Mindset shift needed to combat APTs says industry panel

Rise in APT sophistication and complex attacks underscore the importance of Assurance as a Service concept.

Panelists include (L-R): **Kenneth Wong, Partner at PricewaterhouseCoopers; Paul Haswell, Partner with Pinsent Masons; Marcos Ong, Country Manager, HK & Macau, Palo Alto Networks; Vladimir Yordanov, Sales Engineering Director, APJ, Imperva; and Daniel Kwong, Senior Vice President, Information Technology & Security Services, CITIC Telecom CPC.**

ADVANCED PERSISTENT THREATS (APTs) have become the bane of the Internet world. While they are generally categorized as a network attack where an unauthorized person gets the keys to your network, the real danger is that APTs may already be in your network.

To combat APTs is to combat mindsets, said the industry panelists at a panel discussion during an executive luncheon organized by CITIC Telecom CPC and partners. Entitled *Unravel the myth of APT: The best way to combat APT attack*, the panel discussion noted how APTs have evolved in sophistication while the world wakes up to their potential threat.

APTs become complex, pervasive

Both Daniel Kwong, Senior Vice President, Information Technology & Security Services, CITIC Telecom CPC and Vladimir Yordanov, Sales Engineering Director, APJ, Imperva cited the recent attack by DarkHotel (a.k.a. Tapaoux) as a clear example of APTs' sophistication. During the incident, hackers selectively targeted executives staying at hotels in what is called as spear-phishing attacks, while cracking weak digital signing keys to make their malicious files look legitimate.

"Traditional or legacy security framework will not be enough to cope with today's APT attacks. Application visibility is most important for understanding your network and to protect the whole security network," said Marcos Ong, Country Manager, HK & Macau, Palo Alto Networks, adding that this is becoming more important as BYOD and mobile apps become entrenched.

Yordanov noted that emerging trends such as the Internet of Things (IoT) is going to offer more vectors for APT attacks. "When was the last time you scanned your TV or fridge for malware? Besides, all the operating systems for IoT are based on freeware, so Shellshock, Heartbleed and Poodle are all going to be everyone's concern," said Yordanov. He also highlighted that the ability to hire hackers or procure hacking tools easily is not helping.

Having a service provider at your side is going to be vital when combating sophisticated and multi-national APT threats. "It is very expensive to run a comprehensive security in-house. This is where a service provider like us, with strong partnerships, helps," said Kwong. He added that it will be difficult for many companies to take on the deep resources of today's APT perpetrators, including organized crime, multinational hactivists and governments.

Deploying Assurance as a Service

Kwong further noted that partnerships, like his company's with Imperva and Palo Alto Networks, bring the concept of Assurance as a Service into reality. It combines Security as a Service, led by CITIC Telecom CPC's TrustCSI™ Managed Security Services, Palo Alto Networks' managed firewalls and Imperva's managed Web application security, together with TrustCSI™ Information Assessment Service (IAS) and the company's 24x7, ISO 27001 certified and ITIL-based Security Operations Centers.

"This powerful combination of services and professional expertise can help companies address today's security challenges. Remember, to effectively combat APTs, it is not about having the right solutions; rather it is about having the right solutions in the right place. This is where we can help," said Kwong.

Greater goals

Service providers, like CITIC Telecom CPC, also offer more than just better cost rationalization and comprehensive approach to targeting APTs. "Your threat intelligence may be limited to one organization if you are doing it on your own. We are able to gather it from other attacks to ensure your organization is always ready," he said.

From a legal perspective, partnering with the right service provider makes sense. "We are all now trading on data and the data we hold is more important than any other resources in the organization. So you need to closely look at what security you have in place. In the eyes of the law, the buck will always stop with the collector and user of the data," said Paul Haswell, Partner with law firm Pinsent Masons.