
TREND MICRO
Preparation against Advanced Targeted Attacks
For IT Managers
10-Steps
Bonus - Targeted Attack Checklist Included

Understand your organization's readiness against targeted attacks

— Best Practices for Combating Targeted Attacks —

Step 1

You hold the key

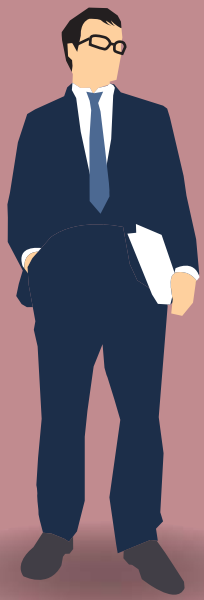
The IT manager holds the key in defending against targeted attacks. Where do you begin? Start by recognizing your organization's current status. Within a few minutes, you'll be able to take your first steps in building a strategy against this new threat.

Executives and senior management lack the understanding of this new threat landscape. Your IT staff are busy operating and maintaining existing security controls. It's up to you to take the lead in preparing your organization against targeted attacks.

You must understand how these targeted attacks are different from previous threats, and why existing security controls are inadequate against the tactics used by cyber criminals.

You'll be confronted with a myriad of products and technologies that claim to address this new threat. Therefore, understanding the problem and challenges is paramount to identifying the appropriate set of solutions that fit your organization.

By using this booklet and a few minutes to survey your company's readiness, you'll be able to take your first steps in creating a custom defense against the customized attacks that are targeted at your people, your network, your systems, and your organization.



Targeted Attacks: Level of Understanding and Organizational Readiness

Self-Assessment Checklist

Q1	Do you understand the various tactics used by cyber-criminals and in advanced targeted attacks?	☐ YES ☐ NO

If you answered "No", go to page 3, 4, 5 ▶ ▶

Q2	Do you know why existing security controls can´t step up to the challenge of targeted attacks?	☐ YES ☐ NO

If you answered "No", go to page 5, 6 ▶ ▶

Q3	Has your organization conducted any training for IT staff and educating employees about targeted attacks?	☐ YES ☐ NO

If you answered "No", go to page 7, 8 ▶ ▶

Q4	Do you know what technology or solution is most effective in addressing targeted attacks?	☐ YES ☐ NO

If you answered "No", go to page 9, 10 ▶ ▶

Q5	Does your organization have a mechanism for detecting unauthorized communications on your network, and is your network monitored for malicious activities?	☐ YES ☐ NO

If you answered "No", go to page 9, 10, 11 ▶ ▶

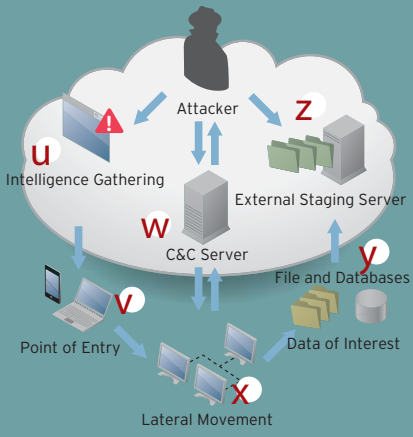
— Best Practices for Combating Targeted Attacks —

Step 2

The anatomy of a targeted attack

Socially-engineered. Customized. Stealthy. Targeted attacks begin with intelligence gathering of targeted individuals on social networks. Once penetrated, attackers establish and maintain a persistent foothold of your network.

1. **Intelligence Gathering:** Identify and research targeted individuals on social networks (LinkedIn, Facebook, etc...), in preparation for a spear-phishing attack.
2. **Point of Entry:** The initial compromise typically involves spear-phishing and/or waterhole attacks - delivering customized zero-day malware (via email/IM or drive-by-download). A backdoor agent is installed on compromised systems and can be remotely controlled.
3. **Command & Control (C&C) Communication:** C&C Communication allows the attacker to take control over the compromised systems remotely, and backdoor agent to update or modify its capabilities, for subsequent attack activities or to evade detection.
4. **Lateral Movement:** Once inside the network, an attacker performs reconnaissance of your network, compromises additional machines, steals credentials, and escalates access privilege levels.
5. **Asset/Data Discovery:** Several techniques (ex. Port scanning) are used to identify the noteworthy servers and services that house the data of interest. DNS and Directory Services are prime targets.
6. **Data Exfiltration:** Once sensitive information is gathered, the data is funneled to an internal staging server where it is compressed and encrypted for transmission to external locations.*



*Data exfiltration will probably continue until you or someone notices it.

— Best Practices for Combating Targeted Attacks —

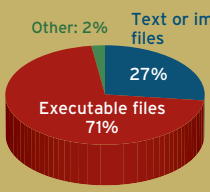
Step 3

Identify persistent footholds

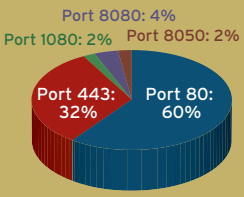
Targeted attacks are stealthy in nature. Cyber criminals attack in such a way that you don't notice either the attack or the theft of information. Why is this?

Being a profitable corporation or a nation state means being in competition. In other words, you are always a possible target for attacks. The moment when someone pays for or sponsors an attacker either from within or from outside your country, it may be the moment when an attack starts. Or it may have already begun.

Attackers are patient and spend an extended amount of time penetrating and monitoring without being noticed. For example, they may use a stealthy technique and disguise an executable file with a malware as a Word file. Another tactic is using a common port (i.e. port 80, 8080, or 443) to transmit instructions to their backdoor agents through what appears to be legitimate web traffic. Often the backdoor agents stay dormant for an extended period of time and only awake briefly when instructed to carry out certain activities. Why do attackers conceal their existence? It is to maintain persistent footholds of your networks – the ability to access your network, and siphon confidential data on-demand. And the result? Perhaps copies of your company's leading products start to circulate around the market, or your company continues to lose revenue for some unexplained reason, and on top of that it could lead to some kind of scandal.



Attachments used by attackers – broken down by type
[Trend Micro study – 2nd half of 2012]



Breakdown of ports used by malware
[Trend Micro study – 1st half of 2012]

— Best Practices for Combating Targeted Attacks —

Step 4

Gaps in existing security controls

Over the last 20 years, we've been focused on perimeter security – building a moat or a wall around our castle (datacenter). Whatever is outside of the perimeter is considered bad; and whatever is inside, we assume is good.

In the mobility and cloud era, organization's IT perimeter demarcation has diminished. Not to mention tactics used (spear-phishing, man-in-the-middle, waterholing) in targeted attacks are leveraging protocols that punch through firewalls. Antiviruses are ineffective because attackers are customizing and testing the malwares against the latest signatures and scan engines of the victim's antivirus solutions, before unleashing them.

IPS with rules to detect network traffic anomalies are failing because attackers are patient and avoid generating excessive network activities.

Attackers also bet on the fact that organizations can't deploy patches whenever vulnerabilities are announced by software suppliers, due to changes in management. It usually takes 1-3 months of standard operating procedures before patches can be deployed after compatibility testing against mission critical and sometimes custom applications.

Lastly, network security solutions have placed too much emphasis on ingress traffic, and failed to provide visibility of internal lateral movement activities.

— Best Practices for Combating Targeted Attacks —

Step 5

Look within your perimeter

Detecting targeted attacks are getting more difficult with existing security controls, as outlined in earlier chapter. Within all the events that are logged within your network each day, a single innocent event can hint at a large-scale attack...

Similar to the profiling of a criminal investigation, you cannot overlook single events. Perhaps an employee experiences system performance issues on his PC, and takes them to his IT helpdesk for a quick look. Upon evaluation, the IT system administrator logs into that PC and runs a routine scan for viruses. A few days later, the same PC's firewall log shows traces indicating that an attempt had been made to communicate with the outside without going through the HTTP proxy, and the communication is denied. Several weeks later, the scheduled scan of an antivirus solution detects a backdoor agent and automatically deletes it. Then, late one night over the weekend, a number of failed login events get recorded on an Active Directory server log.

These events seem to be merely "warnings" which mean nothing individually. However, when an expert sees them, they form a "timeline" showing a history of a surgical attack. The latency of the PC was made intentional; and the infected PC was a trap that was set in order to gain administrator privileges.

Targeted attacks are conducted over time, gradually and stealthily. Using every possible means, attackers never give up until they reach their goal. You and your staff need to keep up with the targeted attack tactics, improve your ability to detect and analyze advanced threats, and find an expert partner to be on your side.

•The Trend Micro Custom Defense Strategy provides you with advanced threat detection and customized threat analysis.

http://apac.trendmicro.com/apt

The importance of internal education

— Best Practices for Combating Targeted Attacks —

Step 6

Educate your weakest link

An employee opens an email from his/her boss, and clicks on the attachment… and at that exact moment the entire company may be exposed. Do you have a program for educating employees about cyber security – not just your IT staff?

According to a Trend Micro survey*, 62.3% of companies understand the tactics behind targeted attacks, but only 40.2% reported having some kind of cyber security education program for their employees. According to the Verizon Data Breach Investigation Report 2013, it's not the IT-savvy developers or administrator that were responsible for most of the data breaches, but customer service staff like call centers and end users.

Carelessness of just one employee could expose the entire company to a targeted attack. That means that every single employee needs to be aware and understand the company's security policies and guidelines.

Who should be responsible for educating and communicating to employees about cyber threats and corporate IT security policies? Is that the role of IT or HR? Employee education and communication may be HR's responsibility; however, HR certainly would not know how to initiate a training program around cyber security. If you feel that your company's awareness for cyber threats is low, start to set up a security awareness program with your HR department.

Who is responsible for the regular patching of your OS and applications? Have you considered all possible countermeasures available to your organization?

Companies carrying out user education on targeted attacks:	**40.2%**
Companies that have dedicated resources in place to deal with incidents:	**29%****
Companies not regularly applying OS patches, or not using alternative means such as IPS:	**38.3%**

*Source: Trend Micro security assessment tools survey "Cyber Attack Countermeasures", October 2012

**The SANS Survey of Digital Forensics and Incident Response, July 2013

— Best Practices for Combating Targeted Attacks —

Step 7

Get executive buy-in

You will no doubt be aware of the need and difficulty in articulating the seriousness of targeted attacks to senior management. It may be difficult to build a tangible ROI justification or to explain why existing security controls are inadequate. Perhaps the proof of a competent IT manager includes the ability to influence and persuade your boss.

Most executives and board members don't fully understand the seriousness of a security or data breach until it actually hits them. This is evident in the size of the IT security budget in comparison to the overall IT spending for most organizations.

While it may be difficult to demonstrate the ROI for additional IT security investment, you must articulate how these targeted attacks are different than previous threats, why existing security controls are inadequate, and why the risk posed by a targeted attack is significantly higher.

The proof that targeted attacks pose a higher risk argument is very evident. In 2012, over US$66 billion were spent on IT security worldwide. Yet, data breaches continue to plague enterprises such as Citibank, Sony, RSA, Google and Epsilon, just to name a few. Not to mention the covered-up breaches in the government sector.

In a recent Trend Micro survey, 100% of the companies surveyed reported traces of an attack, and 85% responded that they detected "threats with a high level of danger". You no longer can afford to assume that this won't happen to your organization. And once confidential information or intellectual property is compromised, the tangible and intangible damage is insurmountable. Therefore, persuading senior management and getting them on your side is your mission as an IT manager.

— Best Practices for Combating Targeted Attacks —

Step 8

There's no silver bullet

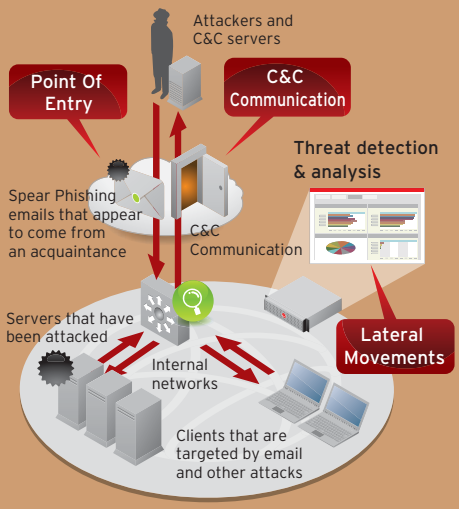
There's no silver bullet against targeted attacks. You'll be foolish to think that you can go out and buy a product or technology, thinking you have this problem solved.

To define what you need, you must understand the phases and tactics used in a targeted attack. Let's start with these:

•**Point Of Entry** (spear-phishing and waterhole attacks) involves initial system/PC compromise and installation of backdoor agents. 95% of targeted attacks involve some kind of spear-phishing and malicious documents; therefore, blocking spear-phishing attacks is half the battle. You need the ability to analyze malware in a customizable sandbox environment to extract additional intelligence on the nature of this attack.

•**C&C communication** is a critical component which allows an attacker to remotely control devices on your network to carry out an attack. Detecting C&C communication in your egress traffic is essential.

•**Lateral movements** take place within your network and your systems. It involves credential stealing, vulnerability exploitation, and making unauthorized changes on your critical systems. You require visibility and monitoring of these activities.



Once you understand how a targeted attack is carried out, it's easy to see that there is no silver bullet, and organizations need to take a holistic but concise approach.

Choose tools that complement existing security investments

— Best Practices for Combating Targeted Attacks —

Step 9

Integrate and adapt

A well-defined solution against targeted attacks requires a wide range of products and services, working hand-in-hand to detect, analyze, adapt and respond to an attack.

"Can't we still leverage our existing security products?" That is probably on the top of most people's minds at this point in time. And it will likely come up during your proposal to senior management. If integrating the new solution with the existing products delivers higher protection, then that can be a huge upside in the justification discussion.

Ideally, new sets of products need to integrate with existing security controls seamlessly.

For example, detection of potential penetration at web and mail gateways can be enhanced by integrating sandbox and document exploitation detection with existing gateway security products.

Threat intelligence such as malicious URL or IP addresses of C&C servers gathered from the analysis of zero-day malware, in the sandbox; can feedback directly to existing firewall, switches, proxy servers and endpoints for immediate protection.

Network security and datacenter security shouldn't work in isolation. Logs from attempts of unauthorized changes on a server should be correlated with brute-force attacks and vulnerability exploitation attempts. In addition, local services and support systems should be on-call to assist with incident response or to develop custom signatures for endpoint cleanup.

Moreover, if you can integrate services and support from experts to assist with security advisory, 24x7 monitoring and alert, and incident response; then you can be certain that your organization has defined a comprehensive strategy against targeted attacks.

•For more detailed information, please visit the Trend Micro Custom Defense webpage.

http://apac.trendmicro.com/apt

Lastly...

— Best Practices for Combating Targeted Attacks —

Step 10

Assume compromise

Advanced targeted attacks have changed the threat landscape. Prevention is no longer possible, and we must assume we'll be compromised. With a shift in this mental model, we have to redefine our security strategy. The Trend Micro Custom Defense Strategy clearly articulates the problems and provides a clear prescriptive answer. For more information, please contact Trend Micro.

TREND MICRO is a registered trademark of Trend Micro Incorporated. Copyright©2013 Trend Micro Incorporated. All rights reserved.

TREND MICRO™

Securing Your Journey to the Cloud

Trend Micro Incorporated.
Contact your regional Trend Micro office for further inquiries.

Trend Micro Continental Europe
Schalienhoevedreef 20H
2800 Mechelen
Belgium
T + 32 15 281 480
www.trendmicro.be

Trend Micro Eastern Europe
Mooslackengasse 17
A-1190 Vienna
Austria
T +43 1 230 60 3535
www.trendmicro.eu\ee

Trend Micro Netherlands
Lange Dreef 13H
4131 Vianen
Netherlands
T + 31 347 358 430
www.trendmicro.nl

Trend Micro Poland
Warsaw Trade Tower
Chłodna 51
00-867 Warszawa, Poland
T +48 22 486 34 50
www.trendmicro.pl