Keeping Advanced Persistent Threats in the Box

Meticulous system updates, intelligent security deployments and enlightened users go a long way in safeguarding enterprises against APTs.

By George Chang, Regional VP, Southeast Asia and Hong Kong, Fortinet

One of businesses' biggest threats today is the stealthy online infiltration by attackers to steal valuable proprietary information. Ghostnet (a botnet deployed in various offices and embassies to monitor the Dalai Lama agenda), Shady RAT (much like Ghostnet but with government and global corporate targets), Operation Aurora (monitoring of Chinese dissidents' Gmail accounts in 2009) and Stuxnet (an attempt to disrupt Iran's uranium enrichment program) in 2010 are just a few high profile examples.

In recent months, these so-called "Advanced Persistent Threats" (APTs) have become so rampant and unrelenting that they are forcing enterprises to question the current security paradigm. Firms are beginning to wonder if it makes more sense to stop focussing on keeping attacks out, and start accepting that sometimes attackers are going to get in, and aim to detect them as early as possible and minimize the damage.

An APT is highly targeted at a specific organisation and takes a muted and often slow and prolonged approach to penetrating an organisation, with the aim of gathering intelligence rather than making immediate financial gain. Precise definitions of APT vary but one can get a good idea of its characteristics through its component terms:

- **Advanced** – Cybercriminals behind the threat have a full spectrum of intelligence gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but may also extend to conventional intelligence gathering and profiling methods. Malware can also hunt and phish for specific information from targeted individuals – this information is then used in a second stage attack. Social engineering techniques are often employed at this stage. While individual components of the attack may not be particularly “advanced”, their operators can typically develop more advanced tools. Attackers often combine multiple targeting methods to reach and compromise their target and maintain access to it.

- **Persistent** – Cybercriminals give priority to a specific task, rather than opportunistically seek information for financial or other gain. A key requirement for APTs, as opposed to an “everyday” botnet, is to remain invisible for as long as possible. As such, APT perpetuators tend to focus on “low and slow” attacks that let them move quietly from one compromised host to the next, without generating regular or predictable network traffic, to hunt for their specific data or system objectives. Tremendous effort is invested to ensure that malicious actions cannot be observed by legitimate operators of the systems.

- **Threat** – APTs are a veritable threat because they have both capability and intent. There is a high level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. Cybercriminals target high value assets and are skilled, motivated, organized and well funded.

Infrastructure Weaknesses Aggravate APT Breaches

APTs breach enterprise networks through a wide variety of vectors, including Internet-based malware infection, physical malware infection and external exploitation. APT perpetuators don’t necessarily need to breach external network perimeters – they can, and often do, leverage insiders and “trusted connection” vectors to access targeted systems.

Once the APT attackers get in, certain infrastructure deficiencies in the organisation may facilitate their obtaining of the desired information:

1. As organisations expand, they combine new and legacy systems, join networks, and integrate with third-party service providers. The complexity created makes it easy for hackers to hide and find unknown or unpatched vulnerabilities. Employee-owned devices and cloud applications add further chaos to the mix.
2. Flat network design is another weakness. While having one broadcast domain costs less and is more flexible than highly segregated networks, it helps attackers roam the network and possibly reach high-value systems.

3. Business applications typically contain millions of lines of code, making exploitable security holes inevitable. Worse, these software are often not updated with the latest patches to help close holes as they get discovered and fixed.

4. Many security teams are unable to detect sophisticated attack patterns. While conventional tools may identify individual events, they don't associate the events to give a bigger picture.

5. Organisational structure may be another limitation. Security teams are often too siloed to accurately interpret multi-modal attacks.

Protecting Organisations from APTs
Fortinet believes that the so-called holy trinity of security will help enterprises thwart APTs:

1. **Educate Users and Keep Security Policies Relevant**
   Users are generally considered the weakest link of the chain by attackers, and are often the target of initial infection. Companies need to educate them on APT infection vectors and social engineering techniques. And, as that won't guarantee that employees will never open an infected document – for instance, Ghostnet got seeded by sending well-crafted and legitimate looking but infected PDF documents to staff of the Dalai Lama's office – IT managers should make sure each user only has the access rights that he/she needs and no more. For instance, the office accountant shouldn't have access to the source code repositories.

2. **Maintain Up-to-Date Systems**
   The latest security patches must be applied. IT-wide signature maintenance, typically obtained through a security services provider, includes making the zero-day window as short as possible to reduce vulnerability and operational risk.

3. **Adopt "Intelligently Redundant" Security Strategy**
   Enterprises need to take a multi-disciplinary and consolidated approach to secure all IT assets. Antivirus and intrusion prevention capabilities are essential but firms should consider data loss prevention (DLP) technologies too, and look at the big picture when it comes to the threat landscape. True mitigation results in a blend of policies and protection against the full threat spectrum. Antispam, Web filtering and application control all do their part to block APTs during different stages of attack. The rule of thumb is that no single security layer is foolproof, and integrating them intelligently helps ward off multi-vector threats.

Here are the layers that enterprises must have:

- **Effective protection against multiple attack vectors.** This involves a wide-ranging approach to build internal technical controls providing protection at a number of levels and vectors, and should include mail, IM, Web exploits, application, malware and botnets.

- **Robust in-depth asset hardening.** This should cover networks, Web applications, data/databases, laptops and servers. The impact of zero-day attacks are best minimized by a combination of keeping patching windows as short as possible, hardening all such assets through robust configuration management based on best practices (e.g. ‘least privileges’), and judicious deployment of two-factor authentication to critical services.

- **Application control.** This enables enterprises to exercise risk/threat-based application channel, peer-to-peer and botnet control. Employees will be able to safely access social networking platforms like Facebook. Botnet control is particularly important since most modern threats rely on an egress communication channel – blocking communication effectively mitigates many of these threats.

- **Monitoring.** This includes infrastructure-wide monitoring to rapidly respond to any real or potential attacks, as well as up-to-the-minute threat signatures on applications, networks, data and DLP. There are far too many documented cases of threats laying resident on systems and eventually creating millions of dollars in damages simply because they were allowed to live for months and, in some cases, years.
When mitigating APT attacks, enterprises must be prepared to deal with highly-skilled hackers with extensive testing facilities and high buying power on the zero-day market. Because an APT hacker can use zero-days and test his binaries against all known vendor engines before sending them to his target, traditional antivirus and intrusion prevention engines likely won't spot the initial attack.

This, however, doesn't mean that firms shouldn't bother installing the relevant security solutions – instead they need to take the additional step of making it hard for hackers to figure out and replicate their environment. It also highlights the fact that human judgement – on things like logs and correlated data – is a prized asset. This judgement, for the time being, is not easily replicated in a testing environment.

The good news about APTs is that an organisation can combat them through its regular risk management process (these protection measures go beyond APTs and also help mitigate traditional threats). APTs simply raise the bar with respect to external risk and impact. How much budget an organisation wishes to allocate to tackling APTs will depend, as always, on its appetite for risk. One thing, however, is for sure – top management, CIOs and risk boards around the globe must urgently assess their exposure to APTs and start taking preventive and remediation measures.