TREND MICRO™

Understanding Targeted Attacks: The Six Components

A TrendLabs℠ Primer

Understanding Targeted Attacks: What has Changed?

Targeted attacks refer to a type of threat in which attackers or threat actors actively pursue and compromise a target's infrastructure while maintaining anonymity. However, there's more to targeted attacks than just bringing companies to their knees. Attacker groups are increasingly picking targets deliberately to pilfer very specific intellectual property, collect trade secrets, or scoop up troves of valuable customer data. To accomplish these goals, attackers are not only focusing their efforts on particular industries but specific organizations as well, including specific individuals whom they hope to deceive into helping them infiltrate their target's network.

Understanding targeted attacks is an important first step in diagnosing targeted attacks. As the number of targeted attacks that resulted in data breaches steadily increase, it's important for an organization to understand what they are, how they work, the motivations, its impact, and how to defend against them.

Targeted attacks often rely on human nature and social engineering techniques, while most companies still model their security practices around generic malware and automated exploits. This weak point makes it easier for attackers to execute their schemes. Additionally, with the constant renovation of threats, attackers can remain within their target's network for an indefinite period—whether they are dormant or active, attackers will continue to build, reinvent, and enhance new tools and methods to carry out stronger and lasting attacks.

When is an attack considered a targeted attack?

An attack can be considered a targeted attack when it fulfills these three main criteria:

- Attackers have a specific target in mind and have spent a considerable amount of time, resources, and effort in setting up and carrying out the targeted attack.
- The main aim is to infiltrate a target's network and steal information from their servers.
- The attack is persistent, with attackers expending considerable effort to ensure the attack goes beyond initial network infiltration and penetration of data.

How is a targeted attack different from hacktivism, a cybercrime operation, and an APT (Advanced Persistent Threat)?

The evolution of threats, along with the growing number of highly vetted cybercrime forums and the advancement in new security technologies, are redefining targeted attacks. With the number of data breach incidents, it becomes difficult to distinguish whether an organization is attacked at random or targeted.

A targeted attack is different from a cybercrime operation, hacktivism, and advanced persistent threats (APT). Though cyber-attacks are designed to steal information and money or disrupt a network, the motivations behind each attack could be different from one another. Here's how they differ:

- **Hacktivism** - Hacktivism or activism-related hacking attacks often yield no network penetration and little to no information theft of any sort. It differs from targeted attacks as they are often driven by a cause, or a motivation to deface, vandalize, or immobilize an organization. Unlike targeted attacks, an attack motivated by hacktivism is done with maximum visibility as they are designed to be seen.
- **Cybercrime operations** – the biggest difference between a targeted attack from a cybercrime operation is the scope, with the former having a very narrow scope that limits its target to just one company or organization. A cybercrime operation is usually done indiscriminately, and aims to victimize as many users as possible in the shortest span of time to outrace security efforts. On the other hand, targeted attacks are purposeful and persistent and are mostly driven by financial intent. Targeted attacks are, at some level, also driven by financial motivations, but the primary goal is to steal information.
- **APT (Advanced Persistent Threat)** – this type of attack is much more sophisticated in nature and requires deft knowledge and skills to execute. APTs are attacks that use code and tools that have been designed from the ground up—not just by hackers like the case of targeted attacks, but by a more elite group of talented engineers. APTs are state-sponsored attacks, which mean that governments are behind them and that they operate on a longer timescale. They typically go after another country's power grids, nuclear reactors, or fuel pipelines.

Impact

The impact of a targeted attack not only affects the targeted organization but also its customers, usually resulting in severe public relations fiascos or devastating financial woes. Additionally, it could also cause mass unemployment, compromise national security, or stiff penalties for those accountable.

How does a targeted attack impact an organization?

The impact of a targeted attack on organizations is highlighted by many high-profile data breaches like those that hit Sony, Ashley Madison, and TV5 Monde. The effects of a targeted attack varies depending on the target and motivations of the attacker. Here is a list of the most common effects that it could have on a company in general:

- **Business disruptions** – a targeted attack disrupts business and operations, caused by system downtime or the lack of manpower due to resources needed to deal with the attack.
- **Intellectual property loss** – if the motive of the attacker group is to acquire information, a company may lose intellectual property. The Sony incident resulted in the leak of an unreleased movie, as well as highly sensitive data of prominent executives and other celebrities including personal information like birth dates, addresses, and emails.
- **Customer Information loss** – the company's information database that includes their customers' PII may be broken into and stolen—which could result in major security risks such as identity theft, blackmail, extortion, or worse.
- **Reputation loss** – the company reputation is tarnished when they are seen as being incapable of handling sensitive data critical to customers and/or national security. This may result in public disgrace following the inability to deal with the impact and aftermath of a targeted attack.
- **Financial loss** – the company may suffer from financial losses resulting from legal troubles such as class-action suits, or from their customers' loss of trust. The company may also have to spend millions of dollars on other damages and invest in better security.

How can a targeted attack affect a company's customers?

- Identity theft – critical data such as the PII of the customer may be leaked. The information could be full names, telephone numbers, addresses, and other information.

Other attacker groups could use the stolen data for malicious purposes such as extortion.

- Blackmail – blackmail is tied to extortion, and one of the ways a targeted attack can affect customers. This happens when the attacker threatens to leak stolen data and information to coerce victims into giving in to their demands.
- Financial loss – leaked financial information of customers can be used to steal from their online banking accounts.
- Reputation loss – depending on the type of data stolen, it could also tarnish the reputation of the customers as private details are exposed.

What are the hidden implications of a successful targeted attack?

As companies look at the costs associated with a targeted attack, it could involve a massive overhaul of their system, network infrastructure, including public layoffs of those deemed to have been responsible. The affected company may also have to collaborate with law enforcement and security vendors to investigate and find the parties responsible. With the disruptions of operations during and after the targeted attack, more losses may even occur.

For an organization's customers, they may be wary of big companies and terminate existing relationships. Employees likewise could also experience dealing with constant complaints because of their employer's inability to secure their data.

Overall, the impact of targeted attacks could be extensive, and they do not simply end with the conclusion of an investigation. Companies need to look beyond traditional protection technologies and stay abreast with the current threat and security landscape to ensure timely elimination of threats.

Motivations of a Targeted Attack

Many cyber-attacks are done at random with automatically-generated exploits targeting vulnerable systems. Today, a growing percentage of attacks are carefully selected to compromise a bigger target. Hence, understanding the motives behind a targeted attack is important because it can determine what an attacker's end-goal is. Knowing the motives can help organizations identify what to protect and how to protect it. Additionally, it provides an idea of what attackers are capable of, and what they can do once inside their target's network.

What are the motivations behind a targeted attack?

While it is difficult to determine each and every attacker's purpose, here are a few strong examples based on how their attacks were carried out:

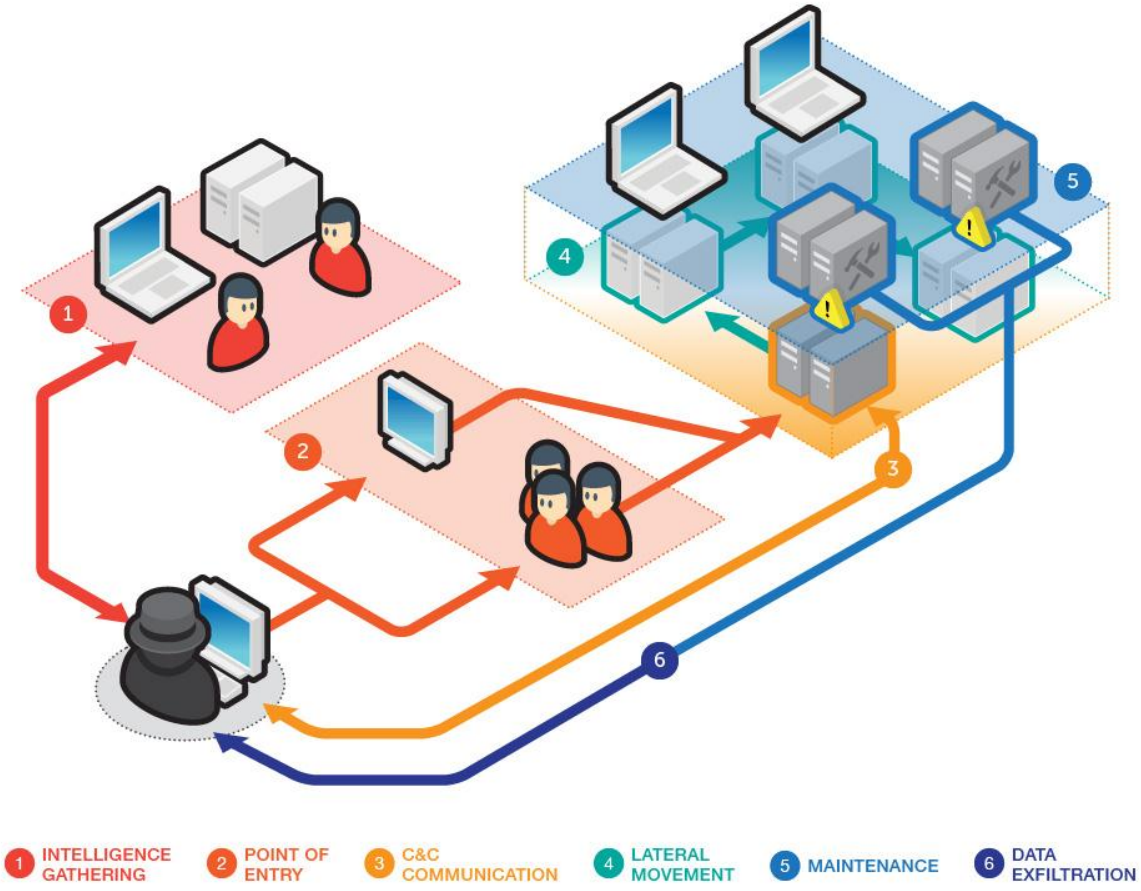
- **Information theft** – when the attacker aims to acquire information the target's information within the target's network such as customer information, business-critical information, or intellectual property.
- **Espionage** – when the goal is to monitor the activities and plans of the targets and steal information that these targets may have.
- **Sabotage** – when attackers aim to inflict destruction, defamation, or blackmail on their targets. This is done to deliberately interfere with the production and operations of an organization.

Understanding what attackers are after is one of the first key steps to defending against them.

6 Components of a Targeted Attack

Well-planned attacks have six components that show how attackers progress deeper within their target's network. It has been several years since targeted attacks were discovered, and both the attacks and our understanding of them have evolved and matured since then.

What has changed about each of the stages? The six "stages" of a targeted attack represent distinct steps in a logical, structured attack. In reality, it is far more complex. A "complete" stage does not necessarily mean that no other activities related to the stage will take place. In some cases, multiple stages happen simultaneously. For example, C&C communications take place throughout a targeted attack as the attacker needs to maintain control of any ongoing activities within the targeted network.



The stages are not particularly distinct

Each component of an attack has different facets that could affect separate portions of a network at the same time. An attack that has been detected at an "earlier" stage does not mean that the following stages are not in progress. An organization's response to an attack could depend on the effects of each component. Here are the six components of a targeted attack:

- **Intelligence gathering**

  The first component of any targeted attack is to gather information about the target. This happens continuously even if the attack is already under way. Beyond information, an attacker gathers knowledge about the connections that exist between various teams, including those that extend outside the target organization. This expands the attacker's prospects for more targets whether inside or outside an organization.

- **Points of entry**

  Spear phishing emails and watering hole attacks have become the biggest and most effective tactics attackers use to break into the networks of target organizations. However, beyond these initial points of entry, other techniques like backdoors are placed to move across the targeted network. They serve as additional entry points into an already compromised organization, providing fresh entry points for attackers when older points are detected and removed. Different employees and target network segments may be targeted to improve the chances of a successful attack.

- **Command and control communication**

  An attacker needs to control any compromised machine within a targeted network to mount a successful targeted attack. Previously, some old methods were used to hide backdoor and C&C traffic. Today, internal machines are acting as intermediate C&C servers that the attacker would connect to before passing it on to other compromised machines within the organization.

- **Lateral movement**

  At this point, attackers have already established their presence within the network and are now trying to seek better vantage points that they can use to find sensitive and profitable information. Lateral movement often involves stealing credentials and using legitimate system administration tools to keep activities hidden. Attackers can move within the network depending on their objectives.

  Lateral movement is also the most comprehensive step as it can encompass other stages of a targeted attack as well. Information gathering and internal reconnaissance is done, and any "intelligence" and assets gathered can be used to identify potential targets for lateral movement.

- **Maintenance**

  Once attackers gain access to the network, they then make sure that this access remains available to them and undetected by the organization. For example, an attacker can keep installed backdoors dormant so they can connect to it when their other points of entry are discovered. Attackers can also use several C&C servers to be able to maintain communication even when the other C&Cs are blocked. They can even go as

far as applying patches to software vulnerabilities found within the network to ensure that other attackers are unable to exploit the same vulnerabilities.

- **Data exfiltration**

  This is the ultimate goal of any targeted attack. However, not every compromised machine contains valuable information. Some systems may not contain information that is worth stealing. The process of exfiltration can be "noisy" as deemed by security solutions. Because large quantities of network traffic may not be found in the course of normal operations, attackers try to "hide" exfiltration traffic by transferring the stolen data to machines within the organization. This covertly exfiltrates data in a more controlled manner without security solutions detecting unusual activities.

Summary

Targeted attacks are a significant problem for any organization today, and will continue to be so for the foreseeable future. It is important for those playing defense to understand that the threat landscape is constantly changing before they can create an appropriate defensive strategy.

Created by:

TrendLabs

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

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com

TREND MICRO™ | Securing Your Journey to the Cloud