Yui Kee Computing Ltd.

Newsletter

December 2005

Contents

Contents 1
Incident Update 1
Editor's Notes 1
Zero-Day Exploit, Microsoft and Google 2
Sony Rootkit Developments 3
Information Harvesting by Mailing List Administration 3
Sophos annual security report names Zafi-D as year's worst malware 4
Virus Risks of RFC1149 and RFC2549 6
The F-Secure data security six-month summary 7
Testing Gmail's Anti-Virus 8
- Test 1 – Plain text EICAR message 8
- Test 2 – EICAR plain text file attachment 9
- Test 3 – Incoming Plain text EICAR message 10
- Test 4 – Drafted message with EICAR file 10
- Test 5 – Zipped EICAR file 11
- Test 6 – Encrypted zipped EICAR file 11
- Test 7 – Control Experiment 12
- Conclusion: 12
- References: 12

How to make the CME Initiative Useful 13
The Human Factor 13
"Titan Rain": Chinese Military Hacking US? 13
Guidance Software Hacked 13
In the Courts: eBay DDoS Culprit 14
Sober Worm Tricks Paedophile 14
Sue A Spammer 14

Incident Update

- Mon Dec 5 14:16:28 2005 CA: Java.Shinwow Family Medium
- Fri Dec 9 03:01:23 2005 CA: Sober.W Medium
- Mon Dec 19 15:46:34 2005 CA: Win32/Rbot Family Medium
- Fri Dec 30 20:31:29 2005 FSC: Information on the WMF exploit 2

Editor's Notes

An extra-large issue to end the year. The most important story is the zero-day WMF exploit, system administrators should examine the workaround immediately. F-Secure and Sophos have published reviews. Our Patrick Lee has taken a look at Gmail's anti-virus capabilities.

For humour, check "Virus Risks of RFC1149 and RFC2549" and "The Human Factor".

Seasons Greetings to all our readers.

Allan Dyer

Zero-Day Exploit, Microsoft and Google

Attackers are actively exploiting a previously unknown buffer-overflow flaw in the Windows Picture and Fax Viewer (SHIMGVW.DLL) to install backdoors on vulnerable Windows systems. The flaw takes effect when a malicious WMF file (a type of image file) is opened on a vulnerable system. Worse, if a malicious WMF file has been downloaded, the Google Desktop software will activate the flaw as it attempts to index the file, even though the user has not attempted to open the file. Microsoft is investigating the problem, but does not have a patch available at the time of writing.

Zero-Day Exploits are the good guy's nightmares – all complex software has bugs, and some bugs are vulnerabilities: they can be used to compromise a system. Responsible software developers have teams trying to find the vulnerabilities before the bad guys find them. A Zero-Day Exploit is a vulnerability that the bad guys know about, but the good guys don't: the good guys lost the race.

Administrators and users can do nothing specific to protect themselves against zero-day exploits (general security best practices can help) before the exploit is discovered. Even after discovery, before a patch has been released, there are few options. The best course at the moment is to disable the affected component: (from Microsoft's bulletin)

Un-register the Windows Picture and Fax Viewer (Shimgvw.dll)

1. Click Start, click Run, type "regsvr32 -u %windir%\system32\shimgvw.dll"

(without the quotation marks), and then click OK.

2. A dialog box appears to confirm that the un-registration process has succeeded.

Click OK to close the dialog box.

Impact of Workaround: The Windows Picture and Fax Viewer will no longer be started when users click on a link to an image type that is associated with the Windows Picture and Fax Viewer.

To undo this change, re-register Shimgvw.dll by following the above steps.

Replace the text in Step 1 with "regsvr32 %windir%\system32\shimgvw.dll" (without the quotation marks).

Attackers are currently exploiting this vulnerability by using malicious WMF files planted on websites to download backdoors including Trojan-Downloader.Win32.Agent.abs, Trojan-Dropper.Win32.Small.zp, Trojan.Win32.Small.ga and Trojan.Win32.Small.ev. The affected websites include:

Crackz *[dot]* ws	unionseek *[dot]* com	www.tfcco *[dot]* com	Iframeurl *[dot]* biz
beehappyy *[dot]* biz	toolbarbiz*[dot]*biz	toolbarsite*[dot]*biz	toolbartraff*[dot]*biz
toolbarurl*[dot]*biz	buytoolbar*[dot]*biz	buytraff*[dot]*biz	iframebiz*[dot]*biz
iframecash*[dot]*biz	iframesite*[dot]*biz	iframetraff*[dot]*biz	iframeurl*[dot]*biz

Do **not** visit those sites, you may want to filter them at your corporate firewall.

The latest news is that the workaround shown above does not stop the exploit from working if you open a malicious WMF file in MSPAINT. Also, the number of trojans known to be exploiting this vulnerability is still rising rapidly.

More information:

http://www.f-secure.com/weblog/archives/archive-122005.html#00000752

http://www.f-secure.com/weblog/archives/archive-122005.html#00000753

http://www.f-secure.com/weblog/archives/archive-122005.html#00000754

http://www.kb.cert.org/vuls/id/181038

http://www.microsoft.com/technet/security/advisory/912840.mspx

http://sunbeltblog.blogspot.com/2005/12/new-exploit-blows-by-fully-patched.html

http://www.f-secure.com/weblog/archives/archive-122005.html#00000755

Sony Rootkit Developments

Sony's original cavalier attitude to deliberately attacking its customers with unauthorized software has faded. In the past month Sony found itself under attack from New York's Attorney General Eliot Spitzer, who found it unacceptable that affected CDs were still available in shops three weeks after the vulnerability was revealed.

In the middle of the month Thomas Hesse, head of Sony BMG's global digital business said that the company would re-evaluate how it protects its products from piracy.

In the past few days, Sony BMG has agreed to compensate a group of plaintiffs in the New York class action lawsuit over the rootkit.

Has Sony seen the error of its ways and the folly of attacking paying customers, or is it making a strategic withdrawal from this battle, but still plans to win the war to wrest control of hardware from their legitimate owners? Only time will tell.

More information:

http://www.theregister.com/2005/11/30/sony_drm_spitzer/

http://news.bbc.co.uk/1/hi/technology/4514678.stm

http://www.theregister.com/2005/12/12/sony_anti-piracy_review/

http://www.theregister.com/2005/12/29/sony_settles_rootkit/

Information Harvesting by Mailing List Administration

How much are your auto-replies and error messages revealing about your organisation or activities? Anyone who administers a large mailing list will be familiar with the varied auto-replies and errors that clutter up their in-boxes. For honest administrators, these are just a waste of time, but they can reveal information of use to less salubrious people. If these examples seem familiar, well, they came from you – the recipients of this mailing list:

- `I am out of office for attending training from 29/Nov to 30/Nov. For assistance, you may contact my supervisor ????? ???? at 1111-1111 or by email to "  @  .edu.hk".`
- `I am on leave and out of town between 28-Nov-05 and 2-Dec-05. Should you need assistance on service issue, you may contact Mr. ??, ???? ????? @ 11111111 / 22222222, email:  -  .  @  .com.`

  We know what he's doing, how long he'll be away and his supervisor's name and contact details, great for social engineering. And we get his supervisor's email address, to sell to spammers.

- `I have annual leave this afternoon, and back on 1 Dec 05, any urgent matter, please contact with ????? ??? (Tel : 66666666).`
- `I will be out of the office until the afternoon of December 2nd and will have  limited access to emails. Should you require immediate assistance please contact ????? ??? (+852) 2222 2222,  .  @  .com`

A bit better, we don't know if the alternate contact is a colleague or a boss.

- `I am currently out of the Office. For urgent matter, please call me at 9111 1111.`
  Hey, everybody: call my mobile!

- `This is the ??????? program at host ?????.?????.edu.hk. < @ . .edu.hk>: host ????. . .edu.hk[1 .1 .1 .1 ] said: 550 No such recipient (in reply to RCPT TO command)`
  Nothing wrong with getting a bounce because an address no longer exists, except that this address was never on the mailing list. The domain name of the address appears to be an internal server at the organisation – if an error is being sent to an external recipient, surely the external version of the problem address should be shown? Was the list message forwarded to this destination?

- `Delivery to the following recipients failed. ???????@hk1.???.com.hk ?????@hk1.???.com.hk ??????@hk1.???.com.hk ?????@hk1.???.com.hk`
  Again, the problem addresses were never on the list, and the name of an internal server is revealed. In this case, the addresses without the "hk1." were on the list – the staff must have left, corporate downsizing, perhaps? Some organisations hide the names of internal servers for security reasons; do they check whether those servers are leaking the names in the error messages?

- `Your email has been delivered successfully to its addressee at ????????-????????. Please note that our email domain has now changed to @????????-????????.com. Kindly update your record.`
  I would update the record, if you told me the old address I need to change!

- ```
  ----- The following addresses had permanent fatal errors -----
  "|exec /usr/bin/procmail"
      (reason: addressee unknown)
      (expanded from: <???????@?????.???????.com>)

  ----- Transcript of session follows -----
  550 5.1.1 "|exec /usr/bin/procmail"... User unknown
  ```
  Do you really want to advertise your system mis-configuration?

What should you do about these problems? First, it is only polite to exclude all mailing lists from your auto-reply (please start with this one). Second, how much information is really necessary? Do they need to know what you are doing, or that Fred is your boss? Third, are auto-replies really necessary at all? You could set up addresses related to function that can be accessed by any of the relevant staff so that enquiries no longer need to be redirected, and more personal contacts can be dealt with more personally.

And check your server configuration – it might not be doing what you expect.

Sophos annual security report names Zafi-D as year's worst malware

New threats increase by 48% in 2005 as cybercriminals turn to targeted attacks

Sophos, a world leader in protecting businesses against viruses, spyware and spam, has revealed the top ten malware threats of 2005, in a new in-depth report into the year's most pressing security issues.

In a year that has seen the number of new threats rise by a staggering 48%, the lingering W32/Zafi-D worm has taken the number one spot in the virus chart, while last year's hardest hitting virus, W32/Netsky-P, has dropped to second place.

In contrast, W32/Sober-Z - only unleashed in November 2005 - has already climbed to third position as it continues to disrupt and clog networks worldwide.
  ```

The ‘Sophos Security Threat Management Report 2005’ was compiled by the experts at SophosLabs™, and reveals that on average, one in every 44 emails was viral during 2005. This rose to one in twelve during major outbreaks, while 15,907 new malware threats were identified.

The top ten viruses of the year, reported at Sophos's global network of monitoring stations, are as follows:

Position	Virus	Percentage of reports
1	W32/Zafi-D	16.7%
2	W32/Netsky-P	15.7%
3	W32/Sober-Z	6.0%
4	W32/Sober-N	4.3%
5	W32/Zafi-B	4.0%
6	W32/Mytob-BE	3.9%
7	W32/Mytob-AS	3.8%
8	W32/Netsky-D	3.0%
9	W32/Mytob-GH	1.9%
10	W32/Mytob-EP	1.8%
Others		38.9%

"Don't let the figures fool you - old-timers may head up the top ten, but the enormous rise in the number of new threats shows that 2005 has been anything but quiet on the malware front," said Graham Cluley, senior technology consultant at Sophos. "This huge increase stems from the escalating interest in authoring Trojans, worms and viruses shown by criminal gangs intent on making a profit. By focusing their efforts on a smaller number of victims, cybercriminals can target them with bespoke malware, increasing their chances of slipping under the security net."

Interestingly, while all of the top ten threats are Windows-based worms, the number of Trojan horses written during 2005 outweighs worms by almost 2:1. In addition, the percentage of malware that includes spyware components rose from 54.2% in January to 66.4% by the end of the year. These figures reinforce the notion that malware authors are engaging in targeted attacks, rather than widespread bombardment, and also help explain a rise in the amount of spam spewed out by zombie computers - now accounting for over 60% of the world's spam.

"Unlike viruses or worms, Trojans cannot replicate on their own, meaning that they must be deliberately emailed or planted on websites in order to spread. It's more and more common for new Trojans to become widespread after being spammed en masse from zombie computers," added Cluley. "It's no surprise that most of the top ten threats allow hackers to gain access to an infected PC, enabling them to create a zombie, steal information, and dish out their malware from under the nose of unsuspecting users."

The Sophos report reveals that unprotected computers have a 40% chance of being infected by an internet worm within ten minutes, turning them into a zombie under a remote hacker's control.

The report also identifies which countries around the world have been responsible for relaying the most spam during 2005, and that pornographic spam and messages attempting "pump-and-dump" stock scams have surged.

Full Sophos Security Threat Management Report 2005:

http://www.sophos.com/virusinfo/whitepapers/SophosSecurity2005-mmuk.pdf

Virus Risks of RFC1149 and RFC2549

Allan Dyer

A recent Gartner report has concluded, "A pandemic wouldn't affect IT systems directly"[1] however, the author feels that Gartner has neglected to consider RFC1149[2] and RFC2549[3] in its analysis. This paper addresses this oversight and makes recommendations for administrators of networks using these standards.

Although first published in 1990, there were no reports of implementation of RFC1149 until 2001, when the Bergen Linux User Group successfully implemented the protocol stack for Linux[4]. However, the standard has attracted a fair amount of attention[5,6,7] including the 1999 update to add QoS, RFC2549[3]. Unfortunately, most network technology surveys do not ask specifically about deployment of RFC1149 networks, so there is no data on the extent of use. Survey respondents with RFC1149 networks might have reported them as a wireless technology and some surveys indicate that wireless usage is increasing. Therefore, it would be dangerous to assume that RFC1149-compliant networks have not been deployed. Other uses for avian carriers have also been proposed[8]. It should also be noted that the use of avian carriers for data communications networks pre-dates TCP/IP[9,10]. This article only considers TCP/IP networks, but the basic conclusions should be applicable to other avian carrier-based networks, and other uses of avian carriers.

The current threat is the spread of a virus known as *avian influenza A (H5N1)*[11]. Note that this name does not conform to the CARO Naming Scheme[12], it is unknown whether avian influenza A (H5N1) (referred to as H5N1 in the remainder of this paper) has been analysed by any CARO members. A CME identifier has not been issued. Although there are many reports of H5N1 in the press, it is not listed on the current Wildlist.

H5N1 may result in:

Infection of carriers leading to Carrier Loss. RFC1149 notes, "With time, the carriers are self-regenerating", but infection by H5N1 may cause loss of carriers faster than they can be regenerated.

Culling. When an outbreak of H5N1 occurs, civil authorities generally require immediate termination of all carriers in the affected area, whether or not infected.

Loss of connectivity. Civil authorities are already imposing a ban on imports from affected areas[13].

Endpoint infection. Although not mandated by RFC1149, current implementations generally use a human to load and unload packets on the carriers. There is a risk of infection of the endpoints from direct contact with carriers[14]. This may also lead to a reassortment event or

[1] http://www.theregister.co.uk/2005/10/18/bird_flu_pandemic/
[2] http://www.ietf.org/rfc/rfc1149.txt
[3] http://www.ietf.org/rfc/rfc2549.txt
[4] http://www.blug.linux.no/rfc1149/
[5] http://www.bpfh.net/sysadmin/ip-over-mpd.html
[6] http://www.xent.com/nov99/0414.html
[7] http://quimby.gnus.org/internet-drafts/draft-bvenkat-chips-on-avians-00.txt
[8] http://www.faqs.org/qa/rfcc-524.html
[9] http://news.bbc.co.uk/1/hi/world/south_asia/1892085.stm
[10] http://disney.go.com/disneypictures/valiant/
[11] http://www.cdc.gov/flu/avian/professional/han081304.htm
[12] http://www.caro.org/tiki-index.php?page=CaroNamingScheme
[13] http://news.bbc.co.uk/2/hi/europe/4369376.stm
[14] http://www.who.int/csr/disease/avian_influenza/avian_faqs/en/index.html#present

adaptive mutation[15]. The resulting strain could cause a human pandemic. Note that the resulting strain would be distinct from H5N1, and it should be given a new name and CME identifier.

Thus, the usual response to an outbreak of H5N1 will cause a network outage far beyond the actual infection. Areas closer to the infection will suffer from a loss of all carriers. In the worst case, endpoints may be infected, leading to loss of endpoints and a global human pandemic.

How should network administrators address these threats?

Administrators of RFC1149 networks should be aware that H5N1 can cause a catastrophic loss of network connectivity. Be prepared to re-route traffic to alternate network connections that are not dependant on RFC1149.

Current computer anti-virus products do not operate low enough in the protocol stack – they are completely unable to detect or destroy H5N1 because it operates at the physical layer. Likewise, encryption (including IPSec VPNs) and integrity checking, while preventing modification of data, will not prevent infection.

A reassortment event is a possibility if an endpoint is infected with H5N1 and a human influenza virus simultaneously. Therefore, endpoints should be quarantined if they show signs of infection by human influenza.

If an infection occurs, carriers should be terminated without delay. Note that, unlike most computer viruses, termination of the carrier does not render H5N1 non-infective. Terminated carriers must be disposed of in a secure manner. Endpoints should not consume terminated carriers.

Endpoints should be handled differently. Note that, in most jurisdictions, it is illegal to terminate endpoints, even if they are infected.

If lost, carriers and endpoints should not be rebooted. The results are usually considered unsatisfactory[16].

It is clear that H5N1 can cause catastrophic failure of RFC1149 networks. Further study is required to assess the deployment of such networks, and the effects of such failure.

The F-Secure data security six-month summary

Steep rise in virus count and two major worm outbreaks define last half year

In the second half of the year the virus count continued to rise with alarming force increasing from 110,000 to approximately 150, 000 by the end of the year - an unprecedented figure in virus history. At the same time, however the trend towards mass assaults using network worms dropped significantly with only two major outbreaks, one in September, with the Zotob worm causing larger disruptions internationally and the second, a worm called Sober. Y flooding email systems in late November. Earlier this year, the Zafi. D worm also made the headlines.

In November, F-Secure detected the use of rootkit technology in the digital rights management software used by Sony. This resulted in a major international issue for the entertainment giant but also raised bigger issues for companies like Sony in the way they handle data security issues and build processes to deal with vulnerabilities.

2005 was also a year characterized by a spate of criminal phishing attempts either directly to on-line banking customers yielding high profits to the malware authors or by exploiting man-made and natural disasters.

[15] http://www.who.int/csr/disease/avian_influenza/avian_faqs/en/index.html#cana
[16] http://www.literature.org/authors/shelley-mary/frankenstein/

2005 was also the year, which saw the number of mobile malware exceed the 100 mark - growing proof that the criminal bodies behind their creation are serious in their attempts to exploit this new arena.

In the meantime, F-Secure has continued to up the ante against the malware community with a number of award winning products in the last six months including F-Secure Internet Security 2006 and its first venture into hardware, the F-Secure Messaging Security Gateway(tm).

For a full look at the last six months, please go to the F-Secure website at:

http://www.f-secure.com/2005/2/

Testing Gmail's Anti-Virus

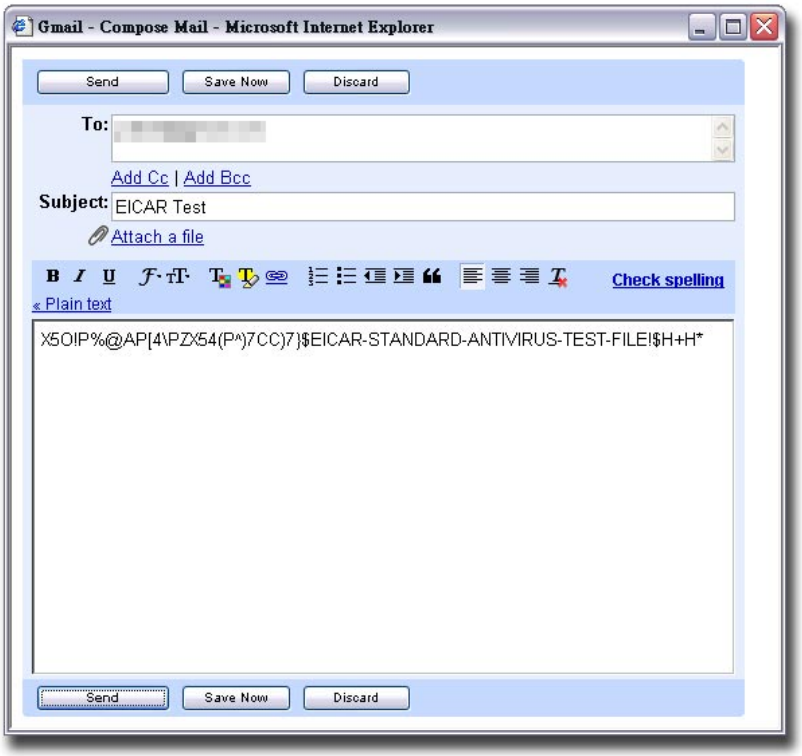
Patrick Lee

Google launched Gmail in 1st April 2004. Twenty-one months later it is still in beta version. The developers of Gmail keep improving the functionalities of this fast emerging free email service. One of the latest features is virus scanning. Google does not announce which anti-virus scanning engine(s) that Gmail is using, but there were rumours.

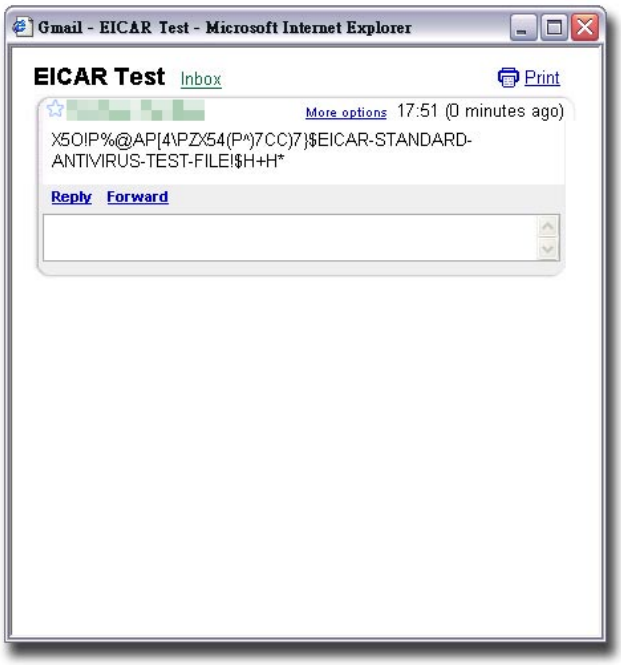
The experiments reported here test the circumstances in which a virus will be detected and blocked by the Google Anti-Virus. One and only one "sample" was used: the EICAR standard anti-virus test file. The test file is suitable for this test because all anti-virus products will detect it in the same way that they detect a virus, but it is not a virus or malicious in any way. Thus, it will reveal when a virus would be detected, or, conversely, missed, but, very importantly, there will be no risk of accidentally starting an outbreak. Obviously, the test file cannot be used to check the detection capabilities of virus scanners, such a test would involve using a large number of different live virus samples, and it would be extremely irresponsible to perform such a test outside a strictly controlled environment; doubly so on a working public service.

Test 1 – Plain text EICAR message

Using the Gmail compose mail interface, a line of EICAR test message was composed as the content of email.



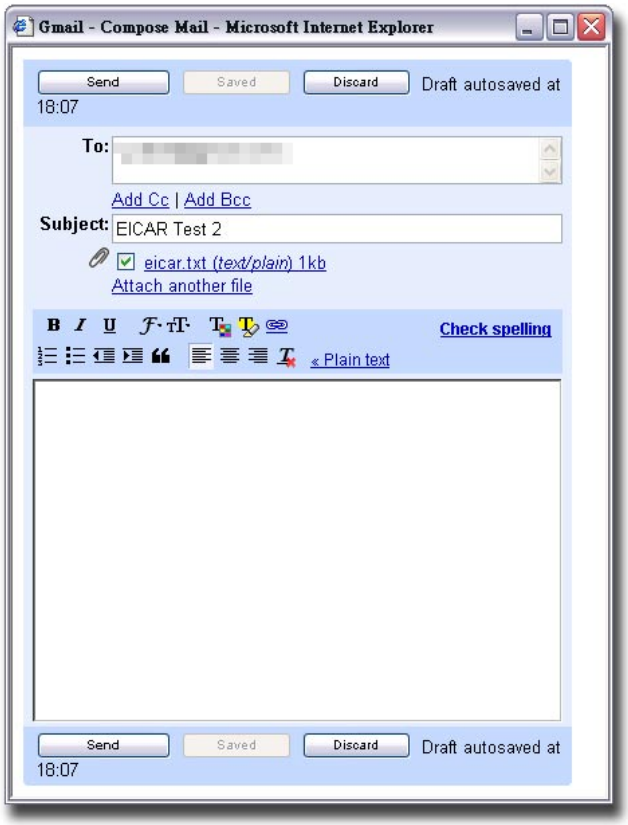
The purpose of it is to see whether the virus scanning engine will scan all contents of the email or solely the attachments. The following image shows the result:



Apparently the engine does not scan the message body.

Test 2 – EICAR plain text file attachment

Gmail had already blocked any file attachments with executable file extensions before the introduction of the virus scanning feature. Therefore a plain text file "eicar.txt" containing a line of EICAR message was produced. It was then appended onto the email as a file attachment:



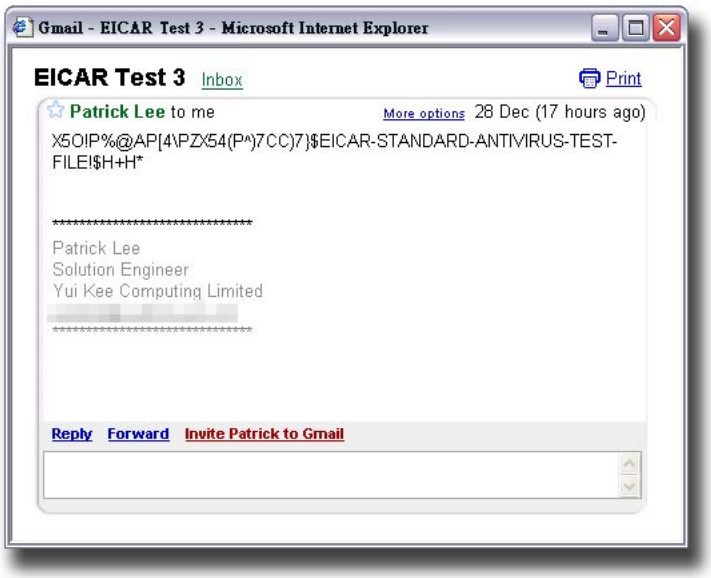
A few seconds later, because of the modifications on the message, the email had been saved as a drafted message automatically.

Upon trying to send email manually, the following alert dialogue popped up:

The system did not tell you what was happening. The same response was received using Mozilla Firefox. Probably the virus scanning engine detected the file attachment as a malware, even though it was not in an executable file extension.

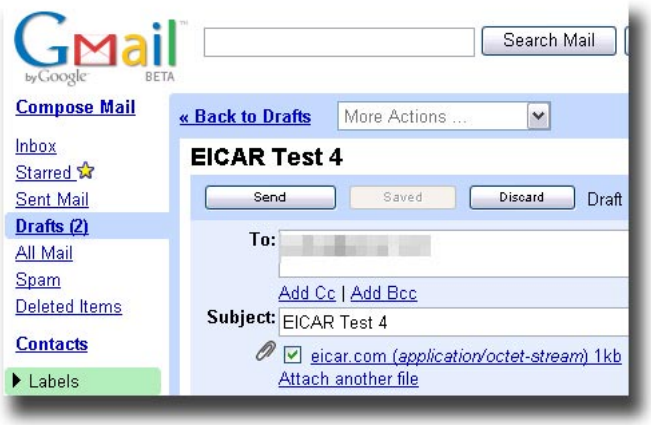
Test 3 – Incoming Plain text EICAR message

This test was similar to test 1, but on the other way round. An incoming message containing the EICAR text string was sent and it did not get blocked by the virus scanning engine:



Test 4 – Drafted message with EICAR file

From test 2 we can see that a message could be saved automatically as a drafted message once it had been modified. The drafted message would then be saved in the drafted message folder, namely the "Drafts" tab.



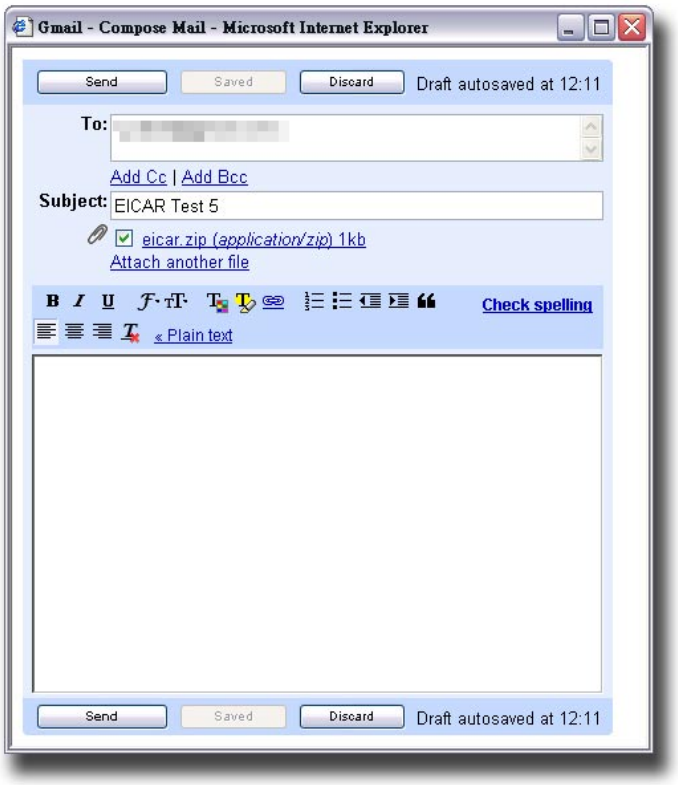
It was surprising that the EICAR file could be downloaded. Consider the following scenario:

Machine A has been infected and the user is unaware about it. The user tries to send an infected file using Gmail (of course presumably the user does not know the file is infected). Gmail responses with the dialogue found in test 2. The user thinks that it might be the problem of Machine A. "Luckily" the whole message has been auto-saved in the "Drafts" tab, the user uses another computer Machine B and try to send the mail again (which will not work), or even download and execute the infected file.

The above scenario is not uncommon. Because of the gigantic storage of Gmail (more than 2.5GB total file size limit per user account), some users misuse it as a medium of mobile file storage by sending files to their own Gmail accounts. Malware could be transferred in such way if the drafted message folder has not been scanned.

Test 5 – Zipped EICAR file

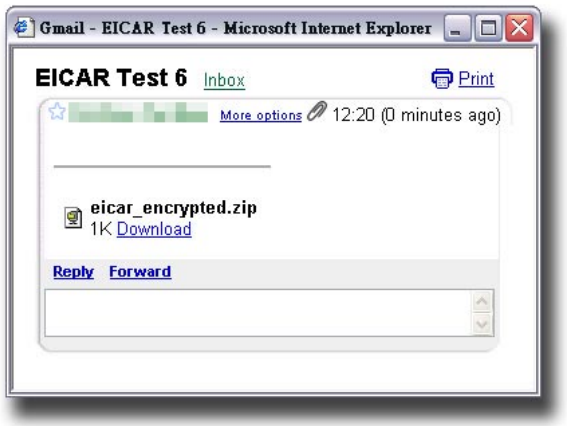
The EICAR file was zipped and was tried to be sent. Gmail prohibited the sending action by the same dialogue from test 2. Unfortunately the message was auto-saved as a drafted message.



Test 6 – Encrypted zipped EICAR file

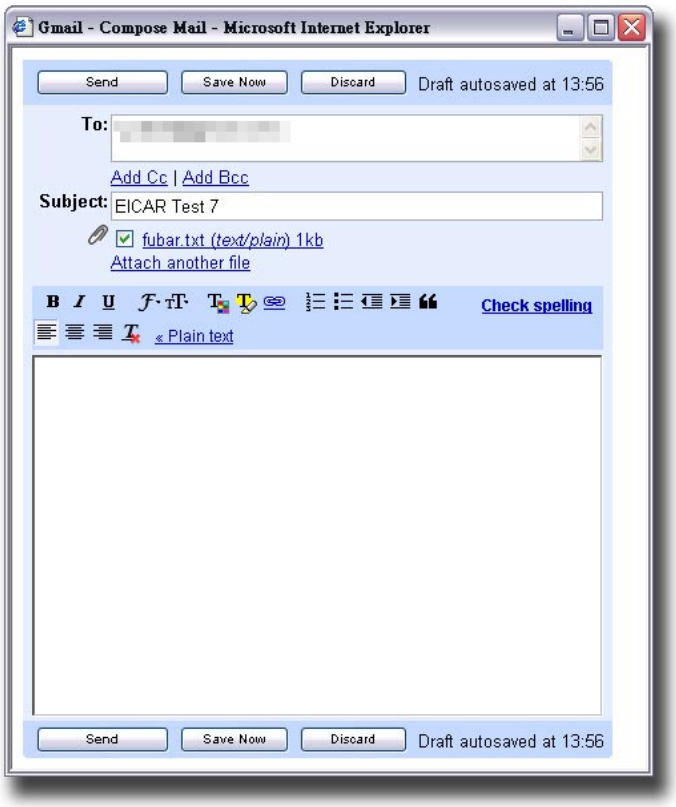
This time the EICAR text file was zipped with password encryption.

The email could be sent successfully.



Test 7 – Control Experiment

This test acted as a control experiment. An arbitrary text file named "fubar.txt" (with the text string "fubar" inside the file) is attached to the email:



Of course the email was sent and received successfully.

Conclusion:

We did not test the detection strength of the anti-virus engine on Gmail, the responses and behaviours of Gmail are similar to any ordinary mail gateways with anti-virus protection, for example, encrypted attachments are not scanned.

The responses presented to users did not always clearly indicate the problem: there is room for improvement in this area.

The behaviour of Gmail with drafted messages is a matter of concern: draft messages with infected attachments are saved and can be retrieved later, quite possibly on a different computer. Gmail can therefore help to spread viruses. The fact that some users make use of Google as a mobile file store means that there is a real threat here. The developers of Gmail should ensure that the drafted messages are also scanned.

References:

Anti-Virus Help Centre of Gmail:

http://mail.google.com/support/bin/topic.py?topic=1567

Note that the explanation of "what is a virus?" is inadequate: no mention of replication is made:

http://mail.google.com/support/bin/answer.py?answer=25759&topic=1568

How to make the CME Initiative Useful

The SANS Handler's Diary has made the useful observation and recommendation for improvement that the CME identifiers lack "additional incident response information". While it is possible to read a participating AV developer's description of a virus, and use the link to find the entry in the CME database, there are no links back. You cannot easily get from the CME entry to the descriptions on all the AV developer's sites.

The reverse links would greatly improve the usefulness of the CME database.

More information:

http://isc.sans.org/diary.php?storyid=895

http://cme.mitre.org/

The Human Factor

Humour:

http://rwanner.blogspot.com/2005/11/human-side-of-security.html

"Titan Rain": Chinese Military Hacking US?

The US military has tracked the activities of a group of perhaps 20 hackers that have been gathering military secrets from the US Defense Department and other agencies. The attacks have been traced to Guangdong and Alan Paller, the director of the SANS Institute pointed to the "intense discipline" of the attackers as evidence of their military training, they "were in and out with no keystroke errors and left no fingerprints, and created a backdoor in less than 30 minutes. How can this be done by anyone other than a military organization?"

Paller commented that espionage is not uncommon among Governments, "Governments will pay anything for control of other governments' computers. All governments will pay anything. It's so much better than tapping a phone".

The UK Government has also cited attacks from the "Far East" as a cause for concern.

Of course, an elite force of highly disciplined military hackers might think of the possibility of counter-intelligence and decide to hide their origin. They might choose to take over a poorly-protected PC to use as a launching point for their attack, say in an area with high growth of broadband connectivity, where there will be many users getting an always-on connection for the first time. Beware of the Zombies: do you know which Government your PC is hacking today?

More information:

http://www.terra.net.lb/wp/Articles/DesktopArticle.aspx?ArticleID=260955&ChannelId=16

http://news.zdnet.com/2100-1009_22-5969516.html

http://www.time.com/time/archive/preview/0,10987,1098961,00.html

http://news.zdnet.com/2100-1009_22-5967532.html?tag=nl

http://news.zdnet.com/2100-1009_22-5749594.html?tag=nl

Guidance Software Hacked

California-based Guidance Software, the developer of the well-known EnCase forensic software, has notified customers that a November attack on its databases compromised the details of about 3,800 credit cards. Californian law obliges companies to disclose information security breaches.

More information:

http://www.channelregister.co.uk/2005/12/20/guidance_security_breach/

In the Courts: eBay DDoS Culprit

An Oregon man has pleaded guilty to launching a DDoS attack against eBay. Anthony Scott Clark, 21, of Beaverton, Oregon, USA and his accomplices took control of 20,000 computers and used them to flood sites including eBay, causing “at least” US$5,000 in damages over a period of one year.

More information:

http://www.theregister.com/2005/12/28/ebay_bots_ddos/

Sober Worm Tricks Paedophile

Like many other worms, Sober tries to use social engineering to encourage recipients to open the attachments of its emails. Sober.Y, or perhaps Sober.Z, sends a message that claims to be from the Police (FBI, CIA, or the German BKA), saying that visits to illegal websites have been detected, and the recipient should fill in the attached questionnaire. A resident of Padenborn, Germany received one of these messages and turned himself in to the Police, who found pornographic images of children on his computer.

A police spokesman commented, "It just goes to show that computer worms aren't always destructive". A fairer comment might be that stupid criminals get caught.

More information:

http://www.f-secure.com/weblog/archives/archive-122005.html#00000745

http://www.sophos.com/pressoffice/news/articles/2005/12/soberzcrim.html

http://www.presseportal.de/polizeipresse/p_story.htx?nr=764168&firmaid=55625&keygroup

http://www.theregister.co.uk/2005/12/20/sober_worm_nets_criminal/

http://www.theinquirer.net/?article=28461

http://today.reuters.com/news/NewsArticle.aspx?type=internetNews&storyID=2005-12-20T095144Z_01_ROB035477_RTRUKOC_0_US-CRIME-GERMANY-WORM.xml

Sue A Spammer

Internet businessman Nigel Roberts has won a landmark legal victory by chasing down a UK spammer and winning £300 in costs by applying EU law.

He is now developing a website to help others to do the same.

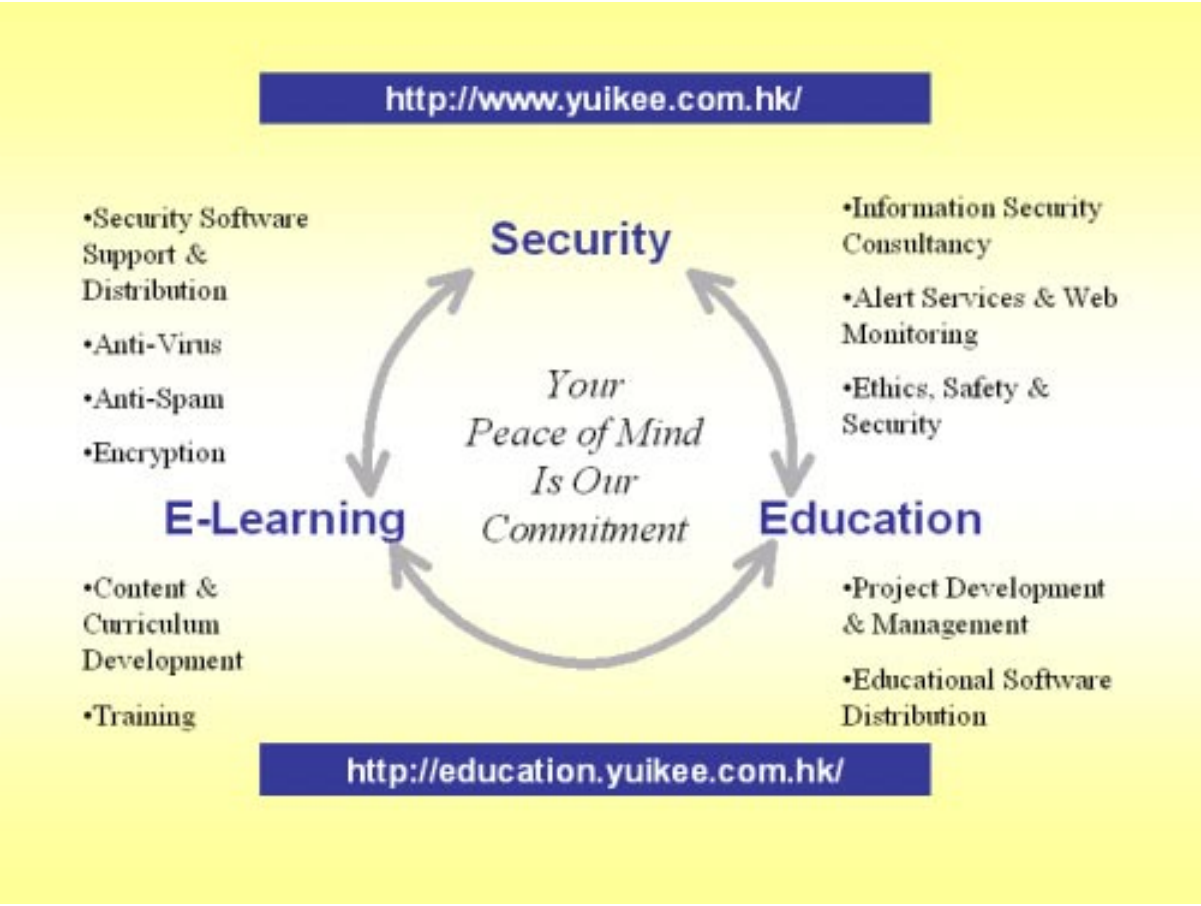
More information:

http://www.theregister.com/2005/12/29/uk_spam_win/

http://www.spamlegalaction.co.uk/

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: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/


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/