State cyber threats will multiply globally

Friday, December 9 2016

(Reuters/John Adkisson)

Hans-Georg Maassen, the president of Germany's domestic spy agency BfV, said yesterday that cyberattacks and disinformation from Russia are expected to rise next year ahead of Germany's elections. He added that there has been a "striking increase" in cyber operations credited to Russian hacking group 'Fancy Bear', also known as APT 28. Advanced persistent threats (APT), a term cyber specialists use to describe government-sponsored offensive actions in cyberspace, have been growing in recent years.

What next

APTs will multiply within the next five years, as states have invested in offensive cyber capabilities. The multiplication of threats may force targeted businesses to collaborate with governments even more closely. As APTs experiment with operational concepts and doctrine, new forms of threats may emerge. Mission objectives are likely to shift from espionage to more integrated cyber operations including sabotage and subversion.

Analysis

Cybersecurity firm FireEye's chief strategist, Richard Beijtlich, defines APTs as follows:

- 'Advanced' refers to the ability of the threat actor to use a range of operational techniques. For example, from using simpler operations, such as social engineering and generic malware, to highly targeted and complex operations, such as researching a target's vulnerabilities to develop custom methods to attack.
- 'Persistence' refers to the threat actor not being opportunistic in their targeting, but rather pursuing a clear objective or mission, perhaps on someone else's orders.
- Finally, a 'threat' refers to the human volition behind the malware, as opposed to automatic intrusions by viruses.

Attackers with financial objectives do not normally fall under the APT category, since even advanced thieves shift their targets based on the risk/return ratio, thereby not fulfilling the persistence criterion.

APT impact

APTs can cause significant harm to businesses and governments. There could be loss of classified information -- for example, former National Security Agency contractor Edward Snowden's documents revealed that Chinese hackers stole the design plans of the Joint Strike Fighter F-35 from Australia.

Other attacks could affect businesses, such as the Iranian data deletion attacks against Saudi Aramco in August 2012.

There could also be attacks against the integrity of data, manipulating or changing them to affect decisions or actually cause physical damage. US Director of National Intelligence James Clapper warned of this potential threat in the February Worldwide Threat Assessment.

Prevalence

Impact

- The multiplicity of APTs will accelerate the proliferation of advanced intrusion capabilities to less advanced actors.
- This will spur growth in the high-end cybersecurity defence market favouring new technologies and novel defensive strategies.
- While the first generation of APTs has largely focused on cyberespionage, future attacks will be more innovative.
- For example, there may more subtle attacks against the integrity of data.
- As the spectrum of operations is explored, governments' incentives to agree on acceptable norms of behaviour will rise.

The attacks against the Iranian nuclear enrichment centrifuges in 2010 (Stuxnet) and the Snowden revelations in 2013 demonstrated both the effectiveness of cyberattacks as well as the reach that cyberespionage can give a state. Since then, investment in expanding state cyber capabilities has grown (see INTERNATIONAL: West is upgrading cyber capabilities - July 8, 2016).

The main APTs are driven by intelligence services and military commands. Cyberspace is judged to be a permissive environment for action, with lower risks of blowback and exposure of assets when compared to the physical realm. Cyber operations are also considered less intrusive, more targeted, and with more nuanced possibilities of deploying effects.

Sometimes, cyber operations are just the first part of a larger mission objective. For example, US intelligence bodies believe that the hacking of the Democratic Party emails was a step in the larger mission to influence the US electoral outcome (see RUSSIA/EUROPE: Moscow will exert multiple pressures - December 8, 2016).

Intermediary targets

Public and private sector organisations can be targeted when they are useful in fulfilling a specific APT's objectives. They will sometimes breach organisations as a preparatory step for reaching their actual targets. Breached organisations could be the mission target or just a stepping stone to fulfilling a larger mission.

For example, if that mission is political, government targets are the main focus, but the targets also include think tanks and political parties. If the mission is technical (that is, to establish access or build capabilities, for example) the targets may include networking component manufacturers, software companies and encryption gear.

If the objective is economic espionage, then it will depend on that state's economic plans. Chinese economic espionage was usually correlated to China's Five-Year Plan (eg, semi-conductors and pharmaceuticals). In Germany, defence, aerospace (including satellite), car companies and research institutes suffer the most cyberattacks according to the Internal Intelligence Service Report Year 2015.

APTs may target private organisations as a step in fulfilling larger objectives

State responses

There are two broad categories of government responses: raise the difficulty of an attack by improving defence or dissuade APTs by making their attacks politically costly.

Governments are improving cybersecurity across the different agencies, with defence and security agencies usually displaying a higher level of readiness. APTs have used this to their advantage by breaching targets that have not yet fully appreciated the value of the data they hold, as was the case in the breach of the US Office of Personnel Management.

Furthermore, some governments share with businesses threat intelligence based on classified sources and methods in order to raise the difficulty of attack (see UNITED STATES: CISA bill sets low bar for industry - November 4, 2015).

Others have entered into a political dialogue about the scope and nature of government-sponsored cyber operations and have signalled their discontent.

For example, in 2013 the United States presented evidence of Chinese intellectual property theft and indicted five members of China's armed services in 2014. In the summer of 2015, the two powers reached a political agreement excluding intellectual property theft for business purposes from the acceptable range of objectives (see CHINA/US: Summit yields more strains than gains - September 29, 2015).

Absent an effective political dialogue, some governments have opted to name and shame APTs, which may render the action costlier to the sponsoring state. For example, Germany has repeatedly voiced discontent with Russian cyber operations by publicly attributing specific attacks to distinct Russian intelligence agencies.

Some states are trying to name and shame APTs to deter them

Business responses

For businesses, defending against an APT is difficult. Some particularly exposed industries, such as the industrial defence bases, have opted to invest into upgrading their own cyber defence and to collaborate closely with governments.

Evaluating whether a business is potentially a target involves the identification of the priorities of various APTs in order to identify whether the data an organisation holds has a large value to a specific APT. For example, research and development in weapons or space technologies is an attractive target for many states seeking to expand their capabilities. EU and European national positions on the Brexit negotiations or any pending trade negotiation with UK involvement could also be targeted in UK espionage operations.

Measures can be implemented to make access to data more difficult. Sometimes, an effective evasion strategy can also be not to hold on to more data than needed.