

# Deceptive Bytes

## Active Endpoint Cyber Defense

### *Prevention by Deception*

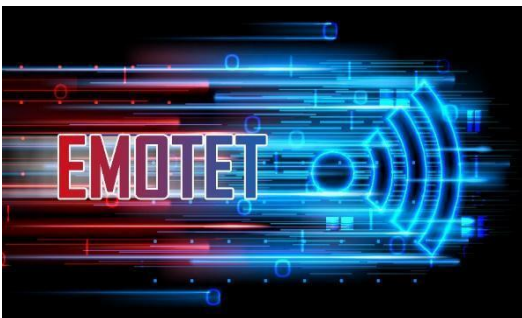
#### Case Study Emotet Attack on Events Services Provider

#### 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 that purchase access tickets with online ticketing systems are the priorities that have led the company to make choices of maximum security and to anticipate possible options with innovative solutions against cyber-attacks.

#### Need

At the end of 2019 - early 2020, after the news of attacks on other events services organizations, the spread of the pandemic and the need to operate in smart working, and given the increase in the potential attack surface and vulnerability, the company has chosen 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 prevent the company and employees themselves from potential attacks in continuous evolution.



#### 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 1<sup>st</sup> 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 (2<sup>nd</sup> stage payload) & neutralized the threat immediately.

#### Overview

In fact, 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.

#### How Emotet Malware Works

Like in many organizations that experienced an [Emotet](#) attack, this type of malware comes into the network via a phishing email that contains an encrypted, password-protected file. The user unlocks the file, which "detonates" the malware, this enables it access to the endpoint & network, ultimately spreading malware through the network. 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.



**Solution**

**Shaping the attackers' decision making**

Deceptive Bytes provides a fully endpoint- centric deception platform that uses existing IT infrastructure, responds to the evolving nature of advanced threat landscape and interferes with attackers attempts to recon & take hold of enterprise IT, in a preventative solution which covers sophisticated malware techniques & defenses in several ways...

**Preemptive Defense:**

Making malware believe it's in an unattractive/hostile environment to attack, reducing its motivation to attack and the chance of infection.

**Proactive Defense:**

Dynamically responding to threats as they evolve, based on the current detected stage of compromise, and changing the outcome of the attack.

**Conclusion**

Deceptive Bytes' solution provided immediate prevention capabilities to the customer while the user mistakenly opened a malicious file. The solution operated automatically without operator 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.

*"Prevention is better than cure, said an old advertisement.... With the Deceptive Bytes solution and the support of Euro Informatica's services, we have added a level of protection, but above all of prevention of attacks, guaranteeing our systems a very high level of security."*

**Director of Information Systems, Events Services Provider**

**Threat Intel**

The file, as it appeared on [VirusTotal](https://www.virustotal.com), seems to be undetected by all other vendors except CrowdStrike, allowing threat actors to spread it easily across organizations uninterrupted.

