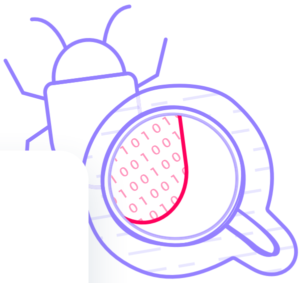
INTEZER ANALYZE

Case Study

iSECURITY
A Calian Company

Managed Security Service Provider (MSSP)



Chris Stewart, Director of Security Operations

Chris leads the security operations center (SOC), helping iSecurity's customers investigate and deal with incidents, from malicious hacking tools like Cobalt Strike to ransomware attacks.

iSecurity delivers a complete lifecycle of digital protection services across the globe for public and private sector clients. Through managed security operations capabilities, they engage with organizations to assess exposures to cyber attacks, build robust security programs and provide advanced threat monitoring and detection.

Accelerate Memory Analysis

Intezer Analyze Endpoint Scanner is quick and easy to run. Even when I'm offsite, like during a recent incident at a hospital, I was able to have the customer's junior, non-technical employees cover a couple of hundred workstations because using the scanner is a very straightforward process.

What appeals to me most is the ease of use and efficiency from a time standpoint. For me to manually dump malware and do malware analysis on memory, which is normally very time consuming, is invaluable. Having a tool that we can deploy at scale and get results in five minutes helps us narrow down the scope of the investigation.

One of the main challenges of incident response is finding that initial attack vector and getting those clues quickly to identify Patient Zero. Intezer Analyze lets us know of an infection and narrows down which machines need to be investigated further."

"The main feature of Intezer Analyze Endpoint Scanner is the efficiency of it. It's an executable file (.exe) which makes it easy to deploy, and it's easy to get results via an API. It's quick, traditionally taking between five and 10 minutes, and it's simple to use. IT individuals onsite can go around to nurses' workstations and other machines throughout the hospital, running the product and following a standard set of instructions. Which speaks volumes to how easy it is to use the tool and to get results. Then, we on the security analyst team can review those results and pinpoint key workstations that need to be investigated."

Identified Ryuk Ransomware

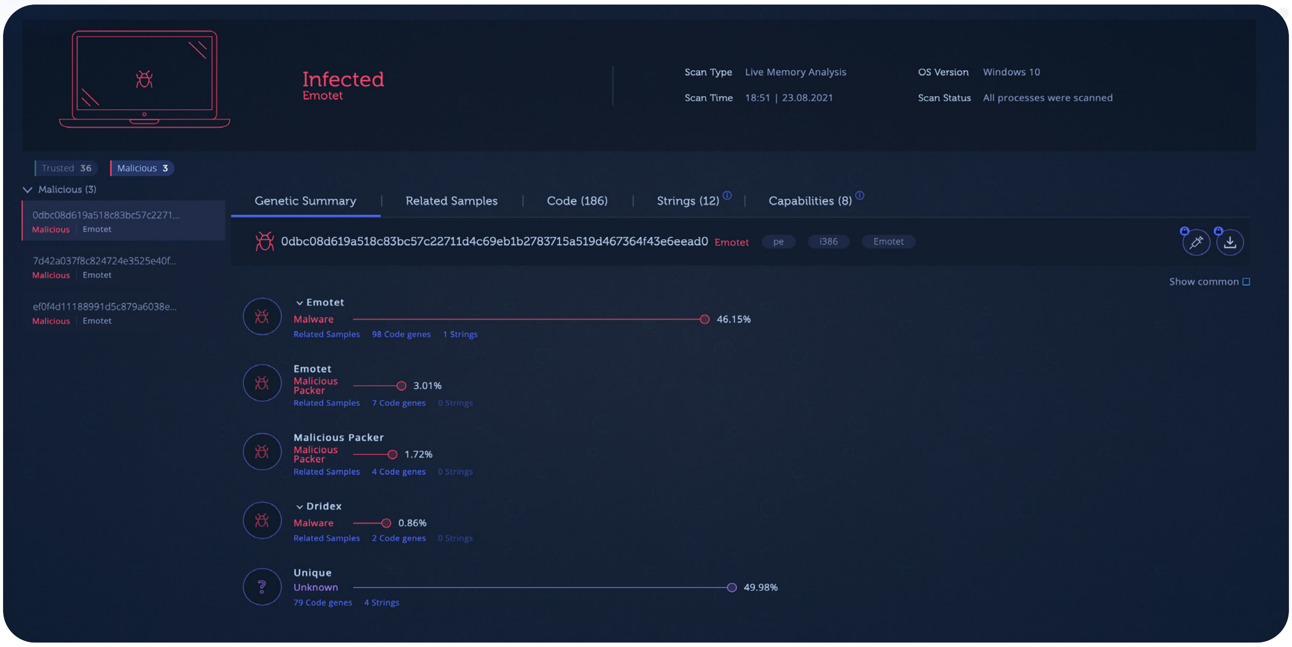
"We have used endpoint analysis in a number of cases to confirm ransomware attacks, including in response to a major Ryuk ransomware attack against a customer in the United States. In the most recent incident, Intezer notified us of Nefilim ransomware. Intezer Analyze helped us pinpoint the first point of infection by finding Cobalt Strike and various other hacking tools on the server which we previously suspected were there. It's nice having a tool to confirm those initial speculations.

Intezer kickstarts our investigations by pointing us in the right direction and narrowing down the scope of the investigation. It's also an efficient way to get IoCs to the customer. If we didn't have the tool in the most recent incident, through firewall log analysis we could pinpoint a few workstations or servers in question. Traditionally, that would have to go through an investigation process where we get the images and investigate each of the workstations.

Typically, that means we're going to have results in a couple of days. Being able to run Intezer Analyze allows us to speed up this investigation process to get immediate initial results. It may not map the entire timeline of the attack but what it does do is give us a very solid foundation to start mapping a timeline and mapping it back to the MITRE ATT&CK® framework."

> **Having a tool that dumps and catches everything that's running in memory is efficient and saves us time."**

Validates our SOC Findings



Infected
Emotet

Scan Type Live Memory Analysis
Scan Time 18:51 | 23.08.2021
OS Version Windows 10
Scan Status All processes were scanned

Trusted 36 Malicious 3

Malicious (3)

0dbc08d619a518c83bc57c2271...
Malicious | Emotet

7d42a037f8c824724e3525e40f...
Malicious | Emotet

ef0f4d11188991d5c879a6038e...
Malicious | Emotet

0dbc08d619a518c83bc57c22711d4c69eb1b2783715a519d467364f43e6eead0 Emotet pe i386 Emotet

Emotet
Malware 46.15%
Related Samples 98 Code genes 1 Strings

Emotet
Malicious Packer 3.01%
Related Samples 7 Code genes 0 Strings

Malicious Packer
Malicious Packer 1.72%
Related Samples 4 Code genes 0 Strings

Dridex
Malware 0.86%
Related Samples 2 Code genes 0 Strings

Unique
Unknown 49.98%
79 Code genes 4 Strings

"We use Intezer Analyze to double check our SOC findings. For example, we sometimes spot a malicious PDF or payload that wasn't blocked by the endpoint. In this case, we provide Intezer Analyze Endpoint Scanner to the customer, they run it, and it gives us a holistic view of what's running on the workstation; validating if the machine is infected or not and if we need to take further action.

We are faced with so many incidents it's hard to keep track of them all. In one recent incident, there were 3 or 4 servers or workstations in question. We ran Intezer Analyze on them for initial findings. It found an njRAT backdoor, Cobalt Strike kit and a whole set of hacking tools present on the machine. It really helped kickstart the investigation, seeing the level of infection from that host."

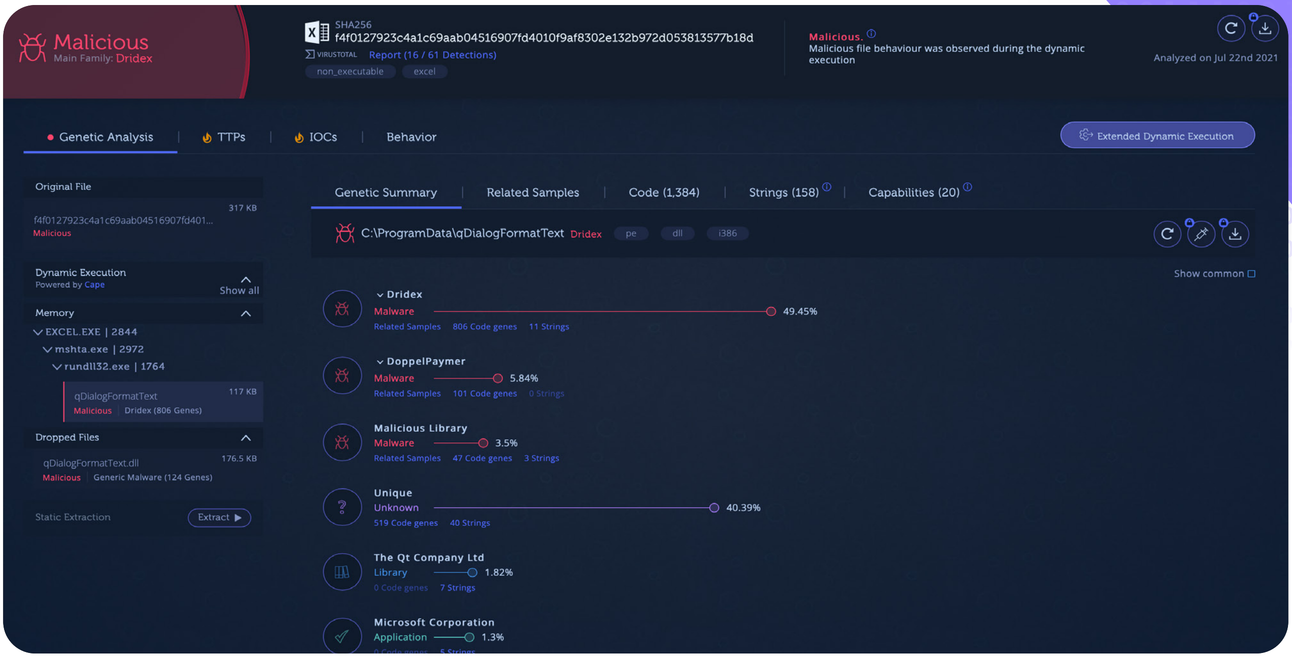
Extract IoCs Automatically

“One of the challenges of incident response is getting the customer’s IoCs from their current ransomware incident. How do we get the customer back online, efficiently, without reinfecting themselves? We need to establish the IoCs in question for the current investigation.

In this case, we were able to run Intezer Analyze, see the backdoor, the loaded Cobalt Strike payload, and the connection to the C2 server. Within 24 hours, we have a short list of IoCs that we can add to the firewall and our endpoint solutions, and start to go down the path of making sure the infection doesn’t spread any further. When we bring resources online to bring the customers back online we have a solid set of IoCs to protect them should anything be missed from a scanning and cleanliness backup restore process.”

File Analysis

“Intezer Analyze gives us fast and accurate analysis results for malicious PDFs and files encountered by our customers. Easy-to-understand reports provide malware classification, TTPs, IoCs, related samples and more. Intezer tells us exactly what the threat is beyond just that it’s malicious.”



Malicious
Main Family: Dridex

SHA256
f4f0127923c4a1c69aab04516907fd4010f9af8302e132b972d053813577b18d
VIRUSTOTAL Report (16 / 61 Detections)
non_executable excel

Malicious.
Malicious file behaviour was observed during the dynamic execution

Analyzed on Jul 22nd 2021

Genetic Analysis | TTPs | IOCs | Behavior

Extended Dynamic Execution

Original File
317 KB
f4f0127923c4a1c69aab04516907fd401...
Malicious

Dynamic Execution
Powered by Cape
Show all

Memory
EXCEL.EXE | 2844
mshta.exe | 2972
rundll32.exe | 1764
qDialogFormatText 117 KB
Malicious | Dridex (806 Genes)

Dropped Files
qDialogFormatText.dll 176.5 KB
Malicious | Generic Malware (124 Genes)

Static Extraction Extract ▶

Genetic Summary | Related Samples | Code (1,384) | Strings (158) | Capabilities (20)

C:\ProgramData\qDialogFormatText Dridex pe dll i386

Show common □

Dridex
Malware 49.45%
Related Samples 806 Code genes 11 Strings

DoppelPaymer
Malware 5.84%
Related Samples 101 Code genes 0 Strings

Malicious Library
Malware 3.5%
Related Samples 47 Code genes 3 Strings

Unique
Unknown 40.39%
519 Code genes 40 Strings

The Qt Company Ltd
Library 1.82%
0 Code genes 7 Strings

Microsoft Corporation
Application 1.3%
0 Code genes 5 Strings

[Start Analyzing]