A Trend Micro White Paper | December 2014

Custom Defense Against Targeted Attacks

Proven Protection Against Targeted Attacks and Advanced Threats

» See how adopting a Custom Defense approach will enable you to enhance your current security investments while providing new weapons to fight back against your attackers.

Contents

Executive Summary..3

The Anatomy of a Targeted Attack..4

The Reality and Costs of Targeted Attacks..5

Strategic Choices and Consequences..6

The Alternative: A Custom Defense Solution..8

The Trend Micro Custom Defense Solution..10

Conclusion..12

Executive Summary

Advanced threats and targeted attacks have clearly proven their ability to penetrate standard security defenses and remain undetected for months while siphoning valuable data or carrying out destructive actions. According to a 2014 Ponemon Institute study, the average cost of just a single targeted attack on a large organization is US$5.9 million. And Verizon's 2012 research findings, revealed a staggering 855 incidents and 174 million compromised records. Despite the mass scale, the response from the security industry has been largely limited to an "advanced-threat marketing makeover" around the traditional security technologies.

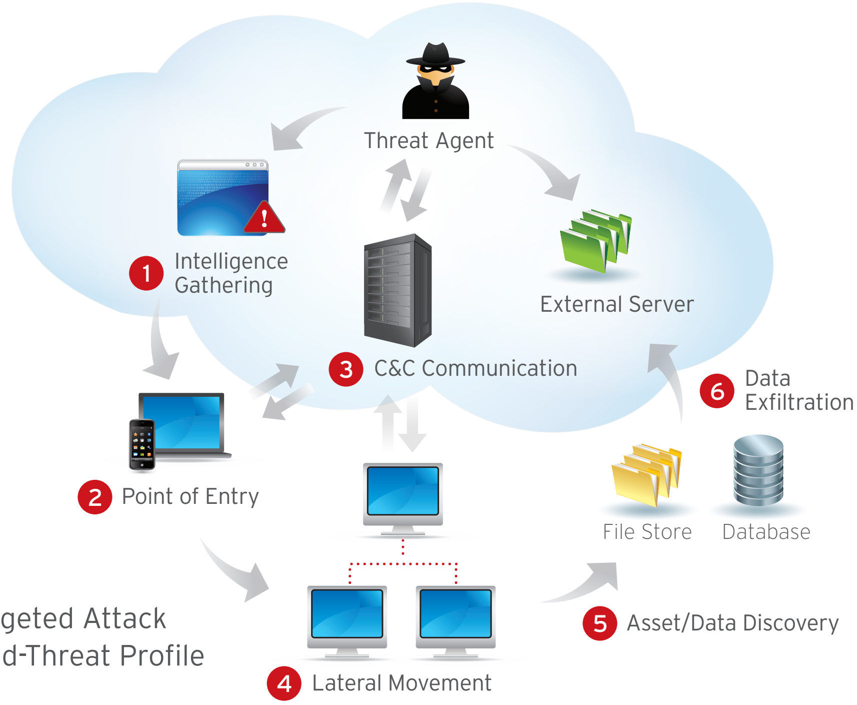
According to the 2014 Ponemon study on the costs of Cybercrime for 257 large organizations located throughout the world, there are 1.7 successful attacks per organization each week, with a median cost of cybercrime at $6.0M.

But standard protection products' signature-based, one-size-fits-all approach cannot deal with the custom nature of targeted attacks and their dedicated perpetrators. These attack groups utilize malware, social engineering, and hacker techniques specifically customized to the task of evading your defenses and successfully attaining their goals against your company. By design, they will defeat standard security products utilizing generic signatures. Combating these custom attacks requires a *custom defense*—a new strategy that recognizes the need for a specific approach and relevant intelligence that is uniquely adapted to each organization and its attackers. A Custom Defense solution augments an organization's standard security by detecting and analyzing advanced threats targeting the specific organization, immediately adapting protection against the attack, and enabling a rapid remediation response.

This whitepaper will describe the challenges faced by information security leaders, their options for dealing with their attackers and how adopting a Custom Defense approach will enable them to deploy a comprehensive Detect–Analyze–Respond lifecycle that enhances their current security investments while providing new weapons to fight back against their attackers.

The Anatomy of a Targeted Attack

Advanced threats are more than a buzzword. Already, we have seen the likes of Stuxnet and Flame as widely recognized examples of carefully crafted attacks focused on specific goals in targeted organizations. While cyber-attacks previously employed a mass scale opportunistic strategy, advanced-threat hackers are well organized, working together as part of a professional team, taking a slow-and-low approach to work their way into specific target companies. The goal of this "one-to-one," targeted approach is to steal valuable intellectual property and money, such as, intercepting bank wire transfers, credit card data, authentication credentials, trade secrets, and other personal identifiable information. Attackers only need to trick a single employee into opening a piece of malware that exploits a zero-day vulnerability, enabling them to take control of the employee's PC, gain access to the corporate network, and execute a cycle of difficult-to-detect maneuvers to attain their ultimate goals.



A Typical Targeted Attack and Advanced-Threat Profile

1 Intelligence Gathering
Identify and research target individuals using public sources (LinkedIn, Facebook, etc) and prepare a customized attack.

2 Point of Entry
The initial compromise is typically from zero-day malware delivered via social engineering (email/IM or drive by download). A backdoor is created and the network can now be infiltrated.

3 Command and Control (C&C) Communication
Allows the attacker to instruct and control the compromised machines and malware used for all subsequent phases.

4 Lateral Movement and Persistence
Once inside the network, attacker compromises additional machines to harvest credentials, escalate privilege levels and maintain persistent control.

5 Asset/Data Discovery
Several techniques (ex. Port scanning) are used to identify the noteworthy servers and the services that house the data of interest.

6 Data Exfiltration
Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed and often encrypted for transmission to external locations.

The Reality and Costs of Targeted Attacks

Already the world has seen great loss and expense from successful targeted attacks. EMC reported spending $66 million in dealing with the fallout from a successful attack against its systems, which obtained information related to its RSA SecureID authentication technology.

But, advanced threats and targeted attacks are not just a concern for large enterprises and government agencies. According to Verizon's 2012 Data Breach Investigation Report, the threat is real for large and small organizations alike, because organizations of all sizes have valuable data. According to Verizon's findings, "nearly all payment card breaches are shown to affect small businesses, [which is a continued] trend... where the bulk of criminal activity targeting payment cards has shifted away from larger organizations to smaller ones, primarily because they can be obtained at a lower risk. [On the other end], it is apparent that larger organizations are on the losing end in the majority of thefts involving trade secrets and other sensitive organizational data."

Based on the more frequent, successful targeted attacks, enterprise CISOs and security teams are starting to take notice and to plan action. According to an Enterprise Strategy Group survey of 244 U.S.-based security professionals, 59% said they were certain or fairly certain their companies had been targeted, and 65% expressed concern that advanced threats are undermining national security and the economy. In fact, 32% of survey respondents said the advanced threat problem "will cause us to increase security spending."

During a presentation at the 2012 (ISC)^2 Security Congress, AT&T's executive director of security technology, Joe Bentfield, talked about his findings after researching the effect advanced threats were having on the company and what could be done to stop them. Bentfield called advanced threats "very much a real threat today," and said, "advanced threats are a stark reality. Organizations that aren't preparing new, defensive tactics to detect and defend against them are already losing ground to attackers."

> “There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don't know it yet.”
>
> - Gartner Research 2012

As organizations now face the reality of advanced threats and look for an approach to mitigate them, it is critical they recognize the key attribute of these threats is stealth. These attacks are slow and steady efforts that go to great lengths to masquerade as legitimate communication and network traffic without generating the recognizable traffic often seen when malware spreads throughout a network. Equally important for organizations to understand is that these attacks are explicitly developed to evade traditional anti-malware and intrusion detection and prevention solutions.

Strategic Choices and Consequences

THE STATE OF INDUSTRY SOLUTIONS

Standard security solutions at the network, gateway and endpoints play a vital role in protecting any organization's data and operations. But their detection limitations, real-time execution constraints, and reliance on mass signature and reputation updates renders them unable to adequately detect and defend against a truly targeted attack. These attacks are successful because the zero-day malware used is designed to be invisible to standard security, and the human attacker activities are typically either undetected or buried deep in the undiscovered logs of IPS, SIEM and other security systems. Targeted attackers effectively evade these technologies and the one-to-many "vaccination approach," which is the backbone of defending against known malware and attack vectors.

The established security vendors have done little to nothing to address their current product limitations or develop any new technologies. Innovation has been left to small, start-up firms, a few of whom have developed products that can detect a portion of the zero-day malware used in the initial stage of an attack. However, these products limit detection to Microsoft-based malware, do not detect attacker activities, and typically act in an isolated manner—independent and unconnected from the other security protections in place.

Finally, next-generation firewall, IPS, and some gateway vendors have attempted to join the advanced-threat bandwagon by bolting on cloud-based sandbox malware detection to their solutions. At best, this adds malware detection of unproven merit and limited scope to their list of otherwise valuable functions. Perhaps more likely, is customer confusion in evaluating solution effectiveness, and customer concern over data privacy and control.

THE REAL CHOICES AT HAND

In spite the growing reality of advanced threats, the industry has left security decision makers with few choices for effective action, and no offer of a comprehensive approach to creating a better defense. How then to reduce your risk of attack?

Option #1: Do nothing

As we have seen, this is a poor choice for any organization. Industry analysts, experts and government agencies around the world have made an unambiguous call for companies to take a proactive stance against advanced threats by utilizing advanced network monitoring. Relying on traditional security products to effectively address this issue is not a viable option for any organization that values security as an essential business enabler.

Option #2: Adopt new, adjacent technologies

Network packet capture has emerged as a complementary tool for compliance and attack investigation and forensics. However useful, it has not proven itself as effective method for timely attack detection and response. Next-generation firewalls offer important protection and control benefits, but cannot offer the breadth and depth of detection required for the job. Investment in these products is an important but incomplete step in a proactive strategy against targeted attacks.

Key Security Challenges

VISIBILITY: What's really happening on my network?

DETECTION: How to identify what is evading my standard defenses?

RISK ASSESSMENT: What's dangerous? What's not? Who is behind this attack?

PREVENTION: Should I block this attack? How?

REMEDIATION: How widespread is this attack and what actions should be taken?

Option #3: Adopt standalone advanced threat detection technology

This direction is advocated by most authorities as the most effective way to address targeted attacks. These products use specialized detection techniques to discover what is invisible to standard defenses. Several vendors stand out for their detection and analysis capabilities but important tradeoffs are in the balance, and consideration of if and how this additional product will augment and work with your current defenses is a must. A multi-vendor evaluation is essential to making the right choice for your particular needs.

Option #4: Add or extend SIEM analysis

SIEM has been viewed by some as the ultimate answer to the advanced-threats problem. But in reality, unfocused SIEM analysis of standard security events it is not an effective nor efficient means to detect targeted attacks. SIEM-style log analysis can be a very effective method for assessing the scope of a discovered attack and directing containment and remediation activities. Combining SIEM analysis and reporting with log collection from an advanced threat detection solution is an option readily being adopted by organizations which have already made a SIEM investment.

The Alternative: A Custom Defense Solution

Until now, the best that the industry has to offer is new technology in the form of an additional network-based malware sandbox product that is largely independent and disconnected from the rest of an organization's existing security solutions. A solution that offers a new level of detection but that at its heart is based on a generic one-size-fits-all approach similar to the standard protection products already in place.

What would an ideal solution be? An ideal solution would weave your entire security infrastructure into a custom and adaptable defense that is tuned to your particular environment and particular attackers.

An ideal solution would not only perform custom detection and analysis of attacks at the network level, but integrate advanced detection technology into your existing endpoint and gateway defenses. Detection at any one protection point would automatically update other protection points to defend against further attack—all working in a multi-vendor security environment. An ideal solution would leverage the global intelligence of a major security vendor to aid in detection, and use it to provide you threat profile information relevant to your particular attack. Finally, an ideal solution would pair this profile with network-wide event analysis to guide rapid containment and remediation.

In short, an ideal solution is a Custom Defense employing a comprehensive Detect–Analyze–Respond lifecycle unique to your particular organization and the threats against it.

DETECT

Identifies attacks with advanced detection at network and key protection points such as email gateway

ANALYZE

Fully assesses threats using customer-specific sandbox analysis and integrated access to relevant global intelligence

RESPOND

Uses attack profiles and network-wide event intelligence to enable rapid containment and remediation

THE CUSTOM DEFENSE ANSWERS THE CHALLENGE OF TARGETED ATTACKS

The technology, intelligence and full lifecycle approach of a custom defense strategy answer the key security challenges associated with targeted attack prevention.

Visibility

Advanced monitoring and analysis of your inbound/outbound and local traffic lets you know what is really happening on your network. In addition to detecting advanced threats, it can reveal: risky applications in use; mobile device access and activities; unusual traffic and data transfer patterns and more. Traffic monitoring is the foundation of the proactive risk management strategies proposed by most security analysts and experts.

Detection

Advanced threat detection at the network can discover the malicious content (malware), communications and attacker activities that are typically invisible to standard defenses. But key to detecting target attacks is to employ sandbox simulation and threat detection rules that are customized to reflect your particular host configurations and IT environment and risk concerns. Additionally, by using an open detection/analysis platform, your can augment the detection and blocking capabilities of standard protection points such as email/web gateways and endpoint security, giving you increased protection against spear phishing and other early phase attack events.

Risk Assessment

An ideal custom defense solution augments automated local threat analysis with relevant global intelligence to provide the most in-depth information available. With the right global intelligence, even zero-day malware and previously unknown communication channels can often be linked to related samples or activities seen elsewhere—giving you a strong set of indicators of the attack nature, objectives and source. Armed with a threat profile based on this custom intelligence you can respond with the appropriate actions and urgency.

Prevention

A true custom defense solution uses custom detection, analysis and intelligence to augment protection from further attack and optionally block current attack activity such as command and control communications. This may include direct blocking at the detection point (network, GW, etc) but should include custom security updates (IP/URL blacklists, AV or other signatures) sent from the detection/analysis platform to all pertinent protection points. In this way, the entire security infrastructure adapts to defend against this new attacker. And sharing this information with the global security intelligence cloud ensures that other companies can better detection attacks with similar characteristics.

Remediation

The in-depth threat profile information will help guide containment and remediation actions and enable the optimum use of specialized tools and SIEM or other log analysis methods to determine the full extent of the attack and perform a detailed forensic analysis of the attack.

The Trend Micro Custom Defense Solution

Trend Micro believes that the attributes of a custom defense strategy make it the best choice to combat targeted attacks—and we are putting that belief into action by delivering a complete Custom Defense Solution. The Trend Micro Custom Defense Solution weaves your entire security infrastructure into a tailored and adaptable defense that is tuned to your particular environment and particular attackers. Using custom sandbox analysis, custom intelligence and custom security updates, the Custom Defense enables you not only to detect and analyze advanced threats and targeted attacks, but also to rapidly adapt your protection and respond to these attacks. The Custom Defense integrates software, global threat intelligence, and specialized tools and services to deliver a comprehensive multi-vendor solution to discover and block targeted attacks and shut them down before real damage occurs.

THE TREND MICRO CUSTOM DEFENSE SOLUTION—HOW IT WORKS

Detect: *what standard defenses can't*

At the heart of the Custom Defense is Trend Micro Deep Discovery—the advanced threat protection platform that performs network-wide monitoring to detect zero-day malware, malicious communications and attacker behaviors that are invisible to standard security defenses.

Unlike other products that rely on generic sandboxing to detect an attack, Deep Discovery uses multiple detection engines and customer-defined sandboxes that better reflect an organization's real-life environment and allow them to determine whether they have been breached. Deep Discovery sandbox simulation is also integrated with other Trend Micro products including Messaging Security products, giving them the power to block the spear phishing and social engineering exploits commonly used by attackers in the initial phase of a targeted attack. And Deep Discovery supports an open Web Services interface so that any security product can integrate with the custom sandbox detection.

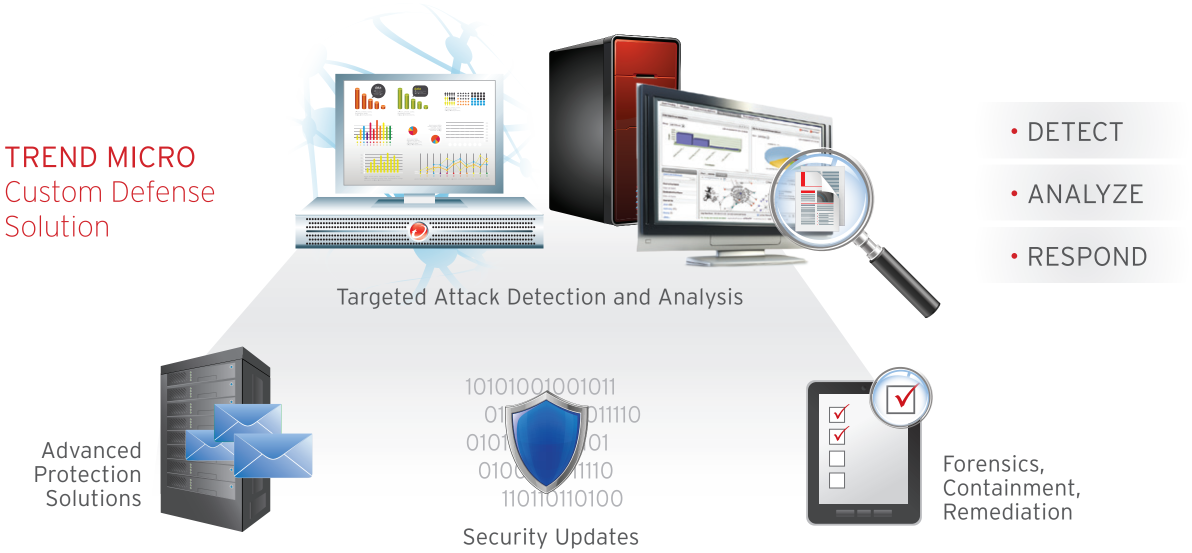
Analyze: *using real-time global and local intelligence*

Upon detection, Deep Discovery analytics and attack-relevant intelligence from the Smart Protection Network and Threat Connect portal create a rich threat profile that enables organizations to understand in depth the risk, origin and characteristics of the attack, and help guide containment and remediation plans. The depth of these threat profiles also enables the adaptive protection capability of the Custom Defense solution.

Respond: *with rapid containment and remediation*

Finally, the Custom Defense solution delivers 360-degree contextual visibility of the attack by combining the rich threat profile with results from employing specialized attack response tools and intelligence gathered from network-wide security event collection and analysis. Alternatively, the threat profile and other findings can be shared with a SIEM system already in place. Armed with this information the organization has the insight needed speed the containment and remediation process and to contact authorities as may be appropriate.

CUSTOM DEFENSE COMPONENTS	
Trend Micro Deep Discovery	Advanced Threat Detection at the heart of the Custom Defense Monitors your environment for malicious content, communication and behavior • Monitors your environment for malicious content, communication and behavior • Uses custom detection methods tailored to your specific configurations • Leverages deep threat analysis to generate custom updates to your protection points • Provides the custom relevant intelligence to guide your rapid response
Trend Micro Enterprise Security Products	Trend Micro security for endpoint, sever and gateway products integrate with Deep Discovery sandboxing and security updates to enhance and rapidly adapt protection against attacks.
Smart Protection Network Intelligence	The industry's largest and most sophisticated security cloud intelligence network and over 1200 threat researchers drive both Deep Discovery and all Trend Micro products. This intelligence is provided to you via the Threat Connect portal to aid in attack analysis and response.
Multi-Vendor Security and SIEM Products	Open Web Services Interfaces allow any product to integrate with Deep Discovery sandboxing and security updates. Direct integration to popular SIEM systems allows for enterprise-wide risk management.
Trend Micro Attack Response Tools	Trend Micro provides free-of-charge a set of incident response and forensic tools to discover and analyze advanced threats in mail stores and network traffic, as well as for searching log files for traces of attack activity.
Trend Micro Services and Support	Trend Micro service specialists augment your security responsiveness and expertise with installation, monitoring and consulting services to further reduce your risk exposure and security management costs.



Conclusion

The face of the threat landscape continues to change, and by all accounts, advanced threats are succeeding in their effort to gain access to the data and systems of target organizations. It is not sufficient to rely on standard security products to detect targeted attacks, and it is equally important organizations don't just simply fill the security gap with new network detection techniques as this only addresses a portion of the issue. Adopting a comprehensive strategy against advanced threats that enables organizations to effectively detect, analyze, adapt, and respond to attacks specifically targeting the organization will provide the strongest foundation for a successful defense.

With its Smart Protection Network threat intelligence and extensive research and collaboration with its customers, Trend Micro has a deep understanding of targeted attacks and the true risk they pose to organizations. It is that intelligence and insight that led to the innovation and development of the Trend Micro Custom Defense, which is the industry's first comprehensive advanced threat protection solution that enables companies not only to detect and analyze advanced threats and targeted attacks, but also to rapidly respond to these attacks.

It is critical for organizations to take immediate action and to include implementation plans for a Custom Defense strategy in their overall security budgets. As they look to implement such as a strategy, Trend Micro should be included in the vendor short list.

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TRENDMICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1408.257.2003