Attack on Japanese Defence Contractor

Submitted by: Query Click Ltd
Tuesday, 27 September 2011

The recent publication of the security breach suffered by the Japanese Defence Contractor, Mitsubishi Heavy Industries is just the latest in a long series of similar breaches around the world.

Once again, the discovery of multiple instances of the installation of malware or viruses on servers and desktops is symptomatic of what could be a very sophisticated attack – frequently referred to as Advanced Persistent Threat (APT) type attack.

It is reported that the breach started with what is known as spear phishing attacks - when attackers use very targeted emails; specially crafted/customised to targeted individuals, to maximise the chances of them being opened and any links within them being clicked on and followed.

Martin Finch, Managing Director of commissum, a specialist Information Security Consultancy (http://www.commissum.com/en/), said that “the organisation targeted here is a typical victim of such an attack by what could be industrial espionage or state sponsored hacking to access either national security information, or intellectual property. Previous victims have for example included, Lockheed Martin, the world's largest aerospace company”.

Chris Williams, senior consultant at Information Security company (http://www.commissum.com/en/), commissum said that “the usual modus operandi is for attackers to establish a foothold through initial breaches, and then use this to both escalate the level of the breach and establish further access points. This frequently continues over what is often a very protracted time-scale. The victim will, if one or more breaches are discovered, be uncertain as to how many other breaches have been established and where these are”.

China, Russia and Korea have been mentioned as possible sources of this type of attack in the past; China in particular in this case has vigorously and indignantly denied any involvement. That is one of the problems with a sophisticated attack of this type; it can be almost impossible to establish for certain where the attack originated. It is clear though that China is just one of the countries suspected of past involvement in such attacks by US and Western European government agencies.

In addition, as is often the case, the victim is downplaying the impact and the level of penetration achieved. It is reported that the Japanese government were not immediately informed of the breach, as is required in the Defence sector; allegedly it was discovered in August but was exposed by the press this week. It is unlikely that the public will ever know for sure if the breach involved a serious leak of information.

About commissum

With 20 years of experience, commissum is adept at offering practical advice and recommending cost-effective solutions, to deliver a joined-up, coherent approach to protecting an organisation's information assets.

Quay House
142 Commercial Street
Leith
Edinburgh
EH6 6LB
United Kingdom
tel: 0845 108 2066
web: www.commissum.com/en