CASE STUDY | DISTRIBUTION

Auto glass distributer chooses Deep Instinct for explicit ransomware prevention after their current endpoint solution fails to detect an attack

11
MALICIOUS FILES REVEALED WITHIN A WEEK OF DEPLOYMENT

152
TOTAL UNIQUE MALWARE CAMPAIGNS REVEALED

DORMANT WANNACRY RANSOMWARE PREVENTED

THE COMPANY

An auto glass distributer based in the US.

Industry: Distribution
Company size: SMB
Existing security solution: Traditional AV
Environment: 100 Windows endpoints

THE NEED

The company was infected by a ransomware attack. Although they managed to restore the loss without paying the ransom, they quickly realized they needed a more comprehensive security solution to mitigate the ransomware threat and other possible threats that might affect its distribution chain.

After a warm recommendation from another customer, the company decided to challenge Deep Instinct and to evaluate the prevention capabilities of new malware.

The proof of concept went very well, while Deep Instinct was able to detect and prevent the malware that the current existing solution, MalwareBytes, was not able to detect. And so Deep Instinct was selected to secure the endpoints in the company.

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

Vicious dormant ransomware "WannaCry" detected on the company devices
Within the first week of deployment, 11 malicious files were revealed over 10 devices, including dormant WannaCry ransomware in 5 different computers waiting to run, worms and other malicious Office droppers.

Deep Instinct prevents what others can't find
After the deployment was finished, it was revealed that 38% of the devices were compromised. 152 unique malware campaigns were revealed; 90 of them were pure malware, making it more than 2 malware on average on each infected machine. Those campaigns include Crysis ransomware, Expiro virus, Zeus banking trojan and other spyware, backdoors, coin miners and banking trojans.

Although the customer had MalwareBytes deployed, Deep Instinct was able to detect dozens of malicious campaigns.

Deep Instinct's malware classification powers the organization to quickly analyze and mitigate threats
The Deep Classification, Deep Instinct's malware classification model, powered by deep learning, performed well and provided instinctive insights for the customer, making the analysis and understanding the threats much faster.

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