Cyber Snipers At Work

Advanced Persistent Threats Uncovered

1 Advanced Persistent Threats (APTs)

APTs are usually targeted at specific industries, organizations, or even individuals and may involve significant research into personnel, offices, IT practices, operations, and much more to help gain a foot-hold

2 Entry Point

Targeted or not, the initial system is usually infected by either:

- Visiting an infected website
- Opening an email attachment
- Plugging in a USB stick

3 Discretely Call Home

The infected system connects to the command & control (C&C) server for further instructions or to start passing sensitive data

4 Covertly Spread

The malware may choose to remain undetected and move slowly or it may attempt to spread to other systems by taking advantage of unpatched vulnerabilities or using hijacked credentials

5 Silently Exfiltrate Data

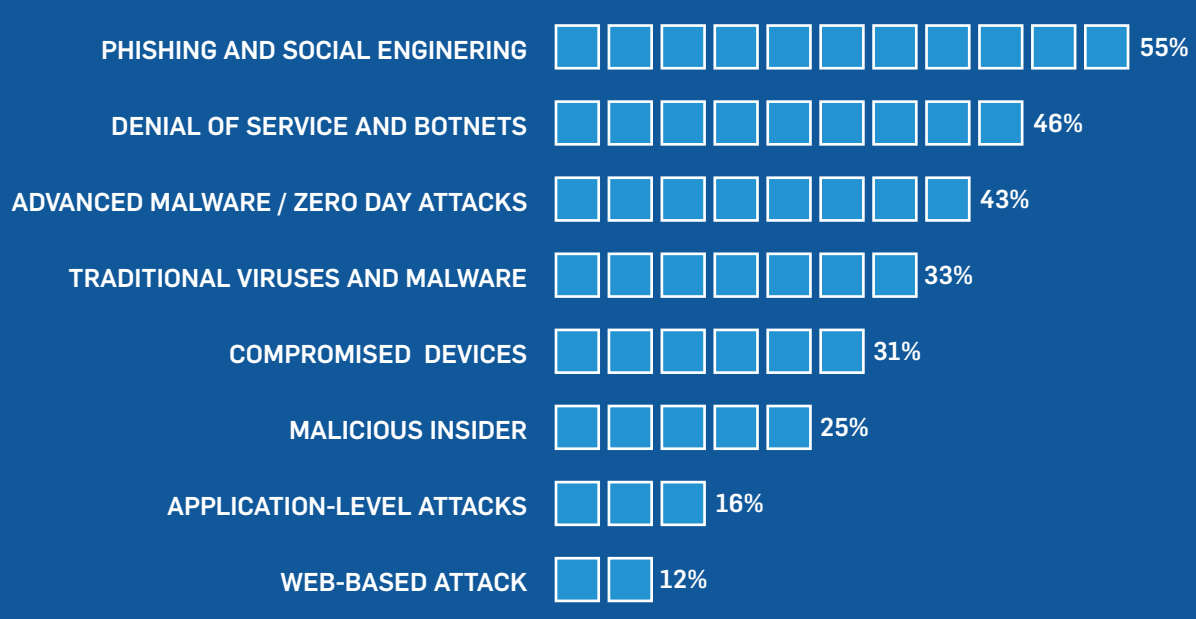
The malware may attempt to steal information from emails, documents, Skype or IM conversations, or even webcams depending on its intentions

68% OF IT MANAGERS DON'T KNOW WHAT AN APT IS

75% OF COMPANIES MIGHT HAVE EXPERIENCED A CYBER ATTACK IN THE PAST 12 MONTHS

51% OF COMPANIES LOST OR HAD SENSITIVE DATA EXPOSED IN THE PAST 12 MONTHS

MOST COMMON TYPES OF CYBER ATTACKS



How Command & Control Works
Watch the video

Learn More About Network Threats
and watch our short 3 min hacking videos

Advanced Persistent Threats: Detection, Protection and Prevention
Get the whitepaper

SOPHOS
Security made simple.

Sources: http://sophos.files.wordpress.com/2013/11/2013-ponemon-institute-midmarket-trends-sophos.pdf