A TrendLabs℠ Primer

A Proactive Approach to Securing the Network from Targeted Attacks

Despite continuing advances in modern enterprise security, many organizations are unable to handle the effects of targeted attacks. While traditional security has become proficient at handling more traditional threats, targeted attacks can often bypass even the most advanced security software by using sophisticated tools and tactics designed to allow the attackers access to sensitive data as well as network privileges.

Preventing the often devastating consequences of targeted attacks generally requires dealing with threats before they can enter the network. This means that organizations need to focus on proactive threat detection, which includes implementing strategies such as network segmentation, logging and analyzing the traffic coming to and from the network, and ensuring all parts of the network are updated and properly configured. The goal for network administrators is not to deal with attacks after they have already occurred but to prevent it from occurring by making it difficult for attackers to gain access to the network — something that can be accomplished by an incident response strategy that involves proactive detection and response to threats within the network.

The Risks of Targeted Attacks

All organizations — from multinational companies with dedicated security teams to medium-sized businesses with IT staff that also doubles as security professionals — can be victims of targeted attacks.

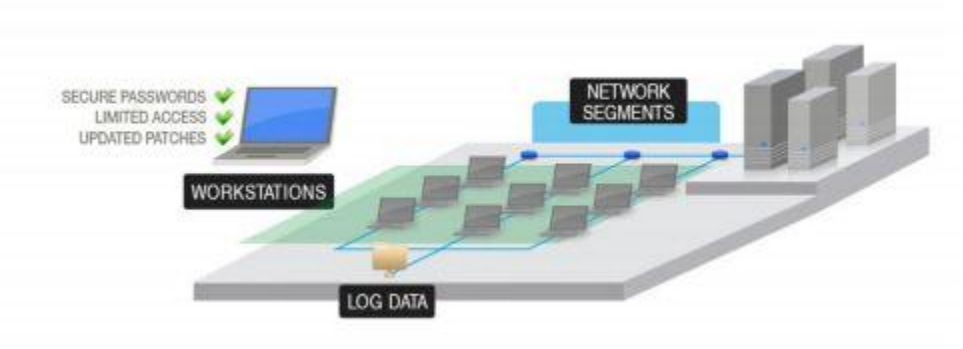
A targeted attack can result in devastating consequences. This is often further complicated by late detection of compromise, when the victim organization learns about the targeted attack after the damage has been done.

Aside from the fact that the organization's network could be at the mercy of the attackers, the most significant risks that could arise from a targeted attack on a poorly secured and configured network include:

- **Stolen credentials.** Threat actors looking to infiltrate deeper into an organization's network will often need credentials that can provide them greater privileges. Thus, one of the common initial goals of a targeted attack is to steal user credentials, usually through a variety of tools such as keyloggers and techniques such as Address Resolution Protocol (ARP) spoofing. Performing brute-force attacks, wherein an attacker can simply guess passwords via a predefined list, is an inelegant but often effective credential theft strategy.

- **Unauthorized access to corporate information.** Targeted attacks are usually conducted as long-term cyberespionage campaigns against the victim organization, and one of the typical goals of these attacks is gaining access to sensitive company information. The immediate consequences, such as stolen data and credentials, are compounded by bigger issues, which may include business disruption, monetary consequences, and reputational damage.

Protecting the Network Infrastructure from Targeted Attacks



While static defenses, including traditional blacklisting and perimeter-based security solutions, are effective against many types of attacks, targeted attacks are designed to slip inside a network stealthily. This is why a proactive approach to security is necessary. Given the massive potential losses that a successful targeted attack can cause, implementing a properly configured and monitored network infrastructure can offset the costs associated with it.

Here are some specific techniques that an organization's IT personnel must implement to maximize its network's security:

Implement network segmentation

Network infrastructures are usually complex, involving many layers of users, servers, workstations, and other connected devices. The more complex the structure, the more it makes sense to break down the individual components into ordered segments. These segments are composed of all devices and workstations that have access to one another. In a scenario where an attacker gains access to the network, network segmentation can help prevent access to every part of the network.

Segmentation can also prevent employees and other organization personnel from accessing parts of the network that they should not be able to access. Networks can be segmented in different ways, such as by department, by location, or by security level. Each segment should be as secure as possible, preferably with a firewall preventing unauthorized systems from accessing it.

Another important aspect of network segmentation is the ability to identify critical assets. Organizations operating in different kinds of industries typically have different kinds of critical assets in their networks. For example, a company that deals in healthcare has its patient records as a critical asset, while a plant that uses industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) most likely counts human-machine interface (HMI) workstations among their critical assets. Accordingly, a

business dealing mostly in online transactions may have their website as its primary critical asset. When creating a comprehensive security strategy, an organization needs to identify the most important or critical parts of their network using risk assessment or other identification techniques.

The next step would be to determine which of the critical assets are most vulnerable to attacks. Critical assets that are of the highest priority within an organization should likewise have the equivalent level of security in place. These can be done via the correct configuration of the network, proper implementation of appropriate security solutions, and sufficient personnel training. Given the significance of these assets, the organization's security team, or at least the department handling security for the network, should know how to detect and mitigate targeted attacks on the network proactively.

Analyze network logs

One of the primary methods for detecting targeted attacks is through the use and analysis of logs. Logging can provide IT and security personnel information on the attackers — how they entered the network, their objectives, and any traces they left behind. In addition, logged information can provide insights into the general activity of the network. Security personnel who have experience in monitoring network traffic can tell if a targeted attack is about to occur by scanning the network for any suspicious activity, allowing them to prevent the attack before it can cause any serious damage. However, it should be noted that logs need to be actively monitored for their use to be effective.

Security solutions such as security information and event management (SIEM) and security event manager (SEM) software can help sift through the data to determine both the health and the activity of large corporate environments in real time. Log data can also provide information on new tools and techniques that threat actors use in their targeted attacks. The most important parts here are the log analysis, the tools that make it possible, and the amount of logs. It is never about the logs and the tools, but both enable log analysis. The amount of logs should enable the security personnel to tell the whole story with just the logs. Not only does log analysis provide new threat intelligence (that is, attacker tactics, techniques, and procedures) but it also allows significant events to float up. For example, low and slow attacks that take a few months to execute can easily get missed as opposed to ongoing daily malware attacks.

User access is often an overlooked aspect of network security. Attackers usually look for user accounts and workstations with weak credentials and security to exploit possible entry points into the network. The situation can easily get worse if a compromised user account also has unlimited access to company data. Placing user accounts under the least-privilege model, which gives accounts access only to parts of the network they need, is one way to minimize possible compromise. The least-privilege model can also help detect suspicious activity. For example, an IT administrator has different privileges from those of a

receptionist. Unusual network activity, such as an IT administrator logging into multiple workstations at the same time, can be a red flag for an ongoing attack.

The use of secure passwords should always be a requirement. This can be strengthened even further with an additional layer of security via the implementation of features such as two-factor authentication (2FA). Users should also change their passwords at regular intervals and refrain from using the same password for different user accounts in the network. User workstations should be kept fully patched and updated, as well as physically locked down when not in use. Each computer should be kept fully patched and have full logging enabled. Certain applications such as integrity monitoring tools can help IT staff detect changes to file systems and registries.

Create an incident response team

In an ideal scenario, an organization would have an incident response team composed of cross-functional members from different departments, including the executive team, the technical staff, the legal department, and the public relations and human resources department, to handle targeted attacks. This group should be separate from the regular IT department and should be trained to address sophisticated attacks that members of the IT department could not handle on their own.

The members of an incident response team should have their own areas of expertise. For example, the technical personnel is in charge of handling attack analysis and determining the motives behind attacks. The public relations group, for its part, will be responsible for creating the messaging strategy for addressing the attacks and providing information to customers, employees, and shareholders. Accordingly, the legal department handles inquiries regarding the legality of any incident response investigation and remediation.

Again, this is in an ideal scenario. The truth is that many organizations simply lack the resources, manpower, and skills to create an incident response team, and may have to source from third-party organizations for their security needs. For example, while typical IT staff members are trained to manage and control the network, they may have minimal experience when it comes to handling attacks — usually relying on traditional security solutions as their main defense against threats. Even in-house security professionals, while having more experience handling network threats, may be overwhelmed when it comes to dealing with more sophisticated attacks. Services with actual professionals who have expertise in advanced threat detection, threat hunting, analysis, and response can help mitigate targeted attacks, as they provide a wide range of skills — from behavioral analysis and impact assessment to damage cleanup and remediation — that form an essential part of a proactive security posture. These services also typically offer 24/7 monitoring and live incident response, allowing security coverage at all times.

An incident response team should only be formed once an organization has its security essentials in order. If the chances of an incident occurring is small, then there is little use of an incident response team. The

reality is this: that many enterprises do not have their essentials in order, and this is why their incident response needs increase.

When considering the high risks that they face with regard to targeted attacks, organizations have to prioritize their network security. Given the sophistication of many modern targeted attacks, it is especially important for companies to adopt a proactive incident response strategy that includes actively hunting and responding to threats and attacks that traditional security solutions may overlook.

Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection.

With almost 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.