intezer Analyze**, the Orange Cyberdefense team was able to correlate two separate incidents at two different customers. This threat intelligence-based collaboration resulted in faster threat hunting, containment and mitigation of both incidents.

Intezer Analyze gives Orange Cyberdefense one platform for their malware analysis needs, enabling them to ensure 24/7 incident response and forensics investigation services to their clients globally.