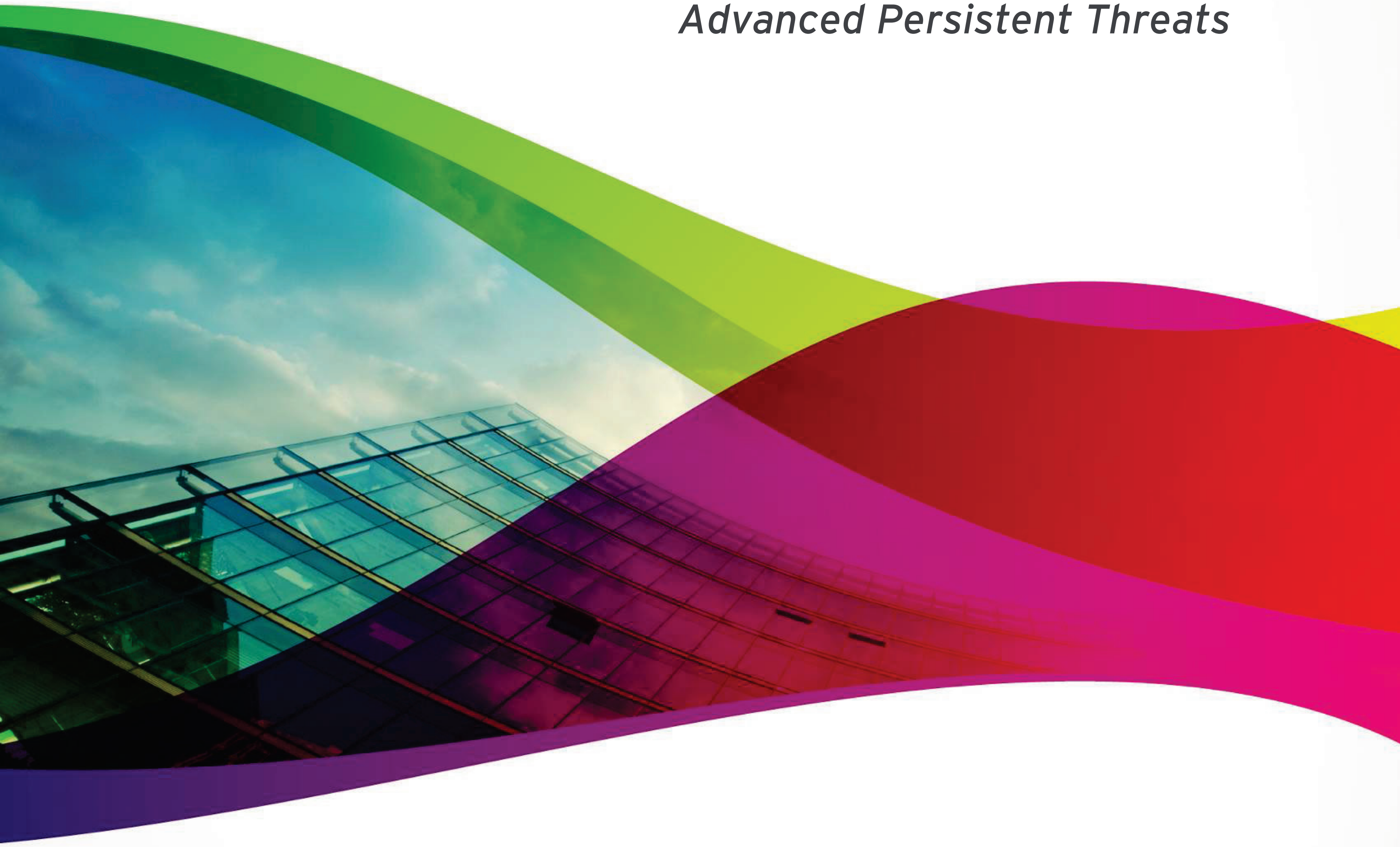
The 10-Step Action Plan

*Building Your **Custom Defense** Against Targeted Attacks and Advanced Persistent Threats*



Trend Micro Incorporated

Introduction

By design, advanced persistent threats (APTs) are able to evade standard perimeter and endpoint defenses. Standard security defenses are critical to the overall security architecture but cannot detect or prevent targeted attacks or APTs. Discovery and containment can take weeks to months and there is great risk of data loss.

Industry analysts and experts have made a clear case that an expanded definition of security due diligence is now "a must" for enterprises and government organizations. New, proactive measures and specialized technology are required as part your risk management due diligence.

This paper will outline ten steps essential for creating an effective action plan to defend against targeted attacks and APTs. These steps will help you to consider your current situational awareness, level of preparation and operative ability to ward off a persistent attacker. These steps include actions to implement the specialized detection and intelligence activities that are key to defending against targeted attacks and APTs.

ACTION 1

ACTION 1: Don't make the mistake of thinking that you are not being targeted

Did you know that industry experts estimate that only 1% of all targeted attacks are ever reported publicly to law enforcement, regulatory bodies, or affected customers and individuals? And of that 1%, a staggering 94%[1] are unaware they are a cyber victim until being notified by external bodies like law enforcement, national cyber emergency response teams (CERT), threat researchers or ethical hackers.

Mainstream media have repeatedly described the threat landscape as constantly evolving, that attacks are becoming more sophisticated and that the people behind these attacks are more equipped.

What are they after, and are they targeting you?

Online fraud has long since moved from being a mere hobby to be a primary means for cybercriminals to earn a living. In a recent report on the Russian Underground, Trend Micro revealed the extent to which fraudsters have monetized cybercrime, effectively creating a *crime-as-a-service* business model where they sell off-the-shelf malware, malware-writing services, access to active botnets, servers, VPN credentials, and much more.[2]

Cyber espionage and state-sponsored hacking have been revealed to be standard operating procedure for a significant number of nation-states of varying levels of development. Government-level data breach impacts entire populations, such as recently experienced by the residents of South Carolina who were left scrambling for credit protection after a stealthy, long-term attack breached 3.6 million Social Security numbers and 387,000 credit and debit card numbers.[3]

What makes you think that you are not a valuable target for cybercriminals?

ACTION 2: Understand what makes you valuable

ACTION 2

Recognizing that there are at least 20 different varieties of services offered and employed by Russian cybercriminals alone, for Action 2, we must consider the different ways that attackers see us as valuable targets:

- what they can steal
- what they can leverage
- what they can use

Intellectual property, financial or corporate data, and customer or citizen information are all prime targets of cyber criminals for resale or blackmail. In addition, online access and credentials for valuable business banking accounts have been proven to be successful attack vectors for organizations of all sizes. Your organization does not need to contain national security secrets to be

[1] Presented by Ryan Kazanciyan, Senior Consultant, Mandiant at Countermeasures 2012, Ottawa, Canada

[2] http://www.darkreading.com/threat-intelligence/167901121/security/vulnerabilities/240012590/shopping-the-russian-cybercrime-underground.html

[3] http://www.reuters.com/article/2012/10/29/us-usa-cybersecurity-southcarolina-idUSBRE89S13T20121029

targeted for espionage; however, data classification and least-privilege access controls should be integrated into the information security practices of every organization.

According to Trend Micro research, 75% of organizations' networks contain at least one active bot initiating command and control (C&C or C2) communications outside of their organization and 90% have active malware. An organization's IT resources could be a launching point for further criminal activities. Even services organizations that have secured their customer lists and do not possess a significant amount of intellectual property still represent a significant valuable opportunity to cybercriminals because of their computing power.

ACTION 3

ACTION 3: Understand what makes you vulnerable

If security has been in the top 10 list of CIO priorities for more than the past 5 years, how is it that bots and malware still exist in up to 90% of enterprise networks? We have detailed best-practice security policies; we manage steering committees; and, we run expert technology. We train and retrain our employees to ensure they understand that we expect them to protect our computer security as they protect their homes.

Our increasingly cloud-based IT environments, which are being forced to cope with an influx of insecure endpoints in the form of employee-owned mobile devices, are not the only reason we are vulnerable to targeted attacks. Attackers seem to be perfecting the art of finding the vulnerabilities in the software and architectures of our networks. We need to be diligent with patching, vulnerability testing and regular security evaluations, yes, but this is only part of the battle.

The people behind targeted attacks now augment their penetration techniques with social engineering activities, exposing another vulnerability, our new social online behaviours. Since email is the leading mode of business communication, threat actors typically deliver exploits through this medium. The attackers conduct open-source research of employees online and use this information to craft effective social engineering lures.

ACTION 4: Look at your employees differently

ACTION 4

We cannot place the blame for social engineering squarely on the shoulders of employees. In many organizations, Facebook, Youtube and Twitter are marketing tools, implemented to attract a wider customer audience. LinkedIn and Google+ are tools of social executives, used to promote, recruit and advance business opportunities. In fact, organizations that do not allow social networking face potential limitations in recruiting the younger and, more connected workforce.

But, let's Consider LinkedIn for a moment. In June 2012, LinkedIn announced they had been compromised with a security breach affecting 6.5 million user passwords.[4] Of your organizations leadership team, how many of them are on LinkedIn? How many of them use the same password for your network resources as they used for their LinkedIn profiles? Did you know that 1 in 4 people use the same password or a variation of it for all his or her accounts?[5]

[4] http://www.forbes.com/sites/georgeanders/2012/06/07/linkedins-password-breach-draws-fbis-attention/

[5] http://blog.trendmicro.com/trendlabs-security-intelligence/infographic-fear-factors/

The advent of Twitter and the 140 character communication has accelerated the proliferation of abbreviated URLs, and URL mapping services which can be used to hide the ultimate direction of a hyperlink in a tweet, an email or web page. 1 in 5 people report that at least once every week they click on links that take them to unexpected locations.[6]

As mentioned above, non-corporate mobile devices—smart phones, tablets and laptops—are increasingly being used to enable today's workforce to be available and working, anywhere and anytime. Smartphones are to the early 21st century what the PC was to the late 20th century–a universal tool valued for its productivity and fun factor but hated for the problems it can bring. Since smartphones are handheld computers that communicate, the threats they face are both similar and different from the PC challenges many of us are familiar with. Like the PC, many of today's mobile malware prey upon the unwary. However, the nature of the mobile malware threat is, in some ways, very different.

According to Trend Micro research, malware targeting Google's Android platform increased nearly six fold in the third quarter of 2012. What had been around 30,000 malicious and potentially dangerous or high-risk Android apps in June increased to almost 175,000 between July and September.[7]

The "bring your own device" (BYOD) movement may offer your organization capital savings and increased employee satisfaction, but without proper security mechanisms, it may introduce high levels of risk that need to be addressed within your security infrastructure.

ACTION 5

ACTION 5: Look at your technology environment differently

When considering our network security, Action 5 demands us to consider the fact that we likely have already been compromised. Well-organized criminal gangs are targeting their cyber attacks with more precision and sophistication than ever before.

Attackers know full well that if organizations are alerted to a breach, IT is likely to check for two things: 1) any vulnerabilities which a hacker might have exploited to gain network access and 2) signs of communication with an unknown IP address. Both incident response activities can be foiled.

Firstly, an attacker will make sure that once they have infiltrated a network they patch any vulnerabilities that they have leveraged to penetrate the network. This is partly to disguise their own entry route and partly to ensure rival hackers do not piggy back on their efforts. They'll also clean up any malware to make sure it doesn't interfere or draw attention to their assignment at hand—exfiltrating you data.

Secondly, command and control communications will be moved inside your technology ecosystem and put on a 'sleep cycle' so that there is no constant and easily detectable connection to a single IP address outside the organization. Now as a digital insider, the attacker will reach out, perhaps once a week or even once a month, to an outside IP address to avoid detection. Trend Micro witnesses this behaviour with the recent IXESHE campaign[8].

[6] http://blog.trendmicro.com/trendlabs-security-intelligence/infographic-fear-factors/

[7] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-3q-2012-security-roundup-android-under-siege-popularity-comes-at-a-price.pdf

[8] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf

The bad guys are also subverting common incident response strategies in an even more insidious way, using security and encryption technologies against the security teams to make detection and analysis arduous and costly.

ACTION 6: Don't forget the cloud

ACTION 6

Many businesses are evolving their data centers to include virtualization and cloud computing to improve resource utilization, accelerate development and deployment of computer resources, and reduce costs. However, these new platforms open additional avenues for threats against data, systems, and reputation.

For the most part, these threats are presented through the same types of attacks – data-stealing malware, web threats, spam, phishing, Trojans, worms, viruses, spyware, bots, and more. However, virtualization and cloud computing raise new infrastructure issues that must be considered when creating a security foundation to protect against targeted attacks.

In virtualized environments, traditional network security appliances are blind to the communication between VMs on the same host unless all communications are routed outside the host machine to this separate appliance. But this security configuration introduces significant time lags, and most organizations do not accept security inhibiting business. This blind spot makes it easier for attackers to hide command and control communications, and move laterally within virtual networks.

One way to eliminate these blind spots is to place a dedicated scanning security VM on the server host that coordinates communication between VMs. This solution works well in a virtualized environment. However, a dedicated security VM is not ideal for a cloud environment. The dedicated security VM integrates with the hypervisor to communicate with other guest VMs. In some cloud environments, such as in a multi-tenant public cloud like Amazon, users do not have access to the hypervisor. In the cloud, protection is best provided as self-defending VMs. Protection is self contained on each VM and does not require communication outside of the VM to remain secure.

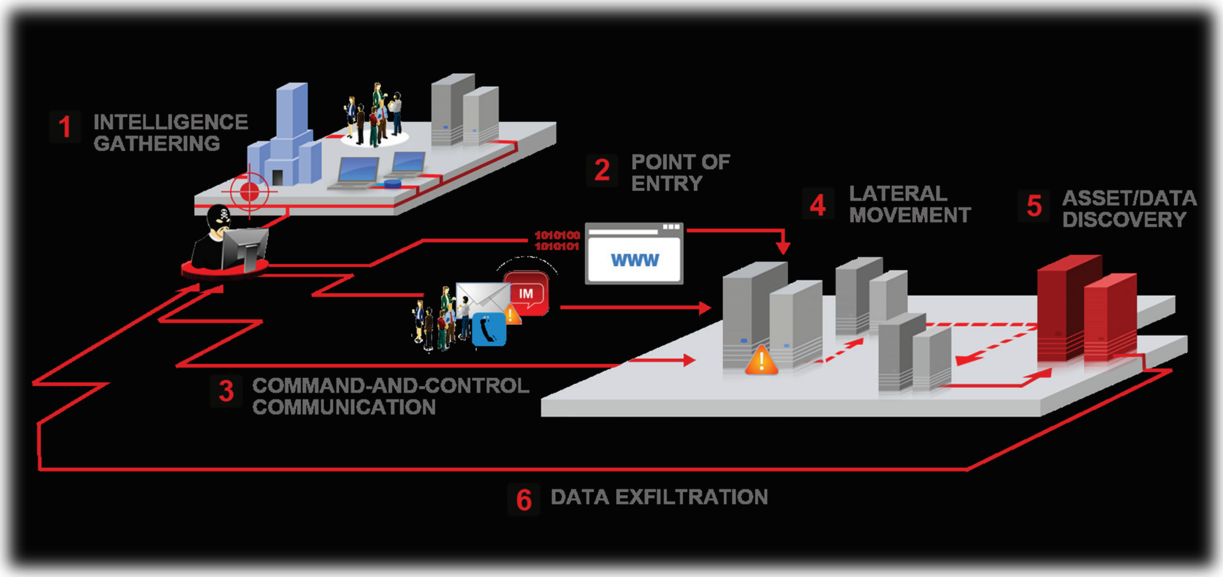
In essence, organizations are well on their way to leveraging virtualization and cloud to improve and increase IT computing resources, but this means that IT managers must proceed with caution. They need to carry out due diligence on technologies and cloud vendors to ensure they know where security is provided and where there are gaps that they need to address themselves. Also, organizations must be prepared to implement strong encryption on all of their data as an emergency failsafe in case their security controls fail to prevent a data breach.[9]

[9] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_security-threats-to-datacenters.pdf

ACTION 7

ACTION 7: Understand the steps of a targeted attack

Reaching Action 7 in this 10-step Action Plan, we have begun to establish a better understanding of our own situation, piecing together a situational analysis that looks at people, technology and context, both of our value and of our vulnerabilities. It is now time to look closely at targeted attacks and break-down the steps of the attackers to understand their purpose and importance, to help us establish a better defense.



Advanced persistent threats (APTs) refer to a category of threats that pertain to computer intrusions by threat actors that aggressively pursue and compromise chosen targets. APTs are often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target's network—and are thus not isolated incidents. In addition, while malware are typically used as attack tools, the real threat is the involvement of human operators who will adapt, adjust, and improve their methods based on the victim's defenses.

How do targeted attacks occur?

Step 1 - Intelligence gathering: Highly similar to a military reconnaissance mission, this initial phase aims to gain strategic information not only on your IT environment but also on your organizational structure. The information gathered can range from the business applications and software you utilize to the roles and relationships that exist within your organization.

Step 2 - Point of entry and compromise: Attackers typically leverage the most common form of office communication, email, as the delivery mechanism for the initial point of entry to your network. However, instant-messaging and social networking platforms are also being utilized to entice your users to click a link or download malware. Armed with knowledge obtained from the intelligence gathering stage and supplementary insights accumulated from prior attacks to your environment, threat actors are able to select and specify the exploits to use that will **work best to compromise your unique environment.** At the end of this stage, a company's network is infiltrated.

Step 3 - Command-and-control (C&C) communication: After an organization's perimeter has been breached, continuous communication between the compromised host and the C&C server needs to be preserved. Threat actors use techniques to maintain C&C communication traffic under the radar often either by blending in with legitimate traffic or fully utilizing go-betweens.

Step 4 - Lateral movement: Once assured that they have achieved constant access to your breached network, threat actors then laterally move throughout the network, seeking valuable resources that house sensitive information or that enable greater access to your resources.

Step 5 - Asset/Data discovery: Noteworthy assets (credit cards, customer or citizen information like personally identifiable information a.k.a PII) are identified within your infrastructure then isolated for future data exfiltration.

Step 6 - Data exfiltration: The attack's ultimate objective is to transmit information from within your organization's perimeter to a location the attacker controls. Data transmission can be done either quickly or gradually wherein information is moved to a staging phase then prepared for exfiltration.

Excerpt from U.S.-China Economic and Security Review Commission Hearing on "Developments in China's Cyber and Nuclear Capabilities" Submission by Nart Villeneuve, Trend Micro, March 26, 2012

While there have been a lot of accusations of "hype" surrounding APT, the problem is severely understated, not overstated. Instead of focusing on the effect of these attacks, most are concerned with the level of "sophistication" and debate whether these attacks are "advanced" or not. I would like to emphasize three key points:

- Targeted malware attacks are extremely successful. The scope of the problem is truly global, extending far beyond the US. It affects governments, militaries, defense industries, high tech companies, the energy and finance sectors, inter-governmental organizations, non-governmental organizations, media outlets, academic institutions, and activists around the world.
- Targeted malware attacks are not isolated incidents of "smash and grab" attacks. They are part of consistent *campaigns* aimed at establishing a persistent, covert presence in a target's network so that information can be extracted as needed.
- Targeted malware attacks are not well understood. However, careful monitoring can leverage mistakes made by the attackers that allow us to get a glimpse inside their operations. Moreover, these malware-based espionage campaigns can be tracked over time through a combination of technical and contextual indicators but this information is not often made public.

By understanding the multi-facets of a targeted attack, and remembering that online markets exist where attackers can easily and readily purchase exploit kits designed to target the exact systems that comprise our networks, we begin to understand that these custom attacks require custom defense mechanisms—**custom defenses unique to our organization.**

ACTION 8: Act like your adversaries - find your own backdoors

ACTION 8

You are reading this paper because you are looking for ways to:

a) combat threats that are targeted at your network, your data, and your people;
b) reduce your risk of damage and data loss from APTs and targeted attacks;
c) gain network-wide visibility with continuous tracking and reporting on your true security posture;
d) measure and prioritize your risk exposure with full characterization of discovered threats and risk factors;
e) enable rapid containment and response with faster recovery with actionable intelligence and security updates.

Action 8 challenges us to address above items c) and d) in a way that considers the six-step, persistent approach used by threat actor. It challenges us to be as persistent in our defense as the attackers and to achieve a new level of situational awareness consistently, across our networks, including extending to BYOD and other devices expanding our threat surface.

Standard perimeter and endpoint security technologies are essential to prevent most attacks and, at their best, may detect or block certain aspects of an APT or a targeted attack. Vulnerability exploits are a key tool of attackers and a proactive stance to vulnerability detection and timely patching is critical. A systematic approach to vulnerability management must match the systematic approach attackers take to vulnerability exploits. Proactive virtual patching or vulnerability shielding strategy will minimize the window of opportunity for attackers. However, frequent penetration testing, and applications scanning must become regular activities for your organization so that you can attempt to locate and close your backdoors before our adversaries. In fact, many security-conscious organizations are beginning to implement their own security lab, or testing ground where they can release captured malware, in a safe environment to be able to track the malware behaviour and analyze its intent. These internal security labs work best when they can leverage sandboxing technologies that can mimic and replicate the exact organization environment.

ACTION 9

ACTION 9: Expand your threat intelligence

The advanced techniques cyber criminals are using to maintain and sustain their perch and control within a victim organization enables them to exfiltrate (steal) data with stealth and precision. These are new and sophisticated threats which require an advanced persistent response predicated on organizations gaining advanced situational awareness in real-time. Firms need to be able to spot the unwanted intruder and then increase the level of discomfort to the point where the adversary flees in search of easier prey.

Gaining this kind of advanced situational awareness requires organizations to look both outside and inside their networks. Firstly, they need to grasp the importance of big data analytics to correlate and associate the various nuances of cyber crime campaigns occurring in the wild with what's going on inside the network. This kind of smart data modelling and analysis should be able to spot if there are any correlations between cyber attack activity on the Internet and an organization's IP addresses, users, domains and networks, giving them the information they need to act.

The Trend Micro™ Smart Protection Network™, for instance, provides Trend Micro products with the broadest and most up-to-date threat detection capabilities. The Smart Protection Network processes over 4TB of data daily, including daily analyses of over 8 billion URLs, 50 million email samples, 430,000 file samples, and 200,000 IP addresses.[10]

Secondly, organizations need to focus on multi-level rule-based event correlation of the sort featured in Trend Micro's own APT-hunter tool **Trend Micro Deep Discovery**. It's another vital piece of functionality in the armor designed to spot unusual activity.

[10] http://www.trendmicro.com/us/technology-innovation/our-technology/smart-protection-network/index.html

Action 10: Put threat intelligence in effect to improve your security posture

ACTION 10

By design, APTs are able to evade standard perimeter and endpoint defenses. Industry analysts and experts have made a clear case that an expanded and layered definition of security due diligence is now a must for most enterprises and government organizations. Trend Micro provides a range of solutions that allow organizations to meet these new requirements, combating APTs with the best protection and proactive detection technologies.

Trend Micro is leading the industry with specialized detection and intelligence that provides a custom defense specifically designed to discover and protect your organization from APTs. The Custom Defense solution from Trend Micro is comprised of a set of security tools that enables you to detect, analyze, immediately adapt, and rapidly respond to the threats that matter most to you because targeted attacks are just that – targeted specifically at you, your people, your systems, your vulnerabilities, and your data.

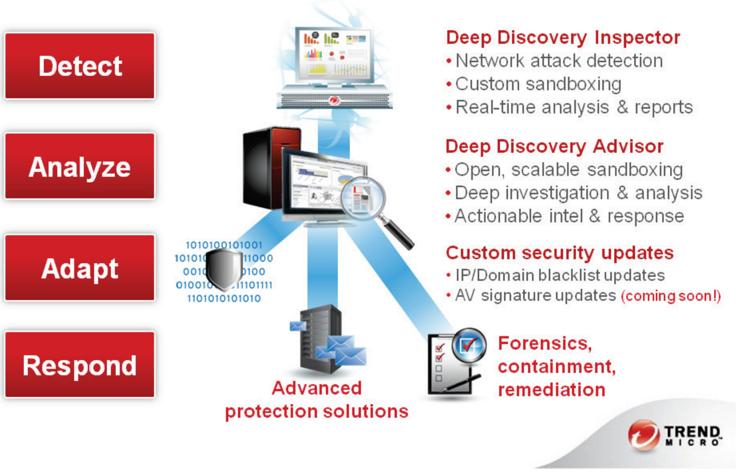
Trend Micro Deep Discovery

Trend Micro Deep Discovery is at the core of the custom defense. It monitors your specific environment, uses detection methods tailored to your specific host configurations, leverages deep threat analysis to generate custom updates to your protection points and provides the custom-tailored and relevant intelligence to guide your rapid response. Its specialized network inspection engines and custom sandbox simulation identify zero-day malware, malicious communications, and attacker activities that are invisible to standard security defenses.

With Deep Discovery your organization will be enabled to detect, analyze, adapt and respond to the attacks that matter to you – those that are targeted at your organization.

Trend Micro Deep Discovery provides you with the network-wide visibility, insight, and control you need to combat APTs and targeted attacks. Deep Discovery uniquely detects and identifies evasive threats in real-time, then provides the in-depth analysis and relevant actionable intelligence that will equip you to assess, remediate, and defend against targeted attacks in your organization.

Trend Micro Deep Discovery:
At the Heart of the Custom Defense Solution


Detect
Analyze
Adapt
Respond
Deep Discovery Inspector
• Network attack detection
• Custom sandboxing
• Real-time analysis & reports
Deep Discovery Advisor
• Open, scalable sandboxing
• Deep investigation & analysis
• Actionable intel & response
Custom security updates
• IP/Domain blacklist updates
• AV signature updates (coming soon!)
Forensics, containment, remediation
Advanced protection solutions
TREND MICRO

The Deep Discovery solution is comprised of two components.

- The Deep Discovery Inspector provides network threat detection, custom sandboxing and real-time analysis and reporting.
- The optional Deep Discovery Advisor provides open, scalable sandbox analysis, visibility to network-wide security events, and security update exports—all in a unified intelligence platform.

Deep Discovery Inspector

Deep Discovery Inspector provides network traffic inspection, advanced threat detection and real-time analysis and reporting—all purpose-built for detecting APT and targeted attacks. It uses a 3-level detection scheme to perform initial detection, then sandbox simulation and correlation, and finally, a cross-correlation to discover "low and slow" and other evasive attacker activities discernable only over an extended period.

Specialized detection and correlation engines provide the most accurate and up-to-date protection aided by global threat intelligence from Trend Micro™ Smart Protection Network™, and dedicated threat researchers. The results are high detection rates, low false positives, and in-depth incident reporting information designed to speed up the containment of an attack.

Advanced Threat Detection

Deep Discovery Inspector focuses on identifying malicious content, communications, and behavior indicative of advanced malware or attacker activity across every stage of the attack sequence using a non-intrusive, listen-only inspection of all types of network traffic.

- Dedicated threat engines and multi-level correlation rules deliver the best detection and minimize false positives
- Virtual analyzer uses custom sandbox simulation to provide additional detection and full forensic analysis of suspect content
- Smart Protection Network intelligence and dedicated threat researchers provide continually updated detection intelligence and correlation rules to identify attacks

Threat Tracking, Analysis, and Action

The Deep Discovery Inspector console provides real-time threat visibility and deep analysis in an intuitive format that allows security professionals to focus on the real risks, perform forensic analysis, and rapidly remediate issues.

Real-Time Threat Console

Places threat visibility and deep analysis at your fingertips

- Quick access widgets provide critical information at a glance
- In-depth analysis of attack characteristics, behavior, and communication
- GeoTrack identifies the origins of malicious communication

Watch List

Delivers risk-focused monitoring of high severity threats and high value assets

- Focused tracking of suspicious activity and events on designated hosts
- Hosts to be tracked determined via threat detection or customer selection
- Detailed event timeline tracks all attack activities involving target hosts

Threat Connect

Provides the threat intelligence you need to understand and remediate an attack

- Direct access to Trend Micro intelligence portal for a specific attack or malware
- Detailed threat characteristics; containment and remediation recommendations
- Direction to available antivirus/other signature updates for this threat

SIEM Management

Integration with leading SIEM platforms delivers improved enterprise-wide threat management from a single SIEM console

- Network detections, confirmed incidents, and contextual data are reported to SIEM
- Deep network visibility enhances correlation and multi-dimensional attack profiling of SIEM
- Enterprise-wide threat management provided by SIEM as the central console

Flexible, High-Capacity Deployment
Deep Discovery Inspector features a high-performance architecture designed to meet the demanding and diverse capacity requirements of customers of all sizes. The product is available on a full range of hardware, software, and virtual appliances supporting multi-gigabit corporate backbones down to remote office locations.

Deep Discovery Advisor

Deep Discovery Advisor provides open, scalable custom sandbox analysis, visibility to network-wide security events, and security update exports—all in a unified intelligence platform. The Advisor augments the analysis power of Deep Discovery Inspector and enables the adaptive protection and rapid response capabilities of the Custom Defense.

Threat Analyzer
The Threat Analyzer is an optional component designed to offer in-depth simulation and analysis of potentially malicious sample files, including executables and common office documents. It can augment and centralize the simulation of Deep Discovery Inspector, as well as provide advanced detection and analysis security for professionals or any security product or service via an open web services interface.

- In-depth threat simulation, and analysis uses sandbox simulation and other advanced detection engines to classify and deeply analyze submitted files
- Custom sandbox execution environments allow the customer to create and analyze multiple fully custom target images that precisely match their host environments
- Scalable architecture supports incremental capacity that ranges up to 50,000 samples/day
- Open, automated, and manual submission supports input from security analysts, as well as automated submission and results loopback by Trend Micro products and third-party or custom products
- Integration with Deep Discovery Inspector and other Trend Micro products provides expanded detection and analysis options to customers

Threat Intelligence Center
The Threat Intelligence Center is a complete analysis environment for event data from the threat analyzer, as well as security events and logs collected from Deep Discovery Inspector, other Trend Micro products, and third-party solutions. Using these sources and integrated Threat Connect intelligence, Threat Intelligence Center provides in-depth insights to drive risk-based incident assessment, containment and remediation.

- In-depth analysis of incidents, and events using automated analysis, visualization, and advanced search and investigation tools
- Risk-focused monitoring and investigation
- Network-wide security event collection of events/logs from most Trend Micro and third-party products ensures a full risk assessment and effective containment and remediation measures
- Threat Connect intelligence is automatically integrated into analysis results, providing detailed threat characteristics and context-relevant intelligence for containment and remediation
- Deep Discovery Inspector centralized reporting consolidates detection results from multiple Deep Discovery Inspector units into a single dashboard and customizable reports
- SIEM connect with leading platforms delivers improved enterprise-wide threat management from a single SIEM console

CONCLUSION

Today's targeted, custom attacks require advanced, custom defenses

This paper outlined ten steps essential for creating an effective action plan to defend against targeted attacks and APTs. These steps will help you to consider your current situational awareness, level of preparation and operative ability to ward off a persistent attacker. These steps include actions to implement the specialized detection and intelligence activities that are key to defending against targeted attacks and APTs.

Trend Micro Corporate Overview

Securing the Journey to the Cloud. As a global leader in cloud security[11], Trend Micro develops innovative security solutions that make the world safe for businesses and consumers to exchange digital information. As the largest independent security vendor[12], with 23+ years of dedicated security expertise, we're recognized as the market leader in server[13] and virtualization security[14] and for delivering top-ranked endpoint, network, and cloud-based solutions. Trend Micro's technology is proven to stop threats faster[15], provide increased performance, and give the visibility and control required to confidently share and protect data in physical, virtual, cloud and mobile environments. No matter what the security need, or how it may evolve over time, Trend Micro is the smart security choice as people journey to the cloud.

A History of Innovation. Since 1988, Trend Micro has pioneered innovative technologies and security services that protect users against threats that target new and emerging platforms and devices. Each beneficial shift in the way people communicate and conduct business online has introduced new security challenges. Trend Micro has been there from the start, being the first to extend threat protection from the desktop to the server and then to the Internet gateway. And as mobility, virtualization, and cloud computing are enabling people to share digital information more easily, more quickly, and more affordably, Trend Micro continues to innovate with mobile device management, data encryption, agentless anti-malware and mobile app reputation technology.

[11] Source: 2010–2014 Technavio – Global Cloud Security Software Market

[12] Source: 2011 © Quocirca Ltd.: Selected independent IT security vendor revenues

[13] Source: 2011 IDC–Worldwide Endpoint Security Revenue Share by Vendor, 2010

[14] Source: 2011 Technavio – Global Virtualization Security Management Solutions

[15] http://www.trendmicro.com/us/technology-innovation/our-technology/competitive-benchmarks/index.html