Yui Kee Computing Ltd.

Newsletter

March 2008

Contents

US Government DDoS's British Town Off the Internet

<web-link for this article>

Over a decade of incompetence by US military system administrators has forced the owner to abandon the mildenhall.com domain. The domain was used to promote the British town of Mildenhall in Suffolk, between Cambridge and Norwich, but it received hundreds of classified emails intended for officials at the US Air Force 100th Air Refueling Wing, stationed close to the town. The correct domain name for the air base is mildenhall.af.mil.

The owner of the domain, Gary Sinnott, tried to notify the senders and resolve the problem with the air base, but his early reports were ignored, and he claims some of the senders reacted badly when he informed them of their mistake, and sold his address to spammers. The domain now receives 30,000 messages a day.

An official letter to Mr Sinnott sent last November stated, "Unfortunately, there is no mechanism to forcibly prevent individuals, when in their private capacity, from sending emails to a particular address.", but this does not explain why Mr. Sinnott received classified emails, including, on one occasion, the flight plan of Air Force One. Do they have any policies about encrypting sensitive information?

More Information

US military secrets sent to factory hand
Mildenhall, Bury St. Edmunds, Suffolk
US government forces military secrets on Brit webmaster

RAF Mildenhall

29A AND 0

<web-link for this article>

In an announcement on its website, the virus writing group 29A has declared itself "retired". The last active member of the group, "VirusBuster" admitted he was unable to contact "ValleZ". "VirusBuster" said he was the first member of the group, back in the days of BBSs, and was now its last.

Over the years, the group was responsible for creating and releasing many firsts, including the first mobile phone network worm, Cabir, the first 64 bit virus, the first Pocket PC virus, Duts and other innovative creations.

Although the group's creations were generally proof-of-concept, and not intentionally damaging, they led the way for other virus writers in causing chaos. Cabir is a case in point: first released in mid-2004, it actually asked the user permission to install itself. 29A later released the source code and, by November 2005 there were 27 variants, some of which had spread worldwide. F-Secure attributed its success to it's persistence in pestering the user: once an infected phone "locked-on" to a target in Bluetooth range, it would keep sending requests until the user accepted it, or moved out of range. As the phone could not be used while a request was unanswered, many users accepted it.

29A was a relic of a former era, the very name, 29A being hexadecimal for 666, the biblical number of the beast, is redolent of nerdy youth rebellion. Nowadays, malware writers don't have pretensions of being k00l cyber-villains, they've snatched and run, leaving no calling-card.

More Information

Infamous malware group calls it quits
29A virus-writing gang shuts down
Science fiction novel inspires first ever Pocket PC virus
Going, Going, Gone!
Worm Targets Mobile Phones
F-Secure Malware Information Pages: Cabir
F-Secure Malware Information Pages: Cabir.B
Caribe (computer worm)
Improved disinfection instructions for Cabir
New information about how Cabir spreads.
Original Cabir source code released too
More than 100 known mobile malware variants
F-Secure Corporation Data Security Summary July to December 2005
Viruses on the stadium

A Sticker to Protect Your Privacy

<web-link for this article>

The Chamber of Hong Kong Computer Industry Co Ltd has announced that it will be issuing certificates to shops that agree to follow its Code of Practice on handling customer data stored on computers sent for repair. The voluntary campaign comes in the wake of the celebrity nude photo scandal that attracted a lot of attention last month.

The Chamber plans to list registered shops on its website, and provide the list to the Consumer Council. It is said that the Code of Practice advises repair workers to get the customer's permission before backing up the data, and erasing the data completely after the computer was

fixed. It also requires repair shops to record their technician's work to ensure they abide by the guidelines. However, neither the list of registered shops nor the Code of Practice was on the Chamber's website at the time of writing.

At best, this Code of Practice can prevent accidental data leaks, and might, in some circumstances, make it easier to trace the source of a leak. However, it cannot prevent malicious leaks, especially in high-value cases. When you hand over your broken computer, you are putting your trust in the technician and this Code of Practice does not guarantee their personal integrity.

Fees Increase for Strategic Commodity and Chemical Weapons Certificates

<web-link for this article>

International Arms Dealers and vendors of encryption software should note that the Hong Kong Government's Trade and Industry Department is raising the fess for three services on 27th March 2008. The new fees are:

Delivery Verification Certificate for the certification of delivery of strategic commodities into Hong Kong HK$235

International Import Certificate HK$79

Permit under Section 9 of the Chemical Weapons (Convention) Ordinance HK$570

More Information

Implementation of New Fees for Delivery Verification Certificate, International Import Certificate and Permit under Section 9 of the Chemical Weapons (Convention) Ordinance

Plausible Deniability is not Guaranteed

<web-link for this article>

Allan Dyer

I didn't notice Dr. John Aycock's 2006 paper, "Good" Worms and Human Rights when it was first published. Anyone living under a repressive regime may hope that human rights organisations also fail to notice it, or have enough sense not to implement the idea.

Aycock's basic idea is that a worm can be designed to spread within the country with a repressive regime and test the internet censorship in place *"avoiding the danger posed to humans who take part in testing"*. Aycock asserts that *"The self-replication mechanism of worms is ideal in this case, because a person whose computer is infected takes part in the testing but has perfect deniability": they performed no deliberate action and have no knowledge of the worm*.

Dr. Aycock has failed to consider that concepts of *deniability* and *innocent until proven guilty* are often lacking under repressive regimes. Instead of being eliminated, the risk is merely transferred to innocent parties. A human rights organisation thinking of creating such a worm should consider the ethical implications of passing responsibility of their actions onto unknowing subjects of the repressive regime.

Dr. Aycock has previously advocated teaching of virus writing.

More Information

"Good" Worms and Human Rights
University to Teach Virus Writing

Consumer Attitudes Toward Internet and Mobile Security Across Europe

<web-link for this article>

F-Secure, has announced the results of its first annual Online Wellbeing Survey. This third-party survey of Internet users aged 20-40 in the US, Canada, the UK, France and Germany, tested respondents' knowledge of online security issues (their 'security IQ') and gauged their confidence in the safety of basic online activities. The results revealed that while most respondents have security software installed on their PCs, many remain unsure that their email is free of malware and other threats. The survey also showed that few consumers realize how frequently their security software's antivirus definitions need updating, and most respondents revealed a misplaced confidence that their definitions were up-to-date. Over three quarters of mobile phone users are aware that malware can infect a mobile device via Bluetooth - but fail to have security software installed, according to this survey.

Online

The survey showed that Internet users in North America and Europe had a basic understanding of online security issues, but still don't have confidence in the security of basic online activities. While the results revealed similar levels of security knowledge and online confidence across those surveyed, German consumers showed markedly less confidence in the security of e-commerce and online banking than respondents in other markets. German respondents also revealed a significantly better understanding of how frequently anti-virus definitions need to be updated.

F-Secure's findings included the following:

Understanding Antivirus Protection

Though most respondents believed that their antivirus software is up to date with the latest definitions, few correctly identified the frequency with which these definitions must be updated, suggesting a misplaced confidence. However, a majority of respondents correctly indicated that online security requires more than just antivirus protection. On average:

- 19% of respondents understood that antivirus definitions need to be updated many times per day
- German respondents scored highest on this issue, with 31% answering correctly, nearly twice other markets surveyed
- 76% of respondents were confident their security software's antivirus definitions were up to date
- 73% of respondents recognize that their computers can become infected with malware if they rely on antivirus protection alone, even if their security software's antivirus definitions are up to date

Email Security

Consumers across all markets showed low confidence in the safety of basic email activities. On average:

- Only 10% of respondents are confident that they can open email attachments without infecting their computers with malware
- Confidence was lowest in the US, at 7%
- Just 9% of respondents are confident that they can open links sent via email without infecting their computers with malware
- Confidence was highest in the UK, at 15%, and lowest in France, at 4%

- 24% of respondents are confident that they are safe from malware sent via email
- Confidence was highest in Germany, at 31%, and lowest in Canada at 17%

General Knowledge of Online Risks

The survey revealed that respondents have a basic understanding of online risks and the ways in which their computers could become infected with malware. Expectedly, the great majority of consumers reported having security software installed on their computers. However, with their understanding of online risks, respondents expressed a lack of confidence in the security of basic online activities. On average:

- 95% of respondents have security software installed on their computers
- 73% of respondents recognize that computers running antivirus software with up-to-date virus definitions can still become infected with malware
- 88% of respondents realize that malware can add their computers to a botnet used to send spam without their knowledge
- 16% of respondents are confident that files they download from websites are free from malware
- 18% of respondents are confident that they are safe from malware spread by Web sites
- Consumers showed generally low confidence in their ability to identify phishing scams. On average:
- 37% of respondents were confident they could spot a phishing email Confidence was lowest in France, at 26%
- 27% of respondents were confident they could identify a phishing site Confidence was lowest in France, at 21%

Perceived Security of Online Transactions

Respondents showed greater confidence in the safety of online banking than in the security of credit cards used for online shopping. In both of these areas, German consumers reported significantly less confidence than other respondents.

- 50% of respondents in the US, Canada, the UK, and France felt their credit cards were secure when shopping online, in contrast to:
- 15% of respondents in Germany felt their credit cards were secure when shopping online
- 65% of respondents in the US, Canada, the UK, and France were confident in the security of their online banking, whereas:
- 28% of respondents in Germany were confident in the security of their online banking

"It's concerning to see that so many consumers believe their antivirus definitions are up to date while not understanding how frequently they need to be updated; this really shows why it's essential for consumers to make sure they acquire their security from a reliable source and make sure it includes professional service as well," said Mikko Hyppönen, Chief Research Officer at F-Secure. "Email security certainly isn't a new issue. Email remains one of the most popular ways to spread malware, and users understandably remain concerned that attachments may infect their computers. While malware is still being spread via email attachments, we've also seen an increase in the use of other techniques, like 'drive-by-downloads', and it's important that consumers be aware that email attachments aren't the only way malware is spread. Security software should empower users to take full advantage of the Internet and their email without worrying about vulnerabilities or security risks - it should provide true online wellbeing."

Mobile

On average, 28 per cent of all respondents said they use their mobile device to access the Internet. A large majority, 86 per cent admitted to having no mobile security. Out of all the countries questioned, the UK had the highest percentage (47%) of users accessing the Internet through their mobile device, while at the same time being the least likely to have a security product installed on their mobile phone. Most users are aware of the security risks involved with using the connectivity features on their phone: only 21 percent regarded Bluetooth connections safe, and a mere 15 per cent were under the impression WiFi connections are safe.

Over half of those questioned felt it was up to the individual user to ensure their phone was protected. A third expected this to be taken care of by their mobile phone carrier, with the US putting the greater emphasis on third-party responsibility. Only 11 per cent of Germans believed their mobile phone provider should be in charge of security, compared with over 32 per cent in France.

"While the mobile threat is low at present, it's only a matter of time before Internet criminals start utilizing the growing potential that smartphone usage presents to them," warned Mikko Hyppönen, chief research officer at F-Secure. "So far there have been about 400 mobile viruses detected, but as smartphones replace PC's as the dominant Internet platform, we can expect this figure to rise."

Geographically the sources of mobile threats are spread around the globe with activity originating for instance in South-East Asia, Russia and South America. While the threat from mobile viruses remains low, there has been increasing activity with spyware applications for mobile phones. Such applications make it possible to get covert access to all the functions of the affected phone, including recording of phone calls, access to messages and switching on the phone's microphone for listening.

The low amount of security software installed on smartphones coupled with the rapidly increasing volume of these devices make them a very vulnerable target for hackers.

The survey was carried out by a third party in January 2008 across 1,169 Internet users aged 20-40 across the US (225 respondents), Canada (228 respondents), the UK (227 respondents), France (256 respondents) and Germany (224 respondents). F-Secure asked respondents a series of basic online security questions and, using a Likert scale, asked them to rate the extent to which they were confident in the security of given online activities.

More Information

Mobile Users Do Not Take Security Precautions
F-Secure Reveals Consumer Attitudes Toward Internet Security Across Europe and North America

F-Secure improves performance with new version of F-Secure® Anti-Virus™

<web-link for this article>

F-Secure today announced the launch of the latest version of its F-Secure® Anti-Virus™ for Windows Servers solution, version 8. F-Secure Anti-Virus for Windows Servers version 8 features several significant performance improvements. Version 8 features F-Secure's new scanning technology, which is capable of meeting the rapidly evolving and more targeted malware threat scenarios better than ever. Extensive testing of the beta version of the software also shows that the memory consumption of version 8 is, on average, up to 50 percent less than in the previous version.

Significant performance improvements in the solution enable companies to safeguard their Windows servers with a better level of protection and lower resource use compared to earlier versions. F-Secure Anti-Virus for Windows Servers version 8 provides real-time protection against viruses, spyware and riskware, and prevents infections from spreading across a company's network.

F-Secure Anti-Virus for Windows Servers version 8 supports Microsoft Windows Server 2008, which is set to be one of the major software releases from Microsoft this year. F-Secure believes that Microsoft Windows Server 2008 will soon become an important part of the corporate IT infrastructure worldwide. F-Secure is committed to providing first class security solutions with clear added value for Microsoft server platforms.

With F-Secure, antivirus protection is fast, efficient and easy. Installations and management can be performed remotely from a single central location, saving cost and time for IT departments.

More than 1300 new virus detections are found each day at the F-Secure Labs, and some of these have the potential of spreading globally within hours. If a virus enters a corporate network, fighting it can prove to be both difficult and time consuming. Virus infections often result in significant financial losses due to network disruptions, decreased productivity, corrupted data and the leaking of confidential data. Even a company's reputation can be in danger if it unwittingly spreads viruses to its business associates.

F-Secure Anti-Virus for Windows Servers version 8 is an excellent security solution for companies that seek to protect their Microsoft server platforms with a centrally managed, efficient solution providing the highest level of security, but requiring less system resources. Deliveries of the solution will start in late April 2008.

More Information

F-Secure improves performance with new version of F-Secure® Anti-Virus™ for Windows Servers

Goodbye Arthur C. Clarke

<web-link for this article>

Father of the communications satellite. Author of the first science fiction I read. Visionary. Storyteller.

Farewell.

Allan

F-Secure News: Parents Worry

<web-link for this article>

According to a research from F-Secure, the majority of parents in both USA and Europe are worried about their children's safety while using the Internet:

- Only 5.5 per cent of parents believe their children are totally safe online
- Parents in Germany are most fearful; UK parents are most confident
- 92.5 per cent fear their children are exposed to questionable material online
- 20.3 per cent strongly agree that their children keep to online time limits set

Nearly half of the parents questioned disagree with the statement that 'my kids are safe online'. F-Secure found that despite the widespread availability of parental controls for Internet usage, parents are fearful about their children's safety while using the Internet.

Fears for children's safety were worst in Germany, where 77 per cent of parents disagreed that their children are safe online. People felt safest in the UK, where 38 per cent disagreed - however, only four per cent of UK parents felt their children were totally safe, compared to seven per cent in Canada and six per cent in the USA and France.

Children's exposure to questionable material was also a major concern for parents around the world. Just 7.5 per cent strongly agreed that their children are not exposed to questionable material, with nearly half of respondents disagreeing with the statement 'my kids are not exposed to questionable material online'. Parents in the US and Canada felt most confident that their kids are safe from such material, with 12 per cent in both countries strongly agreeing with the statement.

Parents in North America were also most confident that their children do not exceed time limits they set for time spent online: 27 per cent in the US and 23 per cent in Canada strongly agreed that their children keep to online usage time limits, with numbers dropping to 17 per cent in Europe, F-Secure's research found.

"Parents are clearly aware of the potential dangers facing their children online, but it is saddening that more don't feel empowered to protect their children by limiting their time online and controlling the content they're exposed to," said Pär Andler, Director of Communications and Brand at F-Secure.

Andler continued: "Responsible parenting now includes being responsible for your children's online safety, but this doesn't need to be a major headache. Internet security software often comes with 'parental controls' as standard, so you can prevent children from being exposed to questionable content and take simple steps to avoid Internet mis-use, such as setting limits to the time children spend online. Parents are right to be cautious, but this should not prevent the family from taking full advantage of the fantastic opportunities the Internet can offer to children in terms of education, creativity and social connectedness."

About the research

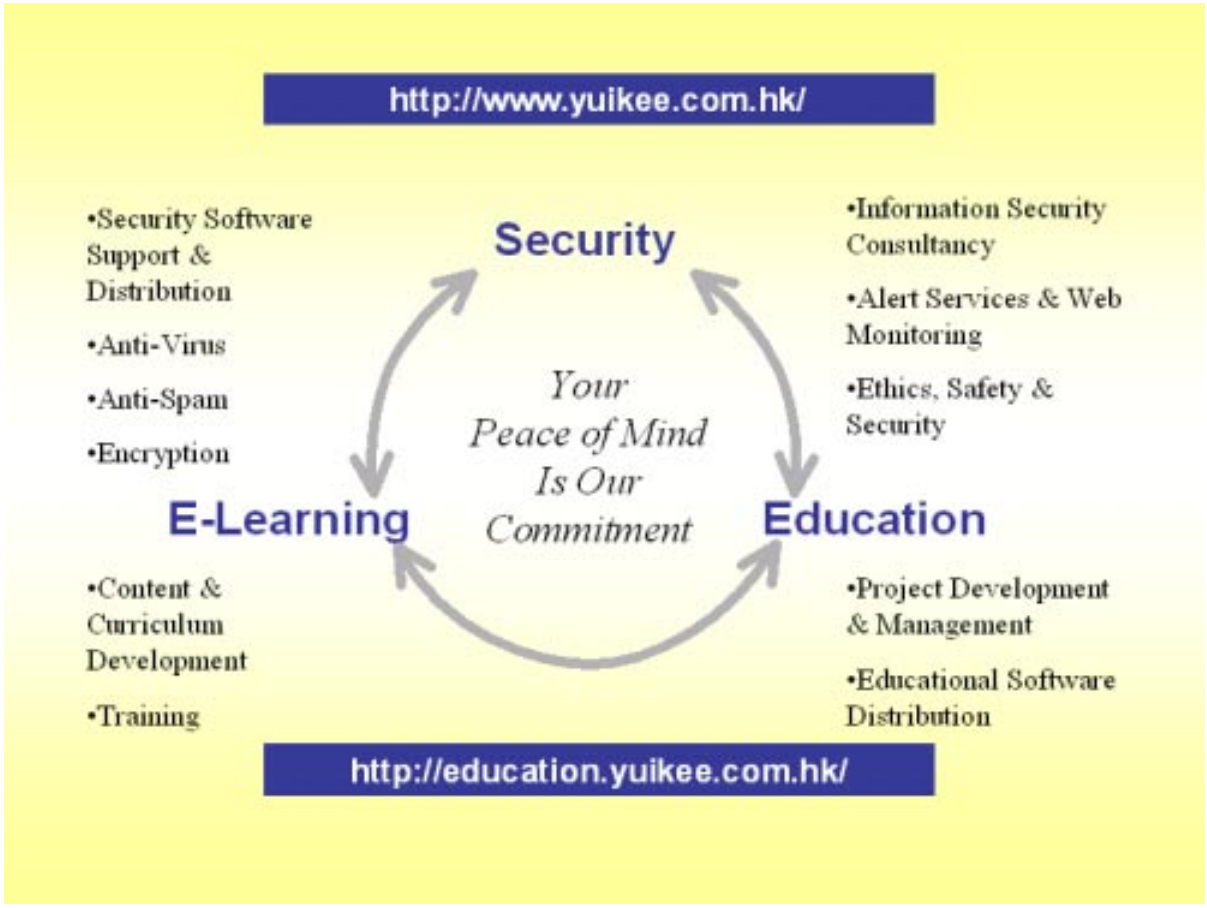
The survey was carried out by a third party in January 2008 across 1,169 Internet users aged 20-40 across the US (225 respondents), Canada (228 respondents), the UK (227 respondents), France (256 respondents) and Germany (224 respondents). F-Secure asked respondents a series of basic online security questions and, using a Likert scale, asked them to rate the extent to which they were confident in the security of given online activities.

More Information

Parents fearful for children’s safety online

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
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/