**Targeted Attacks**

A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity’s infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim’s defenses.  
  
**Background**  
Targeted attacks often employ similar methods found in traditional online threats such as malicious emails, compromised or malicious sites, exploits, and malware. Targeted attacks differ from traditional online threats in many ways:  
  
• Targeted attacks are typically conducted as campaigns. 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.  
  
• They usually target specific industries such as businesses, government agencies, or political groups. Attackers often have long-term goals in mind, with motives that include, but are not limited to, political gain, monetary profit, or business data theft.  
  
Attackers often customize, modify and improve their methods depending on the nature of their target sector and to circumvent any security measures implemented.  
  
**Phases of a Targeted Attack**• ***Intelligence gathering.*** Threat actors identify and gather publicly available information about their target to customize their attacks. This initial phase aims to gain strategic information not only on the intended target’s IT environment but also on its organizational structure. The information gathered can range from the business applications and software an enterprise utilizes to the roles and relationships that exist within it. This phase also utilizes social engineering techniques that leverage recent events, work-related issues or concerns, and other areas of interest for the intended target.  
  
• ***Point of entry***. Threat actors may use varied methods to infiltrate a target’s infrastructure. Common methods include customized spearphishing email, zero-day or software exploits, and watering hole techniques. Attackers also utilize instant-messaging and social networking platforms to entice targets to click a link or download malware. Eventually, establishing a connection with the target is acquired.  
  
• ***Command-and-control (C&C) communication.*** After security has been breached, threat actors constantly communicate to the malware to either execute malicious routines or gather information within the company network. Threat actors use techniques to hide this communication and keep their movements under the radar.  
  
• ***Lateral movement***. Once inside the network, threat actors move laterally throughout the network to seek key information or infect other valuable systems.  
  
• ***Asset/Data Discovery***. Notable assets or data are determined and isolated for future data exfiltration. Threat actors have access to “territories” that contain valuable information and noteworthy assets. These data are then identified and transferred through tools like remote access Trojans (RATs) and customized and legitimate tools. A possible technique used in this stage may be sending back file lists in different directories so attackers can identify what are valuable.  
  
• ***Data Exfiltration***. This is the main goal of targeted attacks. An attack’s objective is to gather key information and transfer this to a location that the attackers control. Transferring such data can be conducted quickly or gradually. Targeted attacks strive to remain undetected in the network in order to gain access to the company’s crown jewels or valuable data. These valuable data include intellectual property, trade secrets, and customer information. In  
addition, threat actors may also seek other sensitive data such as top-secret documents from government or military institutions.

Once a targeted attack is successful and has reached as far as the data exfiltration stage, it is not difficult for attackers to draw out the data. Although targeted attacks are not known to specifically target consumers, their data are also at risk once target business sectors have been infiltrated. As a result, such attacks (if successful) may damage a company’s reputation.  
  
**Why Should Businesses Be Concerned?**Trend Micro sponsored a study with *Quocirca* and found out that the most common impact of targeted attacks is financial data loss. The study says that the growing aspirations of cybercriminals to seek greater profits and the rise of hacktivism have led to more targeted attacks. Thus, it is not surprising that financial data is the asset that cybercriminals have set their sights on. Along with the loss of regulated personal data and intellectual property, data loss is costly for businesses.  
  
**How Can Trend Micro Protect Your Organization?**Moving beyond protection to embrace proactive detection capability is the ultimate step in combating targeted attacks. Early detection is crucial in preventing targeted attacks from exfiltrating confidential company data. Organizations and large enterprises need an advanced threat protection platform like Trend Micro™ Deep Discovery, which can mitigate the risks posed by targeted attacks through its various security technologies and global threat intelligence. At the heart of Deep Discovery is Custom Defense which provides a real-time local and global intelligence. This can help IT administrators understand the nature of the attack they are dealing with. It also supports threat intelligence initiatives with its network-wide security event collection and analysis, which can enable IT administrators to perform remediation and containment plans.