A **TrendLabs** Security in Context Paper

TREND MICRO™

The Enterprise Fights Back (Part I)

Securing Your Network Infrastructure Against Targeted Attacks

Laying the Groundwork for Compromise

Targeted attacks often employ tools and routines that can bypass traditional security and allow threat actors to move deeper into the enterprise network. Threat actors do this to access data and obtain higher privileges that will allow them to steal additional information of interest. Because of the nature of targeted attacks, unprepared information technology (IT) administrators can fail to immediately detect these attacks and end up with unseen adversaries in their network.

To prevent this, enterprises should establish a series of rigorous, security-related procedures. These include segmenting the network, logging and log analysis, and ensuring that user accounts and workstations are configured properly.

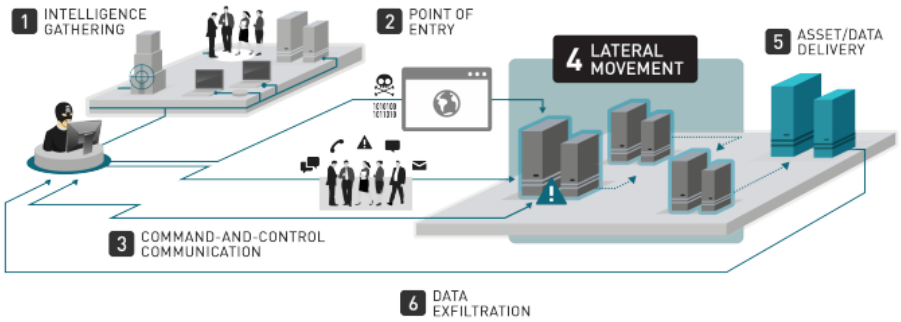

Figure 1: Stages of a targeted attack

Letting Targeted Attacks In

That security breaches only happen to large companies instead of small and medium-sized is a common misconception. In reality, threat actors can find weaknesses in a wide range of targets regardless of business size or industry.

As threat actors target various types of networks, companies with improperly configured network infrastructures risk the following repercussions:

Stolen Credentials and Brute-force Attacks

Depending on information they already have and their goal, threat actors may seek to escalate privileges once inside the

enterprise. Though this is not always needed for threat actors to advance, having login credentials and similar information can still help them go deeper inside the network, like in internal-only servers and databases.

Therefore, threat actors will need to find a way to steal user names and passwords that will help them to move from one computer to another. Tools like keyloggers and techniques like ARP spoofing and hash dumping, are all different methods used by threat actors to accomplish this[1].

Late Detection of Compromise

We can remember that the GhostNet cyber-espionage network revealed in 2009 had compromised over 2,000 computers in 103 countries. The network established persistent control of these computers on an average of 145 days, with the longest being 660 days.

Unauthorized Access to Sensitive Corporate Data

Networks that are not properly configured, for instance by segments or user access, open the entire corporate infrastructure to data theft. In case of compromise, this means that the whole network is open to malware and other routines that can record keystrokes, hear meeting audio, copy banking credentials, steal classified information, and more.

These can contribute to bigger company problems like losing competitive advantage, suffering from a ruined reputation, and losing money.

Disrupting the Attack Process

As the nature of targeted attacks involves staying hidden in a network, predicting and thwarting their steps along the way is one effective way you can help secure the company network.

[1] Trend Micro Incorporated. (2013). TrendLabs Security in Context Paper. "Lateral Movement: How Do Threat Actors Move Deeper into Your Network?" Last accessed October 2, 2013, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf

Traditional blacklisting or perimeter-based security fails in stopping these threats. The diagram below shows critical points which IT administrators can configure to fuel a custom defense strategy for real-time detection.

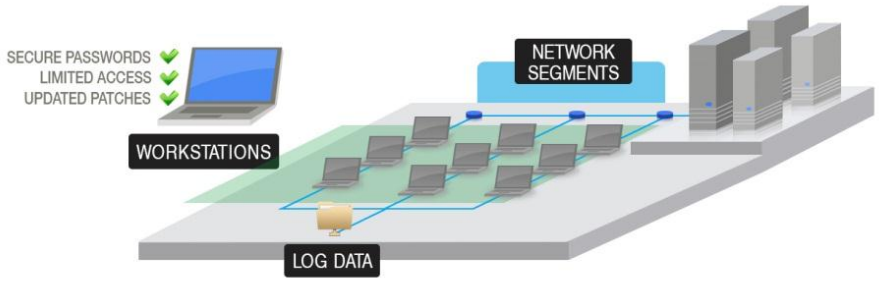

Figure 2: Ways to secure network infrastructure for the enterprise network

Here are the main items that should be on every security checklist:

"Sharp analysts who understand the daily ebb and flow of your traffic may be able to detect a targeted attack early enough in the process to thwart it before it has a chance to take root and spread."

– Jim Gogolinski, senior threat researcher

Network Segmentation

This involves breaking down a corporate network into separate and logical segments. Segments may be separated according to function or department, geographical location, or levels of security, such as classified or top-secret information.

As each segment is usually separated by firewalls, the local IT department can monitor, contain, and control the network traffic coming in and out of each one. Establishing segments helps minimize the impact of compromise using stolen credentials, brute-force attacks, or insiders that snoop on confidential data.

Log Analysis

Logging—and analyzing those logs—is critical in detecting targeted attacks. This allows the response team to understand which areas the attackers infiltrated or stole data from. These data can be fed into technologies like the security information and event management (SIEM) and security event manager (SEM) which can gauge the health and activity of large corporate environments in real time.

Despite the continuing storage and costing issues, log data can be helpful especially when tracing a successful data exfiltration or tracing lateral movement inside your network. Additionally, log data helps in building the company's security intelligence by learning about new possible tactics.[2]

User Accounts and Workstations

User access to company resources is often taken for granted. It is common for employees to have their own accounts and workstations but enterprises need to configure the access of each one to minimize the impact of targeted attacks. The least-privilege model works best in this case as it regulates the amount of information that users can access.

It is imperative that those in charge of network security develop the mindset and tools needed to guard the network and the sensitive data within. Given the evidence discussed, it is high time to defend against targeted attacks and campaigns that aim to steal your company's crown jewels. As such, the first step is to configure your network infrastructure in a proactive stance against targeted attacks.

Trend Micro senior threat researcher Jim Gogolinski details important guidelines for network administrators about securing the network infrastructure in his paper "Suggestions to Help Companies with the Fight Against Targeted Attacks."

[2]Trend Micro Incorporated. (2013). *TrendLabs Security in Context Paper*. "Data Exfiltration: How Do Threat Actors Steal Your Data?" Last accessed October 2, 2013, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/how_do_threat_actors_steal_your_data.pdf

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud