Our Competitors Are Hackers

Mehmet Dagdevirenturk

Security Researcher & CEH

Network Security Changed

There is no Port Scan
No IPS Attack

Develop Custom Malware – Targeted
Bypass Signatured Based Security Solutions
When Malicious File Reach Client,
Sleep for a while,
Then wake Up, Leak Data

Copyright 2014 Trend Micro Inc.

Copyright 2014 Trend Micro Inc.

Gartner®

“There is evidence that email is the preferred channel to launch advanced targeted attacks”

91% of targeted attacks begin with a spear-phishing email

Email attachments remain the most prolific attack vector at

78%

TREND MICRO

What is a Targeted Email Attack?

1.

Attackers use social engineering & background research to target a specific individual or organization

2.

Attackers create and send a spear phishing email that embeds advanced malware in attachments and/or URLs

3.

Email contains user relevant content, context and motivation for recipient to open a URL or attachment

4.

Advanced Malware is delivered and installed recipient's device.

5.

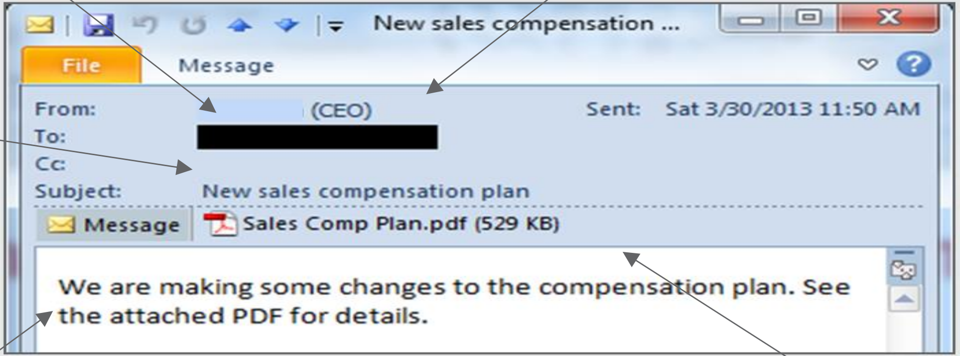
The targeted attack begins

Targeted Email Attack – Good Example

Often sent from a trusted IP address

Spoofed email address of someone known to you

Low volume of recipients



From: [redacted] (CEO) Sent: Sat 3/30/2013 11:50 AM

To: [redacted]

Cc:

Subject: New sales compensation plan

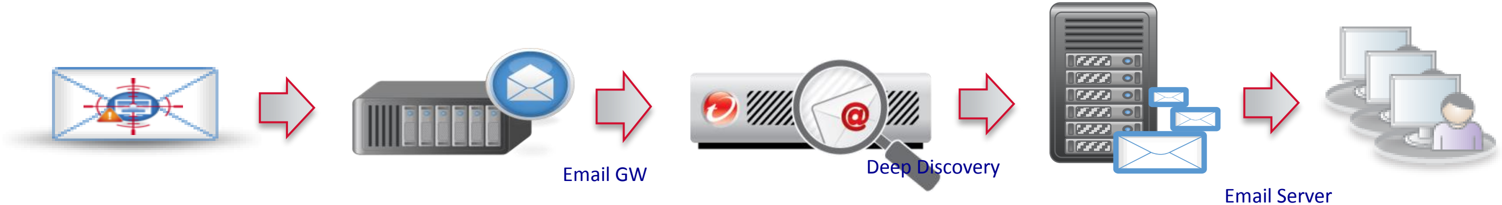
Message | Sales Comp Plan.pdf (529 KB)

We are making some changes to the compensation plan. See the attached PDF for details.

Please download the file from the following link http://sjlsfjdsfjsd.gr

Well-researched, convincing social engineering

Malware concealed in a legitimate looking attachment or URL



Trend Micro Deep Discovery Get in the Middle

Act Like Client

Check what is going On,

Stop APT’s

Share This Information with Clients (Antivirus)

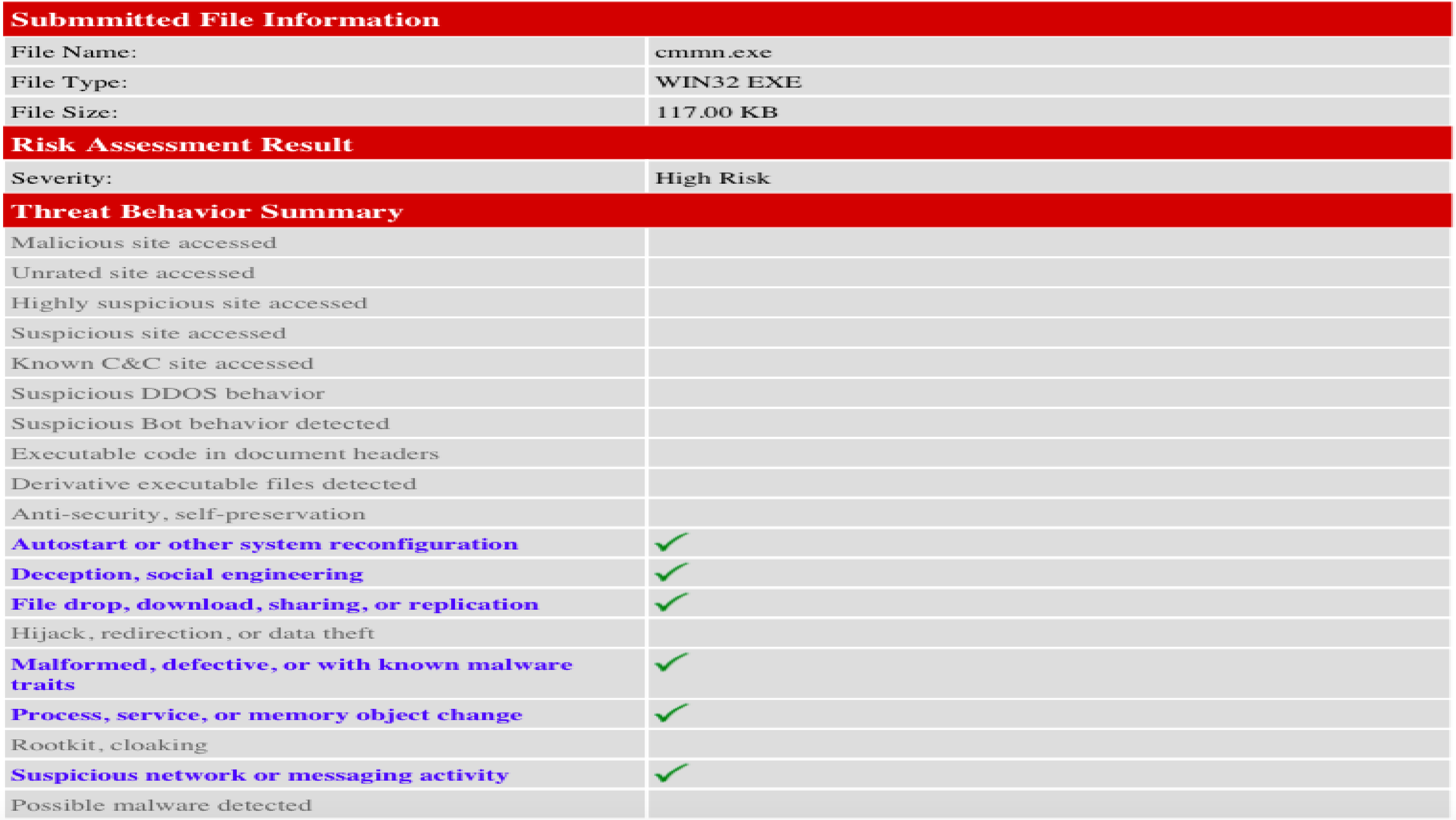
Deep Discovery Email Inspector

Targeted Email Attack Protection

A dedicated email appliance that detects and blocks emails containing malicious content, attachments or URLs

- Custom sandboxing and detection engines analyze email attachments
- Full analyzes embedded URL destinations
- Derives passwords for protected files
- Co-exists with other email security products

➢ ***Stop targeted emails that lead to data breach***



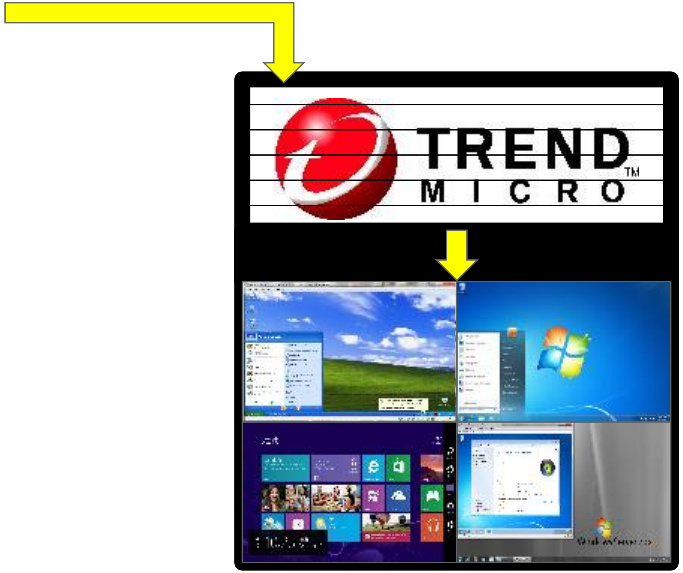
Submitted File Information	
File Name:	cmmn.exe
File Type:	WIN32 EXE
File Size:	117.00 KB
Risk Assessment Result	
Severity:	High Risk
Threat Behavior Summary	
Malicious site accessed	
Unrated site accessed	
Highly suspicious site accessed	
Suspicious site accessed	
Known C&C site accessed	
Suspicious DDOS behavior	
Suspicious Bot behavior detected	
Executable code in document headers	
Derivative executable files detected	
Anti-security, self-preservation	
Autostart or other system reconfiguration	✓
Deception, social engineering	✓
File drop, download, sharing, or replication	✓
Hijack, redirection, or data theft	
Malformed, defective, or with known malware traits	✓
Process, service, or memory object change	✓
Rootkit, cloaking	
Suspicious network or messaging activity	✓
Possible malware detected	

How it Works

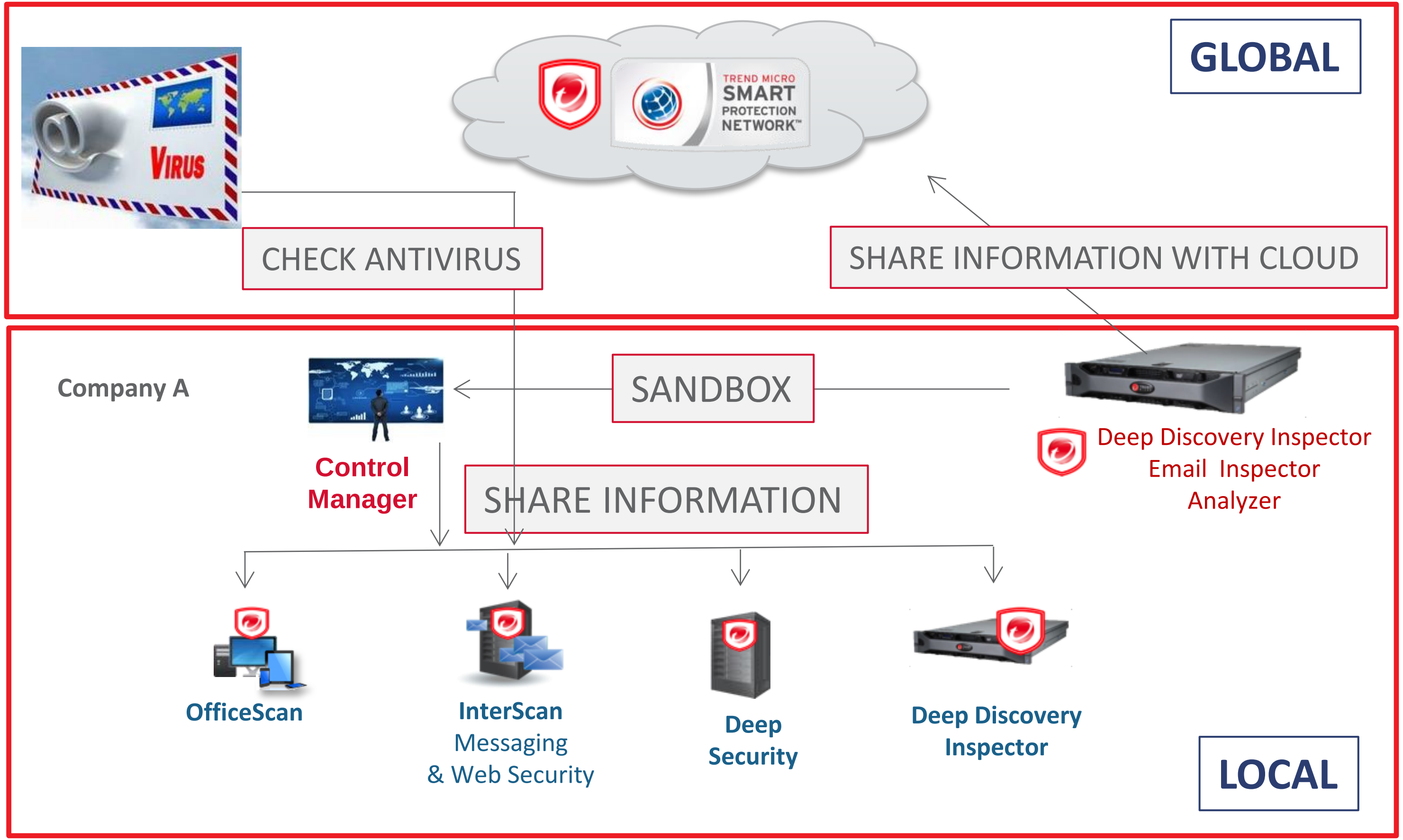
DD listens your backbone or any Managable Switch, show you risks or anomalies in your Network

It Also has Sandbox Technology

Deep Discovery simulates whatever coming to your network then Decide it is good or Bad

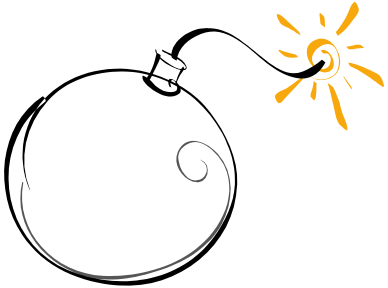


Deep Discovery – Local Information Sharing



Evasion Techniques

- Hypervisor Detection
- Virtual Device Detection
- Network Address Detection
- BIOS/Activation code Detection
- Virtual Driver Detection
- CPUID Detection
- Human Interaction Detection
- Timer Evasion

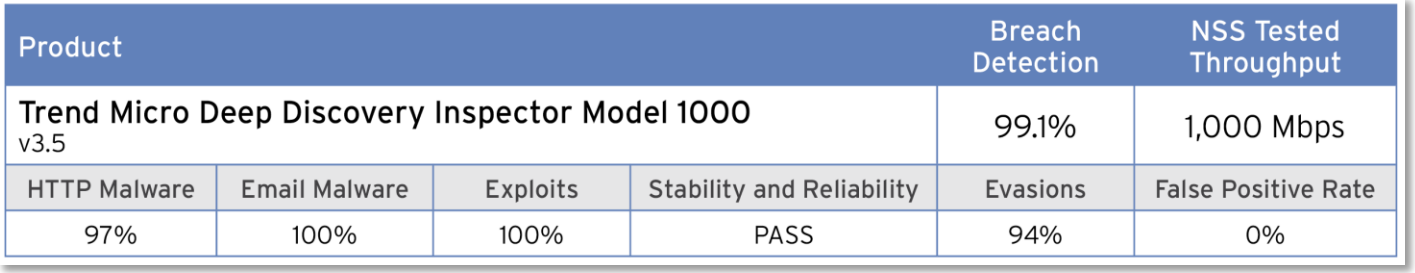


BEST SECURITY FOR UNKNOWN THREATS

Trend Micro™ Deep Discovery

TOP SCORE in breach detection

NSS Labs 2014 Breach Detection Tests



Product				Breach Detection	NSS Tested Throughput
Trend Micro Deep Discovery Inspector Model 1000 v3.5				99.1%	1,000 Mbps
HTTP Malware	Email Malware	Exploits	Stability and Reliability	Evasions	False Positive Rate
97%	100%	100%	PASS	94%	0%

THANK YOU