R&D

Davey Winder

> **AETs require a significant amount of information gathering on a company for them to be executed successfully**
>
> Andrew Blyth

Persistent and Evasive Attacks Uncovered

APTs – and more recently AETs – have divided industry experts in opinion and often been used to scaremonger. Davey Winder reveals the truth behind the APT and AET headlines

There is no doubting that both the complexity of the threat landscape and the cost of defending against it are on an upward curve. More than ever, there is a temptation to rely upon legacy security defenses. However, with an increase in advanced persistent threats (APTs) – as perhaps best exemplified by the Operation Aurora attacks that were first disclosed by Google at the start of 2010, and more recently the real-world emergence of advanced evasion technique (AET) scenarios – this would not only be a false economy, but also a very high-risk strategy.

Advanced Persistent Threats Defined

In talking to several infosec professionals and researchers from security vendors while researching this article, it became clear that everyone has a slightly different definition of what an APT actually is. There seems no doubt that the term itself has been overhyped – not least by those with products to sell in order to combat whatever description has been applied. There is, however, no doubting that the advanced persistent threat is very real.

Taking a composite approach to defining an APT leaves us with a highly targeted method for compromising data security and accessing specific information. Most often reported when aimed at government or military networks, an APT can actually be used against any target, including business enterprises. They are advanced because they use a blended approach of both computer intrusion (hacking/malware) and social engineering (phishing/scamming), in concert with sophisticated management tools to bring the disparate prongs of an attack together.

Unlike the kind of 'spray and pray' phishing and malware attacks that have become prevalent during the last decade, APTs are not only highly focused on a specific data target, but as the name implies, they are persistent in their attempts to access it. Most often this persistence is seen in the form of a 'low and slow' technique, so there will be no constant bombardment of malware, but rather a consistent and stealthy digging away at the defense layers over time. As Adrian Davis, principal analyst from independent security body the Information Security Forum (ISF) says, "typically, any malware used in the attack will have been tested for its ability to remain undetected by commercial anti-virus (AV) products – or will be downloaded via an infected URL. Social engineering or placing someone 'on the inside' may form part of the attack to gain access and bypass perimeter or

The 'P' in 'APT' is seen in the form of a 'low and slow' technique