Yui Kee Computing Ltd.

Newsletter

November 2010

Contents

Tencent and Qihoo in Privacy War

<web-link for this article>

Two Mainland Chinese companies are locked in a battle over privacy, security and business practices. The incident began in September, when Qihoo, which is based in Beijing and makes 360 Safeguard antivirus software, introduced "Privacy Protector", a tool to warn when instant-messaging software was accessing private files, the software soon began warning about QQ instant messaging client, produced by Shenzhen-based Tencent. Then, in October, Qihoo launched Koukou Bodyguard, to protect QQ users' privacy, prevent Trojans and improve the speed of QQ.

Tencent counter-attacked, explaining that QQ had started scanning for trojans in 2006, when account-stealing had become widespread, and accusing the Koukou Bodyguard tool of putting QQ users' account information at risk by scanning QQ records, including usernames, passwords, friends and dialogue when the users logged into QQ.

For a time, Tencent said it would shut down QQ when it found 360 Safeguard running on a computer. It asked users to uninstall 360 Safeguard to protect their own security, saying that it had been forced to make a difficult decision. Late last week, Tencent apologised for that decision and said that if users completely removed Koukou Bodyguard it would allow QQ functions to resume.

The Xinhua News Agency, the official press agency of the government of the People's Republic of China, quoted Qihoo executives as saying that the Ministry of Industry and Information Technology and the Ministry of Public Security had intervened, but a resolution has yet to be reached.

Qihoo and Tencent are important technology companies on the Mainland, 360 Safeguard has 300 million users, and QQ is the most popular instant messaging service there, with 600 million users. The case seems to be as much about competitive control of users' machines as invasion of their privacy.

Tencent is now suing Qihoo for unfair competition and demanding 4 million yuan in compensation in Beijing's Chaoyang District People's Court. Other IT companies have sided with Tencent; Baidu, Maxthon, anti-virus developers Kingsoft and Keniu have announced that their products will be made incompatible with Qihoo's new software.

More Information

Dispute pits mainland top IM client against security firm

Labour Department Website in Security Breach

<web-link for this article>

The Hong Kong Government's Labour Department admitted emailing 220 login names and passwords of other users to other users of their Interactive Employment Service website. The incident, described as a "website technical problem" during a recent upgrading exercise, took place on 1st November. Their investigation revealed that 51 of the accounts had been logged into during the incident, but no amendments were made to the accounts. The department contacted 40 of the 51 users affected, 31 confirmed that they had used the accounts themselves, 7 could not recall, and two said that they had not used their account.

The department said that it would follow up with the remaining 7 users as soon as possible, and that a full investigation would be conducted. The report did not clarify whether the Privacy Commissioner for Personal Data had been informed.

The Labour Department thus joins the Hospital Authority, the Independent Police Complaints Commission, the Baptist University and the Hong Kong Police as Hong Kong bodies that have succumbed to Data Leak Disease.

More Information

LD responds to media enquiries on iES website technical problem
HK Labour Department leaks user log-in details
Data Leak Disease

Discussing Scum in Paradise: AVAR 2010 Conference

<web-link for this article>

Figure 1 Approaching the conference hall

Billed as the "Conference in Paradise", the 13th Anti-Virus Asia Researchers (AVAR) International Conference took place in the lush surroundings of the Grand Hyatt Nusa Dua resort in Bali from the 17th to 19th of November. With thirty papers presented, lazing by the pool took second place to focussed attention in the cool darkness of the conference hall.

The conference had two streams, so not all speakers are reported on here.

In his keynote, Mikko Hyppönen reviewed the development of malware over the last quarter-century (that is something to consider, the first PC virus, Brain, was probably written in December 1985), and showed the deficiencies in our approach. The "State of the Net" is getting worse, the security industry is failing to combat the increase in malicious software and spam. Our solutions are targeting the symptoms, we need to target the criminals. As has been said before, early malware was written by people wanting to attract attention or prove how clever

they were, the biggest change has been the increasing involvement of criminals motivated by personal monetary gain. This leads to malware that does not advertise its presence, and a criminal organisation with different parties taking very specific roles. The software development is highly professional, as can be seen by the boot sector infector Mebroot, that appeared in 2008: if an infected computer crashes, Mebroot will take a diagnostic dump and send it to the developers, presumably so that they can identify whether Mebroot caused the problem, and work out how to prevent it in the next version. How many commercial software development teams are that professional? There may also be a more dangerous side: the large, Ukrainian website hosting company, Hosting.UA, suffered a large data-centre fire in March 2010, shortly after kicking out a dozen illegal sites. Coincidence or retaliation? Certainly, the criminal organisations have successfully monetised malware, so extreme methods of protecting their investment are possible. Mikko finished with two other areas that will be significant in future. Mobile phone malware has been tiny so far, but it is easier to make money infecting phones, so we can expect this to grow. Secondly, Stuxnet is a seminal event, it kills the principle that your security does not need to be perfect, only better than other potential targets. It also reached "unreachable" systems, via USB devices, involved multiple man-years of development and was missed by anti-virus developers for perhaps a year. The resources, sophistication and style of the attack point to Nation State involvement, but there will be copy-cats.

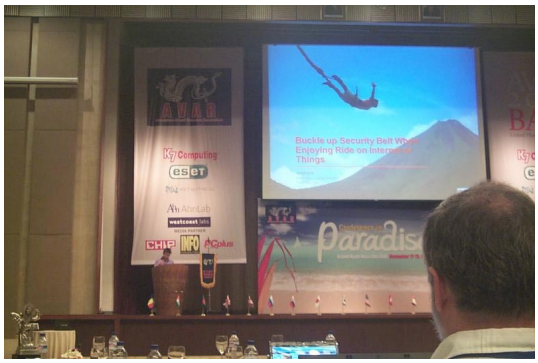

Figure 2 Peter Wei and the 'Internet of Things'

Peter Wei took a look at security in the "Internet of Things" (IoT), where RFID, IPv6 and EPC (the Electronic Product Code, a replacement for the UPC barcodes) are major enablers. Peter noted that security and privacy in these systems are usually very weak, and considered add-on features, leading to information leakage and other attacks. Very often, the back-end systems can be targeted by SQL-injection attacks from rogue tags. He proposed a three-way authentication model between the tag, reader and service provider and cloud-based malware detection, and that these should be considered in the architecture design of the systems.

Roel Schouwenberg warned us that Adobe is currently the most exploited software in the world and identified the key issues leading to this. Many people are not updating their Adobe Reader - recent successful attacks used exploits that were three years old! The Adobe Reader itself, and many alternative parsers, do not follow the formal specifications, for example, they will load a "secure" PDF that has been tampered with. There is no API for hooking into Adobe's script parser, complicating the task for anti-malware developers who therefore need to "reinvent the wheel" before they start to try to detect and identify malware. The Adobe Reader runs in a Limited Account, but the Adobe Updater, launched by the Reader, has full system privileges and therefore offers another opportunity to the attacker. However, there are some positive developments. Many in-the-wild PDF malware do not run in Windows 7, so they will probably disappear. Adobe is introducing a sandbox, with DEP and ASLR, but its success will depend on how good the implementation is.

Cristian Lungu explained the Rise of Icon attacks as a form of social engineering exploiting the user's association of a icon with a program. The percentage of malware families using an icon has risen from less than 50% in October 2008 to almost 70% in June 2010. The icons most often used are from Office tools, Games, Windows environment and System tools. However, identifying mis-use of icons is not simple as malware frequently uses slightly modified versions of familiar icons. Icon comparison is a useful heuristic for malware because, however

many packing layers the file may have, the icon remains the same so that the user can be tricked. Therefore, a slightly modified version of a common icon is a good marker for malware.

Figure 3 Kyu-Beom Hwang and the False Positive Crisis

Kyu-Beom Hwang talked about fileless whitelisting and false positive testing, describing his company's development of a virtual whitelist that identifies files using a block-crc-entropy value and addresses the difficulties of collecting clean whitelist samples. Also on the theme of false positives, Mark Kennedy explained how AMTSO (Anti Malware Testing Standards Organization) had studied the issue of testing for false positives in traditional products and cloud-based services.

Narendra Kumar reported on the development of algorithmic detection for metamorphic viruses based on a semantic signature.

Scott Molenkamp analysed the performance of malicious managed downloaders, often used to monetise malware by "pay per install" affiliate programmes. The proliferation of pay per install schemes and commission sharing creates a demand for configurable software that facilitates and simplifies botnet management. Typically, the tools come with an end user agreement that disclaims responsibility and specifies they should only be used for "research" purposes, but the pricing and prevalence of the tools make innocent use an unlikely explanation. In the questions to the session, the possibility of attacking the pay per install infrastructure by faking millions of downloads with the intention of crashing the market and destroying the trust between criminals was raised.

Wei Yan reported on government/industry cooperation in China, and concluded that we achieve the best security results when governmental policies and regulations are well aligned with the underlying science and practice.

Igor Muttik discussed the different forms of cooperation within the anti-malware industry, including through CARO, EICAR, AVED, VMacro, AMTSO, AVAR, VB and IEEE ICSG. He concluded that, in the face of the rising number rising sophistication and targeting of attacks, cooperation among the good guys is essential.

Figure 4 Sei Murakami thanks the conference organisers at the Gala Dinner

Figure 5 Gala Dinner entertainment

In their combined presentation, David Harley, Lysa Myers and Eddy Willems covered the issues surrounding malware simulation and testing, the limitations of the EICAR test file, and extensions of the concept.

As a replacement presentation, Rand Abrams expounded on endpoint security, whatever the endpoint may be, and how anything from medical devices through card key readers and routers to business centre computers may be the malware endpoint and the critical area for exposure of sensitive information.

Rajesh Nikam reported on behaviour-based detection of file infectors.

Evgeny Smimov described analysis to extract obfuscated text from image spam.

Figure 6 AVAR Balinese Dance: The demon Trojan tries to hide

Stefan Tanase discussed recent targeted attacks, including Aurora and Stuxnet, and their implications. Not only did these events demonstrate the power of targeted attacks, they changed a major corporation's approach to a region (Google's to China), and they were probably discovered after they had been successful in their objectives. They also have advantages over general attacks: if there is a corporate monoculture in the target, they only have to bypass the target's AV. Most corporate networks are focussed on external threats: the eggshell model. Once inside, the attack can work over a period of time undisturbed before exporting all the valuable data in one burst, probably at a weekend when the administrator will be slow to react. Stefan concluded that a security mindset is important. Stefan was voted Best Speaker by the participants.

Figure 7 AVAR Balinese Dance: Having vanquished the demon Trojan, Mr. AVAR introduces the clean software

The final session was a panel session on "Rogue, Anything Rogue", chaired by Righard Zwienenberg, with Andrew Lee, Lysa Meyers, David Harley and Tony Lee. The panel explained some of the many tricks used by rogue anti-malware applications and the consequences. There are also issues in how to define what are legitimate and rogue applications, and possibilities of sleeper applications that, maybe, work as advertised for six months, then go bad. It is all about awareness, as internet penetration spreads the next billion users will be new, naïve targets for the criminals. There is also the younger generation, the "digital natives", who are growing up with this technology, to be made aware.

The Gala Dinner, always a highlight of the AVAR Conference, was notable for two firsts. It was held outdoors, under the tropical moon, and the entertainers choreographed a traditional Balinese dance for the conference, showing the triumph of the wise Mr. AVAR over the demon Trojan.

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/