deepinstinct™

CASE STUDY | FINANCE

Deep Instinct powers leading CPA firm against unknown threats, where traditional AV fails

149
MALICIOUS CAMPAIGNS DETECTED

NEWEST & UNKNOWN MALWARE PREVENTED
Banking trojan campaigns were revealed and fully prevented (Zeus, Dyre, Ursnif and CoreBot)

THE COMPANY

A financial consulting service firm based in North america with two offices, composed of more than 500 partners.

Industry: Finance
Company size: SMB
Existing security solution: Traditional AV
Environment: 800 Windows endpoints

THE NEED

The firm was looking for a comprehensive endpoint security solution to protect their organization from adversaries that might create damage for their customers.

They reached out to Deep Instinct to evaluate the prevention capabilities of new malware. After a successful proof of concept, while Deep Instinct was able to detect and prevent the malware that the current existing solution, TrendMicro, was not able to detect, Deep Instinct was selected to secure the endpoints in the company.

> *“Like most businesses, ACCTFIRM identified the need to combat the unprecedented rise of malware. Unsatisfied with our existing vendors we turned to Deep Instinct, who assisted us in a companywide seamless deployment spanning several cities. With Deep Instinct deployed”*
>
> **Accounting Firm | Director of IT**

THE SOLUTION – DEEP INSTINCT™ THREAT PREVENTION PLATFORM

- **Deep Instinct™ D-Client:**
  - On-device agent includes D-Brain, powered by deep learning. Supports many file types, including PE, Office, PDF, Macros, Fonts, Images, Flash and many more.
  - Detects and prevents any malicious file before it is accessed or executed on the endpoint.
  - Lightweight with zero impact on the endpoints from initial installation. Low memory footprint (<150MB) and requires less than 1% CPU usage
- **Deep Instinct™ D-Appliance:**
  - Management Console for easy monitoring of the organization's security and deployment status.
  - Provides tools for configuring the organization's security policy.
  - Manages different policies for groups or individual devices.
- **Deep Classification:**
  - Rapid classification of malware (known and unknown) in real-time with no human involvement into seven different malware types, using Deep Instinct unique deep learning malware classification module.
- **Remediation:**
  - Quarantine files, restore files remotely, delete files remotely, terminate running process, isolate device network – all to mitigate and operate current existing threats identified in the environment.
- **Advanced threat analysis:**
  - Tool set that performs advanced analysis of threats found in the organization. This includes static analysis, sandboxing analysis, screenshots and network dump of the potential threats.

THE RESULTS

Unknown banking trojan campaigns fully prevented
During the deployment stage, banking trojan campaigns were revealed and fully prevented. This type of trojan aims to steal financial information from its victims. Those campaigns included Zeus, Dyre, Ursnif and CoreBot. The last two revealed were the newest waves of variants, and Deep Instinct was the first vendor to announce them in the media.

One of them, CoreBot, is a sophisticated banking trojan and information stealer, distributed by spam emails with Office documents as an attachment that runs malicious macros, or with JavaScript files. The malware itself uses WebInject technique in order to inject itself to browsers, and by doing so, is able to collect sensitive information such as passwords for bank accounts.

Full protection against any type of file
Although the firm had TrendMicro deployed, Deep Instinct was able to detect 149 malicious campaigns: mostly binary files, but also some malicious Office documents aiming to drop additional files, and PDF files that lead to phishing attempts.

Request an online demonstration of Deep Instinct platform

Click here to set up a free consultation on your endpoint security environment and see how Deep Instinct can help protect your organization in this live demonstration of our solution capabilities against unknown threats.

Request a Demo

TO GET STARTED WITH THE CYBERSECURITY REVOLUTION

ISRAEL

23 Menachem Begin Rd
28th Floor
Tel Aviv
Israel, 6618356

NEW YORK

501 Madison Ave
Suite 1202
New York City, NY
USA, 10022

SINGAPORE

The Working Capitol
1 Keong Saik Rd
Singapore
068907

☎ +972 (3) 545-6600 www.deepinstinct.com ✉ contact@deepisntinct.com

deepinstinct
BEFORE YOU KNOW IT