Towards a C^{2}I Platform for Combating the Cyber-Threat

Paul Kearney

Security Futures Practice, BT Innovate & Design
paul.3.kearney@bt.com

Abstract. In my talk, I outline a number of cyber-attacks that have been reported in recent years, and examine the vulnerability of organisations and critical infrastructure to them. I then discuss an approach to combating cyber-threats that integrates specialised tools within a managed service platform to create a command, control an intelligence (C2I) system used to co-ordinated defences against a diverse collection of resourceful and persistent opponents. The discussion is illustrated with examples from BT research and development projects. Such a system will have to be refreshed and up-graded regularly to keep pace with challenges such as:

- The escalating arms race against threat agents,
- Innovations in technology and business practice,
- Changing regulations and compliance demands,
- A cyber-Moore's Law that dictates a continual shrinking of required response times

Ultimately it will need to be adaptive and to learn from experience.

Keywords: Cybersecurity, Cyber-threat, Managed Security Service.

1 Extended Abstract

Cybersecurity is not a well-defined term. It has come to prominence in recent years due to use of the cyber prefix by the government, defence and law enforcement community to contrast new, ICT-enabled, forms of warfare, espionage, terrorism, activism and crime with their conventional, 'physical world' counterparts. However, the usage has caught on and cybersecurity is often applied more broadly and used as a trendy synonym for information and network security, etc.

In addressing cybersecurity we are primarily concerned with threats that are state sponsored and/or politically motivated. Criminal activities on a scale that threatens national economic or social well-being or the financial health of targeted organisations is also in scope. Such threats include: cyberwarfare, cyberespionage, cyberterrorism, and cyberactivism (aka 'Hacktivism'). Characteristics shared by many of the above include:

- They are well funded and have may have significant black-hat expertise;
- They play a long game, and attacks may be complex and stealthy, and hence difficult to detect and/or interpret;

I. Askoxylakis, H.C. Pöhls, and J. Posegga (Eds.): WISTP 2012, LNCS 7322, pp. 17–19, 2012.

– Individuals responsible may be difficult to identify. Even if they are known it may be difficult to apply sanctions.

The term Advanced Persistent Threat (APT) has been coined as a short hand for threats with these characteristics. Reputedly the term originated within the US Department of Defence (DoD), but it has been taken up and popularised by McAfee and some other vendors, who use it in their marketing literature. Others dislike this name, preferring terms such as targeted threat, as attackers do not necessarily use advanced techniques.

In many ways there is nothing new about APTs, and there have been no major breakthroughs in combating them, so why is Cybersecurity the word of the moment? People have long talked about the feasibility and danger of politically-motivated and state-sponsored cyber-attacks, and speculated that stealthy, probing attacks have taken place. However, in recent years, there have been a number of incidents that indicate that those with the capability and motivation to carry out such attacks are actually willing to do so. Significant incidents include:

– The denial of service (DoS) attacks on Estonia and Georgia;
– Stuxnet: most likely a state-sponsored attack on Iran's nuclear processing capability. An example of a cyber-attack causing physical damage;
– Wikileaks: not only the original disclosure of confidential information, but also the cyberattacks of the supporters (primarily the Anonymous group) and opponents (e.g. HBGary) of Wikileaks on each other;
– A succession of attacks on Sony;
– Nightdragon: the name given by McAfee to a series of covert cyberattacks they believe were launched against several oil, energy and petrochemical companies;
– Operation Aurora / Hydraq: Aurora is McAfee's name for alleged targeted attacks (using the Hydraq Trojan) on the corporate infrastructures of Google and other large companies with the aim of stealing intellectual property and accessing the e-mail accounts of Chinese human rights activists;
– RSA SecurID: RSA has revealed little information on the recent security compromise of their SecurID authentication products, but claim it was the result of an APT. Some reports indicate that the initial penetration was via a phishing attack that planted backdoor software on an employee's PC;
– Fraudulent SSL certificates acquired from Comodo. Iran has been accused of being behind the attack.

In response to these and other trends, a number of governments, including those of the UK, US, France and Germany have proposed to established or strengthen their cybersecurity programmes.

The publicity received by the above-mentioned attacks and government programmes have established the cyber prefix in the popular psyche (one suspects Dr Who had something to do with it as well). Vendors have latched on to this, and as a result numerous information / network products have been re-branded 'with added cyber'. While undoubtedly, serious vendors and service providers

are making gradual progress in combating cyber-threat, there is no new cyber-technology, but rather a continued incremental evolution of information / network techniques and tools.

So, while the definition of the term remains a little vague, we have the image that cybersecurity is about countering sophisticated, knowledgeable and committed opponents, whose goals, if achieved will result in significant negative Impact on the targeted organisation and those who depend on its services. We may also consider nations themselves and supra-national groupings as 'organisations', for whom cybersecurity is about countering threats to their sovereignty, economy, political systems and the rights, safety and well-being of their citizens.

In my talk, I outline a number of cyber-attacks that have been reported in recent years, and examine the vulnerability of organisations and critical infrastructure to them. I then discuss an approach to combating cyber-threats that integrates specialised tools within a managed service platform to create a command, control an intelligence (C^2I) system used to co-ordinated defences against a diverse collection of resourceful and persistent opponents. The discussion is illustrated with examples from BT research and development projects. Such a system will have to be refreshed and up-graded regularly to keep pace with challenges such as:

- The escalating arms race against threat agents;
- Innovations in technology and business practice;
- Changing regulations and compliance demands;
- A cyber-Moore's Law that dictates a continual shrinking of required response times.

Ultimately it will need to be adaptive and to learn from experience.