

DECEPTIVE BYTES

Never Let Your Business Down

ALWAYS ONE STEP AHEAD
T|A|G
DISTRIBUZIONE



Euro Informatica
Our star, your value.

Case Study

Emotet Attack on

Events Services Provider

Customer Profile

Our customer is an important company in the events services sector located in West Europe, which has always been attentive to investments in technology and IT security issues. The protection of internal systems, data, customer registration and transactions (via online access ticketing systems) are the priorities that have led the company to prioritize maximum security and to factor possible options with innovative solutions against cyber-attacks.



Need

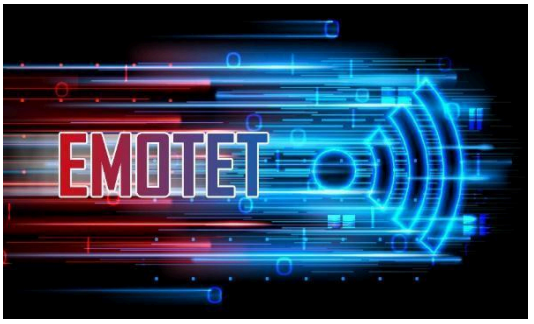
At the end of 2019 - early 2020, after the news of attacks on other services organizations, the spread of the pandemic and the potential attack surface and vulnerability, the company chose with farsightedness to implement - on top of security solutions at the highest levels already implemented - innovative cyber-security solutions able to protect and, above all, to further attacks in continuous evolution.

Overview

Every day, all over the world, malware attacks organizations and companies of all sizes, affecting their daily activities and causing losses to companies that can be significant.
Malware is highly intelligent and evasive and uses several techniques to evade detection and analysis by security systems and researchers. Furthermore,the APT groups that launch mass email spam campaigns by randomly infecting users and with the help of careless or hasty employees, are now supported by evolved attack operators who work in vertically organized structures. Malware botnet operators often rely on social engineering to trick users into installing malware on their systems, even if the computers are running up-to-date Antivirus software.

© Copyright of Deceptive Bytes Ltd., 2025 - All Rights Reserved

How Emotet Malware Works



Like in many organizations that have experienced an Emotet attack, this form of malware infiltrates the network via a phishing email that contains an encrypted, password-protected file. The user unlocks the file, which "detonates" the malware, thus enabling it access to the endpoint, and ultimately the network, spreading malware thereupon. As it spreads across the network, it contacts its *Command & Control* servers (C2) to dynamically mutate the executable file to evade traditional malware detection and remediation tools. Emotet is later used by cyber criminals to perform *DDoS attacks* as part of a *Botnet network*, *Ransomware* attacks as a secondary payload, or as a Banking trojan to steal banking/financial information.

Distorting Ransomware Perception

Deceptive Bytes offers an innovative approach to endpoint security by turning ransomware's own evasive tactics against itself. Through its preemptive and proactive defenses, the solution distorts ransomware's perception of the environment, breaks ransomware logic, and prevents attacks before they can even begin. This forward-thinking strategy not only reduces the risk of breaches but also ensures your business remains operational, resilient, and secure in the face of emerging threats - Never Let Your Business Down!

Think differently. Protect proactively. Stay ahead of the latest threats.

Preemptive defense: Create a hostile or unappealing environment for ransomware to operate, reducing its motivation and chances of infection.

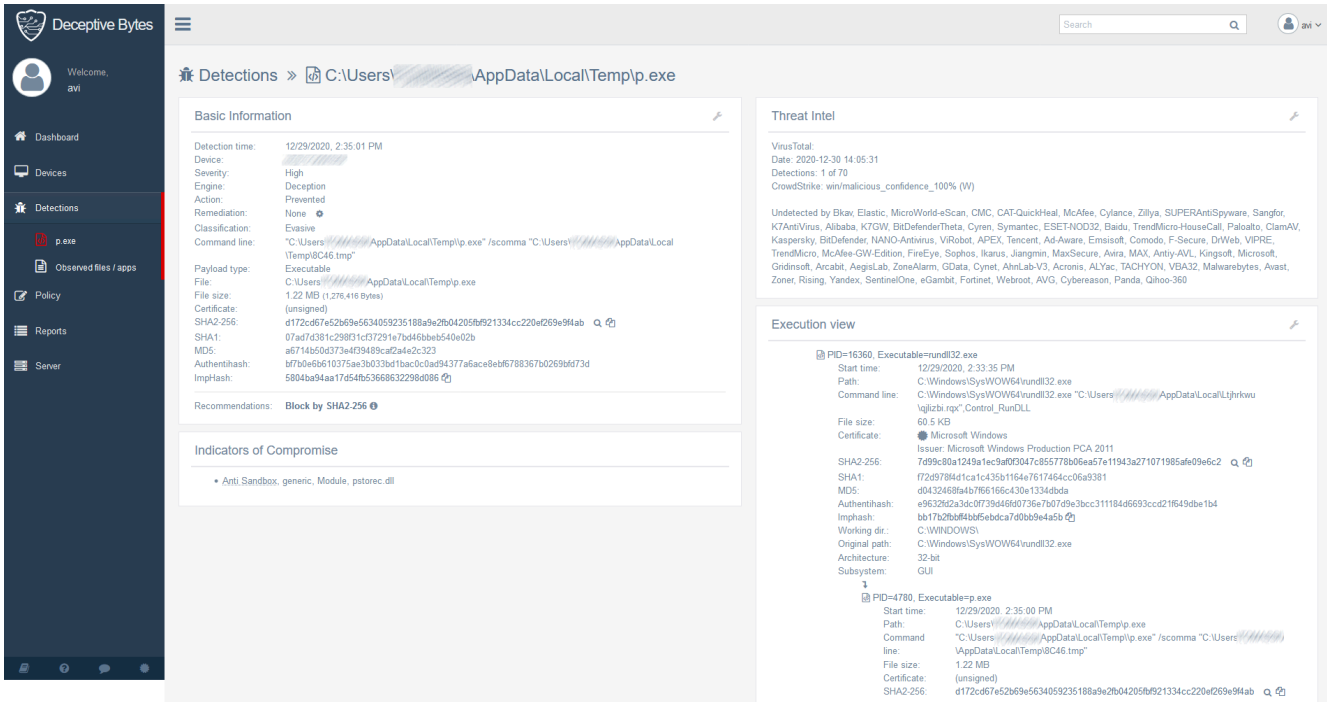
Proactive defense: Continuously adapts the strategy based on the attacker's behavior, effectively countering evolving threats.

Multi-layered approach: Seamlessly integrate with your existing security stack, enhancing your overall defense posture and providing an extra layer of protection.

Incident

During the holiday season, which is a time when attacks are increasing due to lack of attention & monitoring, a user opened a malicious email that contained *Emotet*, thinking it was a legitimate password protected tender document (directed to the company). He enabled the macro in the Word file which initiated the malware attack. Due to the customer's configuration, detecting 1st stage payloads (protecting Office in this case) was off, so the document executed a malicious PowerShell code that downloaded & started an executable file. The agent then detected the execution of the unknown file and activated the Deception engine on it, which detected the malicious executable (2nd stage payload) & neutralized the threat immediately.

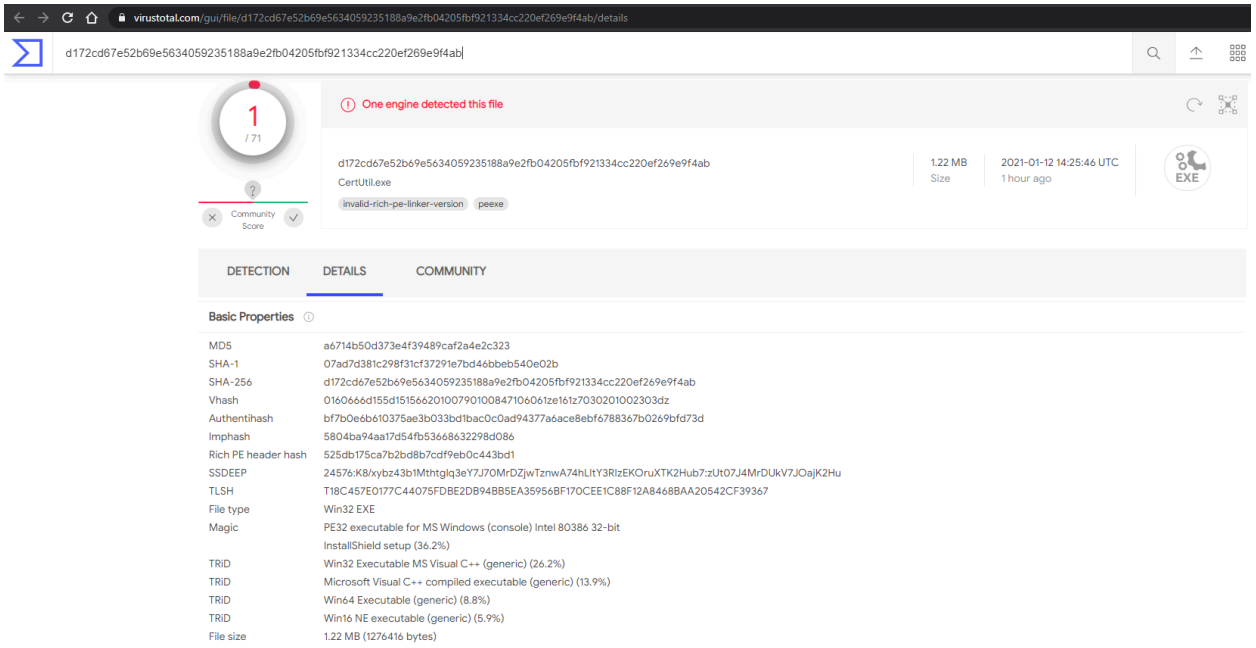
© Copyright of Deceptive Bytes Ltd., 2025 - All Rights Reserved



Prevention & detection information as shown from the customer's management server

Threat Intel

The file, as it appeared on VirusTotal, seems to be undetected by all other vendors except CrowdStrike, allowing threat actors to spread it easily across organizations uninterrupted.



© Copyright of Deceptive Bytes Ltd., 2025 - All Rights Reserved

Conclusion

Deceptive Bytes' solution provided immediate prevention capabilities to the customer while the user mistakenly opened a malicious file. The solution operated automatically without the operator's intervention, reducing the prevention & detection dwell time to zero, and safeguarding the organization from an unknown attack and potentially, any mutation of it.
Deceptive Bytes' team alerted the customer & service provider about the incident, which allowed them the ability to further investigate the malware at their convenience and remove any other related threat while keeping the organization secure.

Statement from the Customer

"Prevention is better than cure, said an old advertisement.... With the Deceptive Bytes solution and the support of Euro Informatica's services" - declares the Director of Information Systems: "We have added a level of protection, but above all of prevention of attacks, guaranteeing our systems a very high level of security. However, our attention remains very high in all scenarios of both attack and innovative solutions that may arise on the market"

About

In today's rapidly evolving threat landscape, ransomware and advanced cyberattacks are becoming more stealthy and sophisticated, targeting vulnerabilities that traditional security tools often miss. Deceptive Bytes offers an innovative approach to endpoint security by turning ransomware's own evasive tactics against itself. Through its preemptive and proactive defenses, the solution distorts ransomware perception of the environment, breaks ransomware logic and prevents attacks before they can even begin. This forward-thinking strategy not only reduces the risk of breaches but also ensures your business remains operational, resilient, and secure in the face of emerging threats - Never Let Your Business Down!

Additional information

Website Email Phone LinkedIn X

Azrieli Holon Business Center, 26 Harokmim st., Holon, Israel

© Copyright of Deceptive Bytes Ltd., 2025 - All Rights Reserved