Yui Kee Computing Ltd.

Newsletter

June 2011

Contents

USA to Bomb Cyber-Attackers, UK Develops Cyber-Weapons

<web-link for this article>

The trend towards incorporating ICT in warfare is accelerating. In the USA, the Pentagon's first formal cyber strategy declares that computer sabotage carried out by another nation can constitute an act of war that warrants a response of traditional military force, or, to put it in simplistic terms, "You hack us, we bomb you". On the opposite side of the Atlantic, the UK's Government Communications Headquarters (GCHQ) is taking the lead in developing a range of offensive cyber weapons for the British military.

According to the USA strategy, computer sabotage would have to threaten American lives, commerce, or infrastructure, and there would need to be indisputable evidence that a particular country was behind a specific incident, before military retaliation was used.

In the UK, Minister of State for the Armed Forces Nick Harvey said that he now regards cyber weapons as "an integral part of the country's armoury" and that the logic and standards that operate in other domains translate into cyberspace.

Coming shortly after China's admission that it has a "cyber army", it is clear that every country that is, or wants to be considered as, a World Power is developing both defensive and offensive cyber capabilities, and planning how to integrate them with existing military strategy.

More Information

Government plans cyber weapons programme
Cyber Combat: Act of War
Sources: US decides hacking can be 'act of war'
Pentagon: Hack attacks can be act of war
Defensive or Offensive, Beijing has Genius Cyber-Army

Chinese Military Academics Compare Cyber War to Nuclear War

<web-link for this article>

Further indications of the accelerating trend towards incorporating ICT in warfare have been provided by an article written by Ye Zheng and Zhao Baoxian, researchers at the PLA's Academy of Military Sciences, in China Youth Daily.

In the article, the researchers say that China must make mastering cyber-warfare a military priority because, "Just as nuclear warfare was the strategic war of the industrial era, cyber-warfare has become the strategic war of the information era, and this has become a form of battle that is massively destructive and concerns the life and death of nations,"

They also accused the USA of being behind many recent cyber conflicts and said that China would call for the international community to establish "cyber territory" and defend "cyber sovereignty". They envisioned a "cyber non-proliferation treaty like the Nuclear Non-Proliferation Treaty to lock up the Pandora's box".

Strangely, this call was echoed at a security summit organised by the EastWest Institute in London where Sir Michael Rake, chairman of BT Group, suggested a cyber non-proliferation treaty should be signed to stop the escalation of Nations spending on cyber defence and cyber warfare.

Quite what these concepts of "cyber territory", "cyber sovereignty" and "cyber non-proliferation" mean is unclear. Deciding control over territory is often quite hard, even after lines have been drawn on a physical map; how much harder for online users of cloud services that are deliberately insulated from the location of the physical machines that provide those services?

Cyber non-proliferation seems totally unworkable. Nuclear non-proliferation worked because many of the technologies and raw materials were specialised and traceable. Even then, there have been a string of failures as states achieved nuclear status despite the treaty. Cyber non-proliferation is more like trying to ban tanks: it cannot work because the facilities required (a car factory and lots of steel) are freely available. In fact, cyber weapons are perhaps more like cakes than tanks - you don't even need an expensive factory to produce them, every home has an oven that can be used with a recipe. The approximately 700,000 new items of malware identified every day are testament that someone has the capability, and it probably is not Sovereign States that are still struggling to impose their power on this new domain.

More Information

China PLA officers call Internet key battleground
PLA Officers Call Internet Key Battleground
China PLA officers call Internet key battleground
Chinese army: We really need to get into cyber warfare
China PLA officers call Internet key battleground
China's View Is More Important Than Yours
China PLA officers call Internet key battleground
USA to Bomb Cyber-Attackers, UK Develops Cyber-Weapons
Summit has few answers on hacking crisis
Web summit considers cyber-nonproliferation pact
Web summit considers cyber-nonproliferation pact
AP Interview: US says cybersecurity covered by law

Humour: XKCD on Cloud Computing Reliability

<web-link for this article>

It's not really like this is it. Is it?

More Information

The Cloud

Microsoft Disables Dangerous Feature for Anti-Malware Success

<web-link for this article>

Microsoft has reported a sharp drop in infections by malware that exploit the Autorun feature of Windows since the feature was disabled by an automatic update on 8th February 2011.

The report in the Microsoft Malware Protection Center blog explains that the update changed the behaviour of Windows XP SP3 and Windows Vista when removable media such as thumb drives are attached, but not for CDs or DVDs. Windows 7 already had Autorun modified, and earlier versions of Windows, such as XP SP2, were not updated because they are out of support.

Statistics collected by the Microsoft Malicious Software Removal Tool showed that infections of major Autorun-abusing families, such as Taterf, Rimecud and Conficker, dropped by 1.3 million, comparing the three months before and after the update. Unsurprisingly, the reduction was greatest for the operating systems that were updated, Windows Vista SP 2 saw an 82% decrease. However, there was also a "herd immunity" effect, with Windows XP SP2 infections dropping about 20% - with a smaller population of infected systems, a vulnerable system is less likely to be infected. This can also be seen in the number of infection *attempts*, which fell by 68% overall.

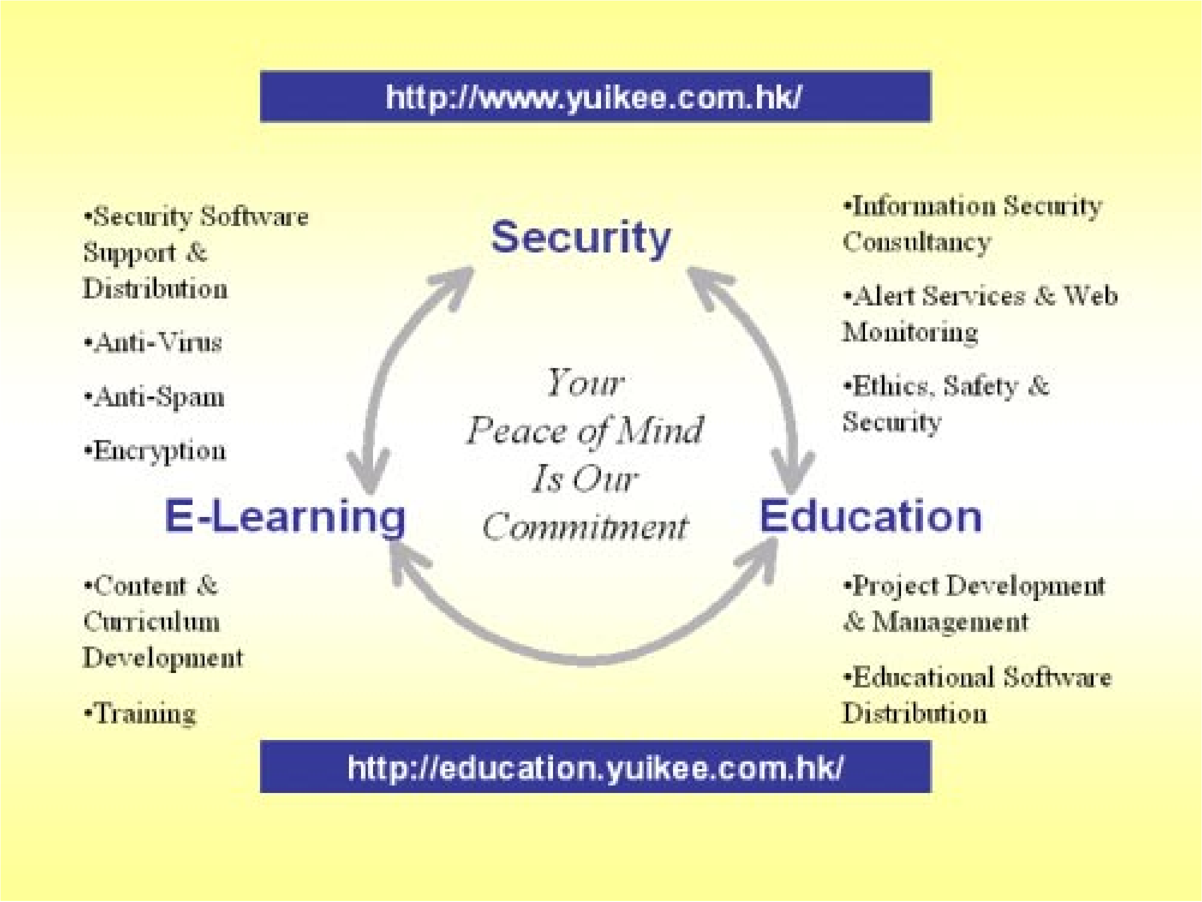
The infection rate did not fall to zero because these malware families have multiple spreading methods. This data is further confirmation of the phenomenon seen with DOS file viruses, boot sector viruses and Office Macro viruses: viruses die out when the environment that supports them changes.

More Information

Autorun-abusing malware (Where are they now?)
Malware abusing Windows Autorun plummets
Microsoft finally says adios to Autorun

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

Security

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Your
Peace of Mind
Is Our
Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/