Trend Micro Deep Discovery Inspector

360-degree detection to address the challenge of targeted attacks and advanced persistent threats
Contents

Executive Summary .................................................... 3
Targeted Attacks: An Overview ...................................... 4
The Design and Motivations Behind Targeted Attacks ........ 5
The Trend Micro 360-Degree Approach ......................... 7
Trend Micro Deep Discovery Capabilities Summary ........... 10
References .................................................................. 13
Executive Summary

At the outset of 2014, TrendLabs predicted the year would see an average of one major data breach per month. Through the first half of the year, this prediction has proven correct. The recent cascade of significant data breaches has resulted in the theft of hundreds of millions of credit and debit card records, userids, passwords, and more. And it has brought major unexpected costs and risks—including both strategic and career risks—to the organizations and individuals charged with preventing such breaches.

Recent research reveals the alarming extent to which targeted attacks have grown to become a compelling business challenge:

• According to 2014 research by Ponemon, the average cost of a targeted attack is $5.9 million US
• The cost of a single successful attack can be much higher than the average; for example, the cost to EMC for the RSA attack was a staggering $66 million US
• IANS found that 50% of organizations surveyed reported being the victim of at least one targeted attack
• Research sponsored by Trend Micro suggests that 58% of surveyed organizations have discovered malware on their network that was not detected by traditional security solutions
• 75% of attacks in 2013 were found to have required little skill to execute, yet subsequent actions to remediate required “advanced skills, significant customizations, and/or extensive resources”

The purpose of this white paper is to empower executives and security personnel to make optimal security decisions, by providing clear, in-depth information about the nature of today’s targeted attacks, and about the capabilities needed to address them. In the sections that follow you will learn:

• How today’s targeted attacks achieve their goals
• Why traditional defenses are unable to detect or block these advanced threats
• How a multilayered, comprehensive 360-degree approach to detecting and thwarting targeted attacks is in the best interest of your organization
• How to implement a comprehensive solution with minimal time and resource costs
• How to avoid the catastrophic costs and career impacts of a successful data breach
Targeted Attacks: An Overview

Today’s targeted cyber attacks may be launched by a variety of actors with a variety of specific goals in mind. Your attackers might be an international criminal gang, a state or corporate spy agency, a hacktivist group, an unscrupulous competitor, or even disgruntled former employees. Their goals may be financial profit, economic advantage, competitive business advantage, making a statement, harming your organization’s brand, or financial harm to your business. They may want to steal confidential customer data, valuable intellectual property, strategic business plans, partner information, and more. Or they may intend to sabotage, vandalize, or destroy your network, servers, or online apps and web sites.

Despite this variety, all these attacks have two things in common:

1. They are purpose built to penetrate your network and your defenses, because they are the result of advance reconnaissance, research, and testing. They circumvent your security measures and exploit vulnerabilities in your software, your system, and your users to penetrate your networks.

2. They target critical data and systems that you are already protecting with significant security investments—and they bypass these defenses, passing through undetected.

Because they are designed to evade your specific defenses, each attack is unique. By definition, they use unexpected combinations of applications, devices, protocols, ports, command-and-control (C&C) communications, exploits, and advanced malware to achieve their objectives. And they are dynamic—changing their behavior and digital “appearance” during the course of an attack to evade detection.

Due to the nature of these attacks, organizations need to develop specific, new security capabilities to create an effective defense against targeted attacks and advanced threats:

1. Comprehensive monitoring of all inbound, outbound, and internal network traffic for malicious behavior, suspect communications, payloads, and attacker behavior. This includes effective monitoring of any and all devices that access your networks.
2. The ability to rapidly identify and triage known components of the early stages of targeted attacks. These may include malicious URLs, C&C servers, known malicious mobile apps, known malicious payloads, and known bad files.
3. Comprehensive analysis of suspicious payloads to detect exploits, zero-day attacks, and evasion techniques. Sandbox environments for analysis should match your operating system and application environments, and be easy to update as needed.
4. Ease of access to correlated and actionable insight on threat activity within your network.
5. The ability to rapidly correlate threat insight from your network with a proven and reliable external source so that your security teams can rapidly identify and respond to threats.
6. The ability to determine the extent of a breach, prioritize actions, and efficiently allocate resources for remediation.

The Design and Motivations Behind Targeted Attacks

The reason that the capabilities listed above are so critical is that targeted attacks and advanced threats are growing in number and sophistication, targeting organizations and networks of all types. The main reason for that growth is that these attacks work—as the headlines prove again and again. What’s more, the popularity of targeted attacks will continue to grow due to:

- **Low Barriers to Entry**: The skills, services, support, and resources needed to directly or indirectly execute a targeted attack are easily accessible and inexpensive. Everything from access to advanced malware and live tech support is easily available through online markets and notice boards.

- **Low Penalties for Failure**: If a given attack method fails, attackers merely change attack methods, payloads, and tactics to obtain what they seek. Further, the attack chain is often widely distributed, with third parties providing services, products, and support for attack research, hardware, pre-packaged code, testing, C&C infrastructure, and attack execution. The loosely coupled structure of these attacks reduces the risk of detection for all parties.

- **Designed to Avoid Detection**: Using advanced reconnaissance techniques, attackers identify ways to evade existing security defenses and avoid detection. Attacks will be designed to use the least expected and least monitored points of vulnerability.

Figures 1 and 2 below demonstrate the dynamic nature of how malware tactics evolve. In both cases attackers have adapted malicious payloads to use varying numbers of network ports and varying communications and application protocols. Without a truly comprehensive approach to detecting suspicious activity, such attacks have a very high chance of succeeding.

![Poison Ivy: Use of Multiple Ports](Figure 1)
Furthermore, how a targeted attack is structured in terms of initial points of attack, C&C, intended targets, and infrastructure evolves over time. As outlined in Figure 3 below, attackers using EvilGrab malware are able to dynamically alter the nature of the attack by changing IP addresses, C&C patterns, the number of compromised hosts, and other attributes.

The ability to detect a broad range of network activity, suspicious payloads, and attacker behavior is critical to a successful defense against targeted attacks.
The Trend Micro 360-Degree Approach to Detecting Targeted Attacks

With attackers now able to seek out vulnerabilities and customize attacks to exploit them, the only effective defense is one that employs 360-degree detection, to minimize the opportunities for a targeted attack. The approach employed by Trend Micro is illustrated in Figure 4 below.

![Diagram of 360-Degree Detection of Targeted Attacks]

Figure 4 – 360-Degree Detection of Targeted Attacks

Any areas that are left uncovered create gaps in your defense against attacks. Without a comprehensive 360-degree defense your organization will, in effect, be providing attackers with sanctioned access to your networks and data.

**Communication Protocols**

It is critical to monitor a broad range of communication protocols. Attackers typically conduct advance reconnaissance on your networks, applications, and communications methods. They use this insight to select communication methods that are least likely to be detected, and those that extend beyond web, email, and file.

**Network Ports**

Attackers do not use a predictable or predefined subset of network ports, but instead exploit an evolving variety of the 65,000 available network ports to launch and manage attacks, and
ultimately to extract data and intellectual property from your network. As conditions change, they can readily change ports to remain elusive. Any unmonitored port is effectively an unpolicerd thoroughfare for attackers.

Threat Insight

Fast, easy access to correlated and relevant threat intelligence is also critical to an effective defense. The ability to rapidly identify C&C servers, bad IP addresses, untrusted files, attack patterns, and other malware behavior is necessary to enable timely identification and reaction to threat activity. In order to enable continuous improvement of threat detection, and of methods of thwarting attack, a solution vendor must have:

- A broad and diverse set of threat insight capabilities
- A sizable and experienced threat research team
- A proven track record of assisting law enforcement with arrest and prosecution of cyber criminals
- A portfolio of integrated capabilities across a variety of security offerings
- The ability to proactively monitor advanced malware, evolving attacker techniques, and the overall threat landscape

Known and Unknown Threats

**Known threats: Detection depends on threat intelligence**

In order to create economies of scale and speed time to attack, perpetrators tend re-use and repurpose C&C servers, payloads, files, websites, and other assets. Without both extensive threat insight, and the ability to rapidly triage all network traffic across all ports and protocols, your IT and security teams may be left temporarily blinded to an attack, and be tasked with needless remediation activities that could have been readily avoided.

With Trend Micro, advance triage is a built-in capability of our targeted attack solution. Part of the efficacy and efficiency of this capability is based on a reliable and extensive source of global threat insight, the Trend Micro Smart Protection Network (SPN). The SPN provides access to services such as mobile application reputation, IP blacklists, identified C&C servers, known exploits, web site reputation, file reputation, email reputation, threat actor intelligence, and much more. All of this data is kept up to date by a vast global network of sensors and teams of highly skilled threat analysts.

**Unknown threats: Beyond malware detection**

The ability to identify unknown threats involves a variety of advanced capabilities. These include the ability to:

- Correlate and recognize attacker behavior
• Identify and thwart sandbox evasion techniques used by advanced malware. (Figure 5 below illustrates how operating system language settings can be used by attackers to avoid detection)
• Identify document, file, and application exploits
• Investigate multiple file types and sizes
• Replicate malware behavior in a sandbox that mirrors your environment and computing images
• Associate new threat insight across all devices and activity on your network

Without these capabilities in place, organizations are likely to fall victim to unknown threats that are able to evade detection.

Figure 5 - Custom sandbox analysis showing detection based on operating system language settings. In this case the custom sandbox using Portuguese language settings detected the advanced malware whereas the generic English sandbox did not.

Evolving Threats

The structure and nature of a targeted attack just for a single malware sample can vary dynamically over time. Identifying changing IP addresses, C&C patterns, the number of compromised hosts, and other attributes enable an organization to make effective decisions about how to adapt their security posture in order to contain and mitigate further compromises or attack outbreaks. Any decisions that are based on a static view of an attack will likely prove to be reactive and therefore ineffective at best.

Network Traffic

The ability to monitor inbound, internal, and outbound network traffic for suspicious behavior and malicious activity is critical. This capability should be system- and port-agnostic and work across tethered, mobile, and any IP-based device. This comprehensive traffic monitoring enables detection of external threats, lateral movement of targeted attacks within your network, outbound C&C communication, and data exfiltration. It also enables you to identify
and terminate any attacks or malicious behavior originating from your network or connected devices, which could target your customers, suppliers, or other outside parties.

Further Reading

For those seeking further background information about targeted attacks and effective defenses, Trend Micro offers a large number of educational and informational resources.

Security Intelligence—Targeted Attack News and Updates

Security Intelligence—Internet Threat Research and Security News

Trend Micro Enterprise Webinar Series

Security Research Papers and Articles

Trend Micro Custom Defense: Proven Protection Against Targeted Attacks and Advanced Persistent Threats

Deep Discovery: Advanced Network Security

Trend Micro Deep Discovery Capabilities Summary

Trend Micro™ Deep Discovery™ provides the capabilities needed to achieve 360-degree detection and effective protection against advanced persistent threats and targeted attacks.

Custom Detection Across Your Network Infrastructure

Custom sandboxing precisely matches your computing images, providing accurate detection and reduced false positives. Images can include anything you use that runs on Microsoft™ Windows™. Your security team is not limited to a checklist of standard products and operating system versions.

Deep Discovery malware detection is more than just sandboxing. It uses multiple threat detection engines and multi-level threat correlation rules to detect malware in several ways. Among the benefits: detection of Macintosh™ OS X and mobile malware.

Malware is only one part of an attack. Deep Discovery detection engines and rules also identify C&C communications and other high-risk attacker activities.
To avoid leaving gaps and openings for attackers, Deep Discovery monitors all ports and more than eighty protocols—not just email and HTTP traffic and associated ports. And a simple control panel makes it easy to configure your own custom blacklists and threat detection rules.

In breach detection tests conducted by NSS Labs in 2014, Deep Discovery earned the highest scores among all the products tested, demonstrating the value of 360-degree protection as delivered by this unique integration of multiple, advanced detection technologies and capabilities.

**Custom Intelligence for Quick Risk Assessment and Response**

- Direct access to extensive threat insight and information in an intuitive form that expedites fast risk assessment and response:
  - Threat Profile: The characteristics, origins, and variants of detected malware.
  - C&C Information: The nature of the detected C&C communications, and the C&C addresses known to be associated with this malware or incident.
  - Attack Group/Campaign: Who and what is behind this threat?
  - Containment and Remediation: Known indicators of compromise to look for, and clear instructions to contain the attack, remediate the damage, and eradicate the malware.
- Collection and analysis of logs from any security product you own, in order to let you quickly match the threat profile to events across your network, to determine the extent of the attack.

**Lower Total Cost of Ownership**

- A single appliance provides detection across all protocols and ports, and all web, email, and internal traffic. No separate appliances are required for different kinds of traffic, reducing the resources needed to coordinate and integrate multiple products.
- An optional separate server—Trend Micro™ Deep Discovery Analyzer—can be added to provide additional custom sandboxing capacity beyond the native capabilities provided with Deep Discovery Inspector, in order to increase speed and throughput without investing in multiple, redundant capacities.
- Deep Discovery runs on standard hardware, giving you the flexibility to purchase Trend Micro’s bundled hardware appliances or virtual appliances, so you can choose the most cost-effective appliance for your situation.
- Competitive pricing, flexible form factors, and a single-appliance approach mean that the price of Deep Discovery is typically about half that of competing solutions.
- In its 2014 Breach Detection Competitive Testing, NSS Labs found that Deep Discovery’s TCO was more than 25% lower than the average of solutions tested. (View summary or complete report [here](http://campaign.trendmicro.com/forms/NSS_Labs_Breach_Detection_Comparison_Report))
Deep Discovery Powers Your Custom Defense Against Targeted Attacks

Deep Discovery adds the comprehensive, 360-degree network detection and analysis capability that your organization needs in today’s threat environment. But Deep Discovery can do more than that.

Deep Discovery has open APIs that allow its malware detection engines and sandboxing capabilities to be integrated into any other Trend Micro or third-party security product or used directly by your security response teams. This also allows sharing of detected C&C information with firewalls, gateways, and other security products.

All information can be fed to your SIEM, but focused log analysis can speed your response without the complexity of a SIEM.

These capabilities effectively unite your entire security infrastructure into a better defense against targeted attacks—what Trend Micro calls a Custom Defense. Because it is as uniquely suited to your network as the attacks that target it, the Trend Micro Custom Defense enables you to swiftly detect, analyze, and respond to targeted attacks before they can do their damage.
References

i Ponemon Institute, LLC May 2014


v Verizon 2013 Data Breach Report


- Summary of Trend Micro results:
- Full Report:

About Trend Micro

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with more than 25 years’ experience, we deliver top-ranked client, server, and cloud-based security that fits our customers’ and partners’ needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro Smart Protection Network cloud computing security infrastructure, our industry-leading cloud-computing security technology, products, and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe.

Additional information about Trend Micro Incorporated and the products and services is available at TrendMicro.com.