What are APT's?

And how can they affect your business?

By Jack Vile, June 2014

What is an APT?

APT stands for Advanced Persistent Threat. The goal of this form of hacking is to infiltrate the network of an organisation and slowly steal or harvest data while remaining undetected. In the world of cybercrime this is essentially the long con, as opposed to the smash and grab style of attacking quickly and doing as much damage or stealing as much sensitive data as possible.

A helpful way to gain more understanding is to define each word in the right context.

- **Advanced** – The hackers involved will have a high level of expertise and plenty of financial resources to sustain the project. They will also be creative to avoid detection inside the network.
- **Persistent** – The attack may be carried out over a long period of time, anywhere between months and years.
- **Threat** – The people behind the infiltration will coordinate the attack themselves and have specific intent such as sabotage, espionage or commercial abuse of the harvested data.

An APT can make its way into a system in a variety of ways including; internet-based malware infection, physical malware infection, phishing emails and other social engineering techniques. Once inside, the APT's first port of call is generally to establish a back door into the network. The next step is to infect additional machines, access more information and obtain network administrator privileges. Finally the information will need to be extracted directly or via the infected machines on the network. Examples of types of data likely to be stolen are emails, documents, sound, database contents, webcam images, screen dumps, certificates and hashes. These, in turn, could contain sensitive content such as customer details, proposals, sales figures, strategic plans, designs and other intellectual property.

Where do APT's originate?

We now know that the hackers behind an APT have the financial resources to sustain a project for years. This narrows down the possible origins significantly, including the possibility of state-sponsored projects.

This doesn't mean that all attacks are government inspired or that APT's only exist in a world of spies and espionage. APT's also have ties to organised crime where the extracted data could be sold on the information black market.

Is it just large companies and governments that are at risk?

Today, the main targets of APT's are organisations in high value or critical sectors such as financial services, manufacturing, utilities, government and defence. However, even if you or your company are not involved directly in such sectors, if you are affiliated with or within the supply chain of such organisations, you could still be at risk.

This is because, prior to an attack, the crooks behind it may infiltrate your systems to gather more information on their ultimate target and/or use any infected machines on your networks as part of the attack.

How do you protect against APT attacks?

Now, you may be thinking that being informed about the threats is all well and good, but how can you protect yourself from them?

For an APT to infect your system it must have a way in, so you will need all your basic firewall, anti-virus and other malware protection in place on the network. Beyond these relatively simple defences, vendors then offer various solutions to take protection to the next level, e.g. content monitoring/filtering, DLP (data loss prevention), content redaction, behaviour analysis (people and traffic) and more. However, it may not be possible to block all initial infection through technology; you also need to educate users on how to spot and avoid the various social engineering tactics deployed by hackers.

While one of the imperatives of an APT within your system is to remain undetected, with the right countermeasures an intrusion can still be spotted. This is achieved is by creating 'normal' profiles for data use, network traffic and system use, then monitoring activity and comparing it to these profiles to detect anomalies. The main point is to ensure you have monitoring tools in place and assign time to check things on an ongoing basis, not just by exception.

Where can you go for more help and advice?

Protecting yourself in the ways we have described may sound like a very daunting prospect, but various companies offer services that can help.

Below are examples of some of the key professional services you might want to consider.

- **Advisory and Integration Services** – These are available from vendors, ranging from system health checks and security assessments, which can help you put the right mix of point solutions in place, through to help with setting up your own SOC (security operation centre) to conduct continuous network monitoring.
- **Managed Security Services** – These can range from providing security analysts for your SOC all the way to comprehensive real time monitoring of your network. These enable the vendor to alert you about breaches in your system and the areas affected. In effect, this is about outsourcing your security monitoring and management to someone who has the necessary skills and resources.
- **Incident Response** – This is another vendor service, which offers rapid response, diagnosis and repairs the damage caused by APT's. They will also provide you with measures to stop these same problems recurring and identify gaps to help you discover existing holes in your security.

Many companies can supply services like these, including IBM, Symantec, Trend Micro, Clearswift, CA, HP, EMC / RSA and McAfee through to various system integrators and other point solution vendors.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.