Japan tightens cyber security as threats grow

Wednesday, October 23 2013

The government is intensifying its efforts to protect Japan from cyber attacks. Central to this is the revision earlier this month of a Cold War-era Japan-US security agreement to include cyber attacks among the issues that would elicit a joint response from the two states. In addition, Japan is consolidating its cyber specialists within government. These efforts coincide with cyber attacks on several government bodies and the discovery of a group of cyber mercenaries that has repeatedly targeted Japanese organisations over several years. Japan is struggling to keep up with the threat from state-sponsored and independent hackers. Highly targeted attacks against government departments and defence contractors are of particular concern, and officials have acknowledged that viruses are becoming more difficult to discover on their systems.

American and Japanese officials pose for photos during their meeting at the prime minister's residence in Tokyo (Reuters/Koji Sasahara/Pool)

What next

Improving cyber defences will take time. The change in approach earlier this year to support hackathons -- hacking competitions that were previously discouraged for fear they would increase online crime -- will help the government identify talented individuals for recruitment. This also suggests a renewed determination to tackle cyber attacks.

Analysis

The US secretaries of State and Defence and their Japanese counterparts, at the Japan-US Security Consultative Committee Meeting earlier this month, updated 15-year-old security guidelines detailing mutual cooperation to include cyber attacks. Washington is concerned that Tokyo lacks the ability to defend itself in this area, and to protect its communication systems. This poses a security threat to the US military bases within Japan. A particular fear is an attack from China designed to disable systems or access classified information. The revised guidelines mean that if there is a cyber attack against Japan's defence systems, the US military will support Japan's Self Defence Forces in a joint response.

This revision is part of the increased focus Japan has put on cyber defence in the past few months:

- September saw the first cyber-defence training session for civil servants, held at the Ministry of Internal Affairs.
- The government has also established a cyber security group, which, when it comes into effect next year, will bring together specialists currently spread across departments into a single unit within the Ministry of Defense.
- Similarly, Japan is following other countries in designating cyberspace as an area of national defence, alongside land, sea and air.

Recent attacks

These greater efforts are necessary. Two sophisticated, and apparently successful, breaches have been discovered since the summer. Both were targeted attacks against specific government organisations and related companies, designed to retrieve classified documents.

Impact

- Tokyo must demonstrate that its networks are secure in order to continue exchanging sensitive information with other governments.
- Weaker security and access to classified information make supply chains an increasingly attractive target.
- The emergence of skilled, professional cyber mercenary groups presents a considerable threat to businesses and governments.

The first was a virus, discovered in September, and was found in 20 organisations, including central government bodies and large companies. The foreign ministry, the Ministry of Economy, Trade and Industry, and defence companies are also thought to have been targeted, though officials have not revealed whether attacks on these were successful.

The virus was highly specialised: it was concealed on websites frequented by government employees and only attacked computers with IP addresses from organisations in which the attackers were interested. It then exploited a vulnerability in Microsoft's Internet Explorer to gain access (Microsoft released a patch for this on September 18).

'Icefog'

The second discovery is not a specific attack, but an Advanced Persistent Threat (APT) group that focuses its efforts on Japan and South Korea. Known as 'Icefog', it appears to operate as a group of mercenaries, contracted to acquire specific information quickly. APT teams traditionally break into systems and remain there, stealing information continuously over a long period. The approach of the Icefog group, which has apparently operated since 2011 and is expanding, is different: they directly target specific information identified in advance, acquire it over a period of days or weeks, and then abandon the system.

The members of the group appear to be based predominantly in China, with some in Japan and South Korea. As well as classified data, the group has stolen company plans, passwords, and email account information. Their targets are primarily government institutions, the military, defence contractors, and software and telecoms companies. To achieve this, they appear to have taken advantage of the weaker security of companies that comprise the supply chain of their intended target; the supply chains of Western companies have also been targeted.

Growing threat

Japan has been relatively slow to respond to a growing cyber threat. The small team within the Cabinet Secretariat that monitors attacks on the government's network revealed that there were 1,080,000 attempts in 2012, up from 660,000 in 2011.

History of attacks

Japan's government and major companies have suffered several high-profile attacks in recent years:

Japan has been relatively slow to respond to a growing cyber threat

- In January, hackers stole 3,000 classified documents from the Ministry of Agriculture, Forestry and Fisheries. Included in this cache were draft statements from Japan's then-Prime Minister Yoshihiko Noda and US President Barack Obama and other documents regarding negotiations over the TransPacific Partnership trade agreement. This attack used a Trojan programme known as HTran. Thought to be Chinese in origin, HTran was also used in an attack on Japan's finance ministry from October 2010 to November 2011.

- 2011 saw several significant cyber attacks. That September, the defence ministry ordered an investigation after weapons manufacturer Mitsubishi Heavy Industries admitted it had been attacked. The company revealed that it had found eight or more viruses on 38 of its computers and 45 servers. The hackers apparently sought information related to submarines, missiles and nuclear power plants, supposedly without success. Other defence contractors were also targeted, but the attacks were prevented by their security systems.

- In July 2011, computers of both houses of parliament were infected with a Trojan when an MP opened an email attachment. The incident was not revealed to security until late August. In the meantime, hackers stole passwords and data. It was alleged at the time that hackers in China were behind the attack; it is now believed to have been the work of the Icefog group.

Deceiving employees with personalised messages enjoys a high success rate

Nationalist hacking

Japan is a major victim of crude hacking by Chinese netizen activists (see INTERNATIONAL: 'Hacktivism' poses lasting threat - February 15, 2013). The Diaoyu/Senkaku islands territorial dispute has sparked attacks for years, and the scale increased when tensions spiked in September 2012, when the websites of a court and Tohoku University Hospital were replaced with the Chinese flag and a statement declaring sovereignty over the islands (see CHINA/JAPAN: Island patrols increase risk of clashes - September 18, 2012). The Ministry of Internal Affairs website, along with those of businesses associated with Japan -- including banks and Japan Airlines -- were also attacked. Though a lesser threat than other cyber attacks, these Distributed Denial of Service attacks often cause disruption.