Yui Kee Computing Ltd.

Newsletter

December 2007

Contents

Malware Doubled in 2007 - Or Did It?

<web-link for this article>

F-Secure has released its threat summary for the second half of 2007, leading with the headline that the estimates of the number of types of malware detected have doubled during the year, "What previously took twenty years to accumulate — was now accumulated in just one year". There are now about half a million types of malware, and the numbers will continue rising.

Also in the same summary, F-Secure discusses a significant increase in the threat to Mac users, noting, "Apple Mac's market share is now significant enough for the Zlob parasites to target, as malware gangs don't make an effort to develop something without the promise of a profitable return."

The summary has been widely reported, including by Kevin Allison in the Financial Times, who wrote with the title Macs attacked. The security newsletter CyTRAP Labs - EU-IST - InfoSec news has attacked the F-Secure summary and the F.T. report as silly statistics to get the media attention, citing the poor, unexplained methodology.

Poor methodology would be a concern if the report was a reviewed scientific study, however, it is a summary of what the vendor's lab has seen, more like Police statistics of the number of reported burglaries than a scientific study. The discussion of Mac malware is not emphasised in the summary, one can imagine that Mac users would be rightly concerned if security vendors were ignoring a notable threat to their systems, and the fact that criminals are addressing the growth in Mac users is certainly a notable threat, even though it is at a much lower level than the current threat to PC systems. The choice of the F.T. reporter to put "Mac" in his headline is entirely his choice.

More Information

IT Security Threat Summary for H2 2007: Bulk Amounts of Malware, Storm, Apple, and Databases
CyTRAP Labs - EU-IST - InfoSec news since 2000, Archive for December, 2007
Research that aids publicists but not the public

Call for Papers: 2nd International CARO Workshop

<web-link for this article>

The Computer Antivirus Research Organization will hold its second international workshop on 1st and 2nd May 2008 at the Crowne Plaza Hoofddorp in The Netherlands.

As with the previous workshop on Iceland last year focusing on the Testing of AntiVirus, this workshop will have a theme as well. This year the focus will be on the technical aspects and problems caused by Packers, Decryptors and Obfuscators in the broadest sense.

The group has issued a Call for Papers with a deadline of Tuesday 15th of January.

More Information

2nd International CARO Workshop
Call for Papers

Lawyers Warn Santa In Breach of Data Protection Laws

<web-link for this article>

An article at OUT-LAW.COM warns that Santa Claus (also known as Father Christmas, Sinterklaas, Joulupukki or Sint-Nicolaas) may be breaking Data Protection laws by storing children's christmas lists, and monitoring their behaviour for the legendary naughty/nice database.

More Information

Santa putting children's information at risk, warn experts (OUT-LAW.COM)
Santa putting children's information at risk, warn experts (The Register)

Script Kiddies Deface Security Forum

<web-link for this article>

If a website forum of a security company got defaced, the last place you'd hear about it would be from the embarrassed company itself, right? Wrong! F-Secure were first with the news that their forum had been defaced by Turkish hackers on December 14th. They followed up with more information about how the site was vulnerable, and what to check in future.

Security is difficult, let's keep learning from each other.

More Information

Turkish Defacement - F-Secure Weblog
Turkish s'kiddies deface security forum
Welcome to our Forum - F-Secure Weblog

Stopping the Mules

<web-link for this article>

F-Secure, the well-known anti-virus company, is supporting the work of volunteer activists to expose money laundering web sites run by criminal organizations. Criminals frequently use the

Internet to recruit so-called money mules, which enables them to launder stolen funds and money gained from their use of banking-trojans, key-loggers, and phishing.

"We want to support the excellent work carried out by volunteer crime fighters like Bob at Bobbear.co.uk in exposing these activities, and help to build a community of volunteers in the fight against network crime," says Sean Sullivan from the F-Secure Security Labs.

People looking for jobs on the Internet can be tricked into becoming part of a money laundering operation in several ways. The criminals recruit so-called money transfer agents with spam messages and unsolicited emails, by placing job adverts on real recruitment sites, and by creating professional web sites that look perfectly legitimate to the untrained eye. Sometimes the web site is a spoof where the whole template has been stolen from a reputable company.

In all cases the purpose of the criminals is to convince the job hunter that the employment opportunity for a money transfer agent is made by a genuine, legal company. Typically, money transfer agents or financial operators are promised a 5-10% commission for 'processing payments' or 'transferring funds' through their personal bank accounts. After providing their bank details to the criminals - a major security risk in itself - money mules receive transfers of stolen money into their bank accounts, which they withdraw in cash and send to the criminals by using a more anonymous money transfer service, such as Webmoney, E-Gold or Western Union (which are legal services as such). Hypothetically, the transfer agent is forwarding the money to a software developer in a developing country. In reality they forward the money to criminals.

The promise of easy money for a few hours of simple work has lured many unsuspecting people to sign up as money mules. However, when the police and the banks discover money-laundering schemes, it is the money mule at the bottom of the crime chain that is often the first to be caught. The consequences can be serious. People suspected of receiving and forwarding stolen money may have their bank accounts frozen while they are investigated. Becoming a money mule can also ruin a person's credit history and lead to criminal charges.

Volunteer fraud investigator Bob at Bobbear.co.uk has uncovered a number of e-mail based job scams on web sites that Internet users should be aware of. As part of a Web 2.0 -style community approach to improve security on the Internet, F-Secure challenged interested volunteer experts to carry out further research on other suspected money laundering web sites that will help to get them shut down. The best material sent to Bobbear.co.uk was rewarded with prizes by F-Secure. The details of the challenge are available at:

- http://www.Bobbear.co.uk
- http://www.f-secure.com/weblog/archives/00001314.html

The criminals, who don't like the information Bob is providing to Internet users, have recently targeted his web site in retaliation. They attacked Bob's reputation by spoofing his domain name and making it look like he was sending out spam, which resulted in an investigation by his own Internet service provider in which they temporarily took his site offline. "Dedicated volunteers like Bob are really helping to improve security on the Internet," says Sean Sullivan from the F-Secure Security Labs. "Collecting evidence that a web site is involved in a money laundering operation is harder than showing it is spreading malware or stealing data from people. But if we all contribute to the research on how people are being deceived by these web sites, there will be greater awareness of the dangers and less people will sign up as money mules. It means a safer Internet experience for everyone in the end."

More Information

F-Secure supports fight against Internet money laundering with community approach

Espionage and Arrest in Tor Sniff Case

<web-link for this article>

Dan Egerstad, the security researcher at the centre of the Tor mis-use incident previously reported and updated in this newsletter, was arrested and interrogated last month. Although his home was searched and his equipment was seized, he has been released and not charged. He reports that his is "suspected for 'computer break in'".

In an interview, Mr Egerstad also suggested that he may have inadvertently stumbled on a spying operation when he sniffed the traffic passing through his Tor node, saying, "The whole point of the story that has been forgotten, and I haven't said much about it, many of these accounts had been compromised. The logins I caught were not legit users but actual hackers who'd been reading these accounts." In this scenario, the Tor network users accessing the accounts were not the legitimate users, but hackers using guessed or stolen passwords to spy on the legitimate users' emails.

More Information

Police swoop on 'hacker of the year'
Interview with Dan Egerstad
The hack of the year
Hong Kong Liberal Party Can Count but Sin Chung Kai uses Wife's Name in Password
Anonymity and Secrecy: Why Sin Chung Kai Should Apologise
Embassy Emails Hacked: 1,000 email accounts compromised

Crack Passwords with Google

<web-link for this article>

Steven J. Murdoch describes a neat trick he used to crack an MD5 hash of a password used by an intruder on his system: search for it on Google! Some programmers use MD5 to generate unique filenames for uploads, and similar purposes, so the hashes of many common words are in URLs.

More Information

Google as a password cracker
Google knows your passwords

Kaspersky Users Suffer Two Bad Updates

<web-link for this article>

On 13th December, a threat signature update released by Kaspersky Labs led to system instabilities and, rarely, to system failure on a small number of computers with Kaspersky Anti-Virus 7.0, Kaspersky Internet Security 7.0 and Kaspersky Anti-Virus 6.0 for Windows Workstations MP2 and MP3. Kaspersky rectified the problem the same day.

Days later, on 19th December, the anti-virus database released by Kaspersky included a false positive for an uncommon version of Windows Explorer (explorer.exe, not Internet Explorer, iexplore.exe). The program was detected as infected with Worm.Win32.huhk.c; depending on the configuration, Kaspersky Anti-Virus might quarantine, or, in the worst case, delete. the file. A database update fixing the problem was released within two hours. The falsely-detected explorer.exe version was released via the Microsoft Windows Update service as an Update for Windows XP on 24th July 2007.

Anti-virus software is complex and has to keep up with the large quantity of malware being released, so occasional quality problems with updates are to be expected. However, to have two within one week is... unfortunate. Kaspersky has apologised and said it will upgrade its testing.

More Information

Kaspersky Lab announces the detection and correction of an error in threat signature update
Kaspersky Lab corrects false positive detection in threat signature database
Kaspersky false alarm quarantines Windows Explorer
Update glitch derails Kaspersky

OFTA Increases Complexity of Spam Reporting

<web-link for this article>

On 22nd December, the second phase of the Unsolicited Electronic Messaging Ordinance cam into effect in Hong Kong, and the Office of the Telecommunications Authority (OFTA) has updated its' online report form accordingly. However, some of the features that make reporting spam long-winded and inconvenient have not been improved. The sections of the form are now:

1. Contact details: name and phone number. These need to be entered for each report made. It would be convenient if these could be entered once for a bunch of reports.
2. Company / Organisation name. Like the contact details, needs to be repeated for multiple reports.
3. Address. The option to be informed of the result of reporting, by email, fax or in writing. Again, needs to be repeated for multiple reports.
4. Type of message received, and the receiving address.
5. Content of the message. Options for non-email, email headers, email contents and file upload:
   - As the type of message has already been specified, the email and non-email options are superfluous.
   - For email, the simplest method would be to upload the entire message as a single file. This makes the header and content fields a superfluous repitition.
   - The upload dialogue specifies, "Maximum size per attachment file is 2MB.", spam larger than 2MB is uncommon, but surely an alternate procedure for sending large files should be specified?
   - The upload dialogue also restricts the file types to, "TXT, RTF, DOC, GIF, JPG, TIF, PDF, CNM". To quibble, these are file extensions, not file types (TIFF is the full abbreviation for the Tagged Iage File Format), and a file in these formats may not have the specified extension. More seriously, it seems strange to refuse to accept evidence from a victim on the grounds that it is not correctly formatted, or of the wrong size, "I'm sorry, we can only accept fingerprints in black ink on paper, and that bloodstain is too large".
   - The dialogue also informs the reporter, "To avoid receiving an infected file, your attachment will be scanned", which leaves the question of how a victim is supposed to report infected spam. To be safe, OFTA should assume that any file uploaded is potentially malicious. OFTA should have the expertise to receive and handle potentially malicious samples in a safe, secure manner. If it does not have this expertise, it should acquire it as soon as possible.
6. Other details. This section asks for a mixture of information that is mostly unknown, epetitious or can be obtained in other ways:
   - "Name of sender: (if you know)". Why should the recipient have reliable information on this? The message may be fraudulent or misleading about the sender, and the

question is encouraging the recipient to make unjustified assumptions, based on the message content.

- "Caller Number or Calling Line Identity (if applicable):". Good, but the type of message has already been specified, so it is unnecessary to ask this for email.
- Date and Time of receiving the message. This can be more accurately ascertained from the email headers. Unfortunately, the time can only be specified in 12-hour format, and email headers generally use the 24-hour clock.
- "Are you residing in Hong Kong?". Necessary for establishing the Hong Kong link.
- "Did you receive the message in HK?". Could be determined from the IP address in email headers, or the receiving number for fax or phone.
- "Particulars of the Reports". Options for the most likely UEMO offences. Good.
- "Other contact details of the sender". Is this necessary when section 7 is present?

7. "Further information which you think may be useful for our investigation". Necessary.
8. "Consent for Disclosing Personal Data and Documents to the Sender". This question seems odd when there is potential that an investigation may lead to a criminal prosecution with punishment of up to 10 years in jail and an unlimited fine. Do the Police ask witnesses if they mind whether their personal details are revealed to the suspects for crimes with similar punishments?
9. "Consent for Disclosing Personal Data and Documents to Other Government Departments or Parties as part of the Investigation". A necessary formality.
10. "Consent for providing further statement(s) and acting as witness in court proceedings where necessary". A necessary formality.

On submitting the form, the user is presented with a preview of their report, with a field for entering the text from a Captcha image. The Captcha image has been upgraded, the old version was four numeric digits, the new version is four letters. The page explains, "To prevent our service from being abused by automated scripts, please type the security code as shown in the picture", but spam is an automated offence, why is OFTA requiring manual reports, which, in effect, adds an unnecessary burden to the victim? OFTA should aim to assist users by providing reporting mechanisms that can be automated easily.

Herd Intelligence is the New Digital Immune System?

<web-link for this article>

A recent article in Computerworld cites a report from the Yankee Group that describes a "new" trend of security software vendors (specifically mentioning Symantec) changing their tactics to use customers' machines as their initial line of threat detection intelligence because of the threat of customized malware. This is described as "herd intelligence". Desperately mixing metaphors, Yankee Group Analyst Andrew Jaquith explains, "the herd network effectively turns into a giant honeypot". He also said that security vendors may also need to begin sharing more of that information with their rivals to create a larger network effect for thwarting malware on a global basis, but it could be difficult to get rival vendors to work together.

One wonders what Analyst Andrew Jaquith is an "expert" in. Those who have followed anti-virus technology for some time will know:

Steve R. White first developed the concept of a "digital immune system" where endpoints collected unknown software and communicated them to analysis centres while at the IBM's Thomas J. Watson Research Center last millennia. Steve reported on his team's progress at several conferences.

Symantec got the technology from IBM, and continued developing it.

The research teams anti-virus developers work closely together, securely distributing samples, regardless of the rivalries of their marketing departments.

Developments along these lines are important, but to describe them as "new" or "changing tactics" is misleading, and capriciously inventing new terms for already-named techniques is simply unhelpful.

More Information

Herd intelligence benefits IT security
Beyond Virtual Vaccinations
The Digital Immune System, Enterprise-Grade Anti-Virus Automation in the 21st century

Humour: MessageLabs closure Parody

<web-link for this article>

Vmyths co-founder Rob Rosenberger reminds us of MessageLabs' dire 2001 prediction that the internet could become "unusable" by 2008. Who's planning to switch off tonight?

On the other hand, can anyone argue that the internet has not become less useful because of the volume of malware-generated junk?

Note to Rob: You can't give your article a "UK" feel just by mentioning the Queen, in the UK, a "Public School" refers to a private or 'independent', fee-paying secondary school - think Eton or Harrow.

More Information

MessageLabs calls it quits
MessageLabs CTO: 'our company is doomed!'

Unsubscription Information

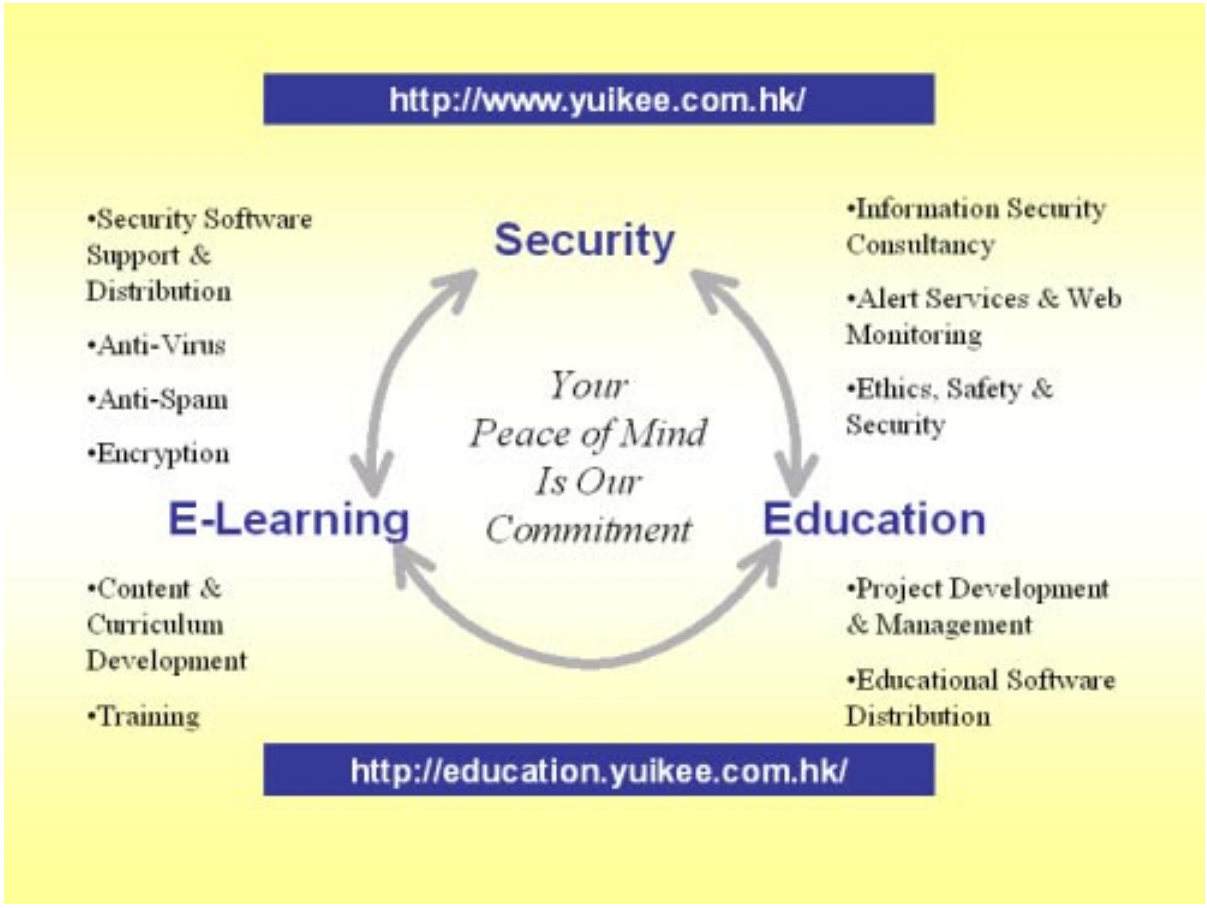
To subscribe, send an email to Maiser@yuikee.com.hk with subscribe newsletter in the message body. The Subject can be anything. Send the subscription email now. If successful, you will receive a welcome message.

To unsubscribe, send an email to Maiser@yuikee.com.hk with unsubscribe newsletter in the message body. The Subject can be anything. Send the unsubscription email now. If successful, you will receive a farewell message.

You can only subscribe or unsubscribe the address you are emailing from. If you need to add or remove another address from the list (eg. you have changed email addresses and want to unsubscribe the old address), or you have any other problems concerning the operation of the list, please contact the Postmaster.

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/