TREND MICRO | research

# Understanding Targeted Attacks: Defensive Measures

# Securing the Network Infrastructure

Targeted attacks often employ tools and routines that can bypass traditional security solutions and allow the threat actors to move deeper into the enterprise network. Threat actors do this to access data and obtain higher privileges that enable them to steal information of interest. The kind of information stolen depends strongly on the attackers' motives, which can vary greatly. That security breaches only happen to enterprises and not to small and medium-sized companies is a common misconception. In reality, threat actors can and will attack a wide range of targets regardless of business size or industry.

Because of the nature of targeted attacks, unprepared information technology (IT) administrators can fail to immediately detect these attacks and end up with unseen intruders in their network. To prevent being caught off guard, enterprises should establish a set of rigorous security policies and procedures.

## The Enterprise Security Checklist

As the nature of targeted attacks involves staying hidden in a network, predicting and thwarting their TTPs is an effective way to secure the company network. Here are the main items that should be on every security checklist.

- **Implement 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 firewalls usually separate each segment, 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.

- **Collect and analyze logs.**
  Logging — and analyzing logs — is critical in detecting targeted attacks. It allows the response team to understand which areas have been infiltrated or stolen from. The log data can be fed into technologies like security information and event management (SIEM) and security event manager (SEM) that can gauge the health and activity of large corporate environments in real time. Log data can be helpful for tracing data exfiltration or lateral movement inside your network. It also helps build the company's security intelligence by revealing possible new tactics.

Notably, the use of logs is not only maximized through analysis itself but also by taking into account the number of logs up for analysis. If the volume and sources of logs for analysis are sufficient, security professionals can be equipped to tell the complete story that is happening in the network. For instance, Trend Micro™ XDR goes beyond SIEM and SEM to provide security professionals substantial amounts of logs to analyze as the service integrates detection and response functions across networks, endpoints, emails, servers, and cloud workloads. This way, organizations are provided with a wider scope of visibility across the organization's IT infrastructure, giving security professionals enough information to paint the whole picture of the network environment or of an incident.

- **Strictly manage 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 each account 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. The first step is to configure the network infrastructure in a proactive stance against targeted attacks.

# Protecting Sensitive Data From Targeted Attacks

Detecting targeted attacks at the data exfiltration stage is very challenging for enterprises. It is recommended that enterprises assume compromise, enforce preventive measures, and use an airtight custom defense strategy that can detect threats in real time. It cannot be stressed enough that securing the network infrastructure is the first step in the fight against targeted attacks. The next vital step: protecting valuable data.

- **Classify "core data" from normal data.**
  Every department or business unit should classify the "crown jewels" or mission-critical data — those whose release can negatively affect an organization — from normal day-to-day assets. These include government information, scientific research, and pharmaceutical formulas. Sharing and downloading them must require privileged access. They can be spread across the network to prevent threat actors from getting the whole information with a single intrusion.
- **Establish endpoint-to-cloud protection.**
  PCs, mobile devices, and removable devices should be secured by encrypting files, disk, and removable media. Identity-based encryption solutions can be used to protect emails. Data should also be encrypted when using cloud applications, public or private cloud infrastructure, and virtual environments.
- **Build a data protection architecture.**
  A protected infrastructure requires tiered access, where top-level information pieces are in a disconnected network, second-level ones require a special two-factor authentication process, and third-level ones on regular file servers.

# Building an Incident Response Team

An incident response team is composed of members with various functions, from technical, threat intelligence, human resources, legal, public relations, and executive management. The roles and responsibilities of this group differ from those of the IT team and should be documented and cascaded to every member. Its members should undergo sufficient training to ensure fast response time and efficiency should an attack occur.

Enterprises should form an incident response team before a data breach or attack occurs since properly responding to and mitigating the effects of an intrusion require specific skill sets and training. During an attack, the incident response team should keep track of the investigation's progress and constantly inform the management team of any update.

## Importance of Incident Response Teams for Enterprises

Apart from configuring the network and building a data protection architecture, enterprises should also form an incident response team that will be responsible for detecting and containing ongoing network attacks. Incident response and management is a critical security control that every enterprise should implement.

Not having an incident response team can lead to the following scenarios:

- The IT team may not be able to prioritize the investigation should an incident occur because it is primarily tasked to maintain the enterprise's operations. This can affect the investigation and can delay mitigation. Delays are detrimental to an enterprise given that fast action is crucial when an attack occurs.
- Threat intelligence refers to indicators such as tools and techniques used to tell if an attack is currently occurring. Lack of it would make it arduous for enterprises to probe deeper into how an attack occurred.
- The absence of an incident response team can make it harder for an enterprise to deal with legal and compliance issues should an incident arise. A dedicated incident response team can address legal and compliance concerns properly and quickly.
- Customer notification is also an important aspect of managing security breaches from targeted attacks. Improper handling of external communications may further damage an enterprise's image and reputation and even cause legal or regulatory penalties. Internal communication is also critical to raise awareness within the enterprise.

# Building Threat Intelligence

Threat intelligence refers to any information pertaining to the tools, tactics, and procedures (TTPs) attackers use to carry out campaigns. Security analysts and researchers can learn how threat actors operate and monitor ongoing campaigns via technical indicators and available information. Through good threat intelligence, targeted attacks can be detected earlier in their life cycle, thus reducing risks of exfiltration of any confidential company information.

## Internal Threat Intelligence

Enterprises are encouraged to set up their own threat intelligence group, which should focus on learning about exploits and the TTPs threat actors use. This group's role is critical in processing and understanding the data that resides on the network. The information the group gathers should be handed over to the security team so it can be incorporated into security systems. The group can also recommend how the enterprise can defend its network against threats.

## External Threat Intelligence

External threat intelligence providers refer to third parties that offer threat intelligence deliverables like reports on new campaigns and threats. They also provide feeds or collated data like lists of malicious URLs and email headers, among others.

The Trend Micro™ Deep Discovery™ solution can protect enterprises and large organizations against targeted attacks by detecting malicious content, communications, and behaviors that indicate attacker activity in a network. It has custom sandbox simulation and advanced detection engines that classify and analyze submitted files. It also provides network traffic inspection, advanced threat detection, and real-time analysis and reporting, thus mitigating the risks targeted attacks pose before threat actors reach the data exfiltration stage.

## Experienced Cybersecurity Experts

Experienced cybersecurity professionals who process and make sense of logs and data collected from and transmitted over a network are an integral part of defending against targeted attacks. By making sense of threat intelligence, they can provide various defense strategies against any security threat that an enterprise may encounter. Combining threat intelligence, knowledgeable cybersecurity professionals, and security solutions can help mitigate the risks posed by threats such as targeted attacks.

# Managed Detection and Response (MDR)

Ideally, organizations should have an in-house cybersecurity incident response team, but the widening cybersecurity skills gap makes it more difficult to assemble one. While some in-house IT staff members and security professionals are trained to manage and control the network, they may have minimal experience when it comes to targeted attacks.

To address this challenge, organizations can look into sourcing a third-party incident response team for their security needs, that is, internal and external threat intelligence and experienced cybersecurity experts. Services featuring security experts who have expertise in advanced threat detection, threat hunting, analysis, and response have become available recently. One type of service is managed detection and response (MDR), which provides cybersecurity professionals who will be responsible for monitoring networks, analyzing incidents, and responding to attacks.

Trend Micro™ Managed XDR is one such service that offers a wider scope of visibility and expert security analytics by integrating detection and response functions across networks, endpoints, emails, servers, and cloud workloads. Using advanced analytics and artificial intelligence (AI) techniques, the MDR monitors the organization's IT infrastructure 24/7 to correlate and prioritize alerts according to level of severity. Organizations can have access to experienced cybersecurity professionals who can expertly perform a root cause analysis to get an understanding of how attacks are initiated, how far they spread in the network, and what remediation steps need to be taken.

**TREND MICRO™ RESEARCH**

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com