Yui Kee Computing Ltd.

Newsletter

September 2005

Contents

Incident Update

- Tue Sep 13 17:16:36 2005 CA: Win32.Mydoom.O Medium
- Mon Sep 19 23:31:24 2005 FSC: Bagle variant spammed as TEXT.EXE 2
- Sat Sep 24 05:01:07 2005 CA: Win32.Mydoom.O Medium

Yui Kee in the News

Our Chief Consultant has a column about anti-spam legislation in Computer World HK:

http://www.cw.com.hk/computerworldhk/article/articleDetail.jsp?id=177443

A Rose by any other name…

Microsoft's spin department is working hard, in a statement reacting to a vulnerability report the company said, "this attempt to bypass these features is not a software security vulnerability, but a function within the operating system that could be misused."

More information:

http://www.theregister.com/2005/08/31/spyware_writers_get_more_sophisticated/

http://isc.sans.org/diary.php?date=2005-08-25

The End of Email?

Perhaps the largest ISP in Hong Kong has introduced a policy to control the number of recipients per mail and rate limit the number of mails send from each mail server within a minute. Why?

The obvious answer is to reduce spam, but a moment's thought reveals that these measures are ineffective against the worst spammers, who are using illegally gathered botnets. Those spammers can easily split the spam to the ISP over thousands of zombies, so the rate limit and recipients per mail limit are never exceeded.

Conversely, the policy is disruptive to organisations with legitimate mailing lists using a single server who are trying to be efficient in the use of resources. Although bandwidth is now a lot more abundant than when SMTP was designed, transferring a message once for delivery to all the recipients at a site obviously reduces traffic.

Spam is slowly killing email; do we need the policies of shortsighted ISPs to make things worse?

Bait and Switch?

Microsoft as a leading member of the Trusted Computing Group (TCG), has been working hard to define a Trusted Platform Module (TPM) and a Best Practices document for building systems around a TPM. Microsoft is also working hard to produce its "next generation" operating system, Vista, which has been touted as the secure future of computing ever since it was called Longhorn. Now, Microsoft is apparently stalling the TCG to make sure that the Best Practices document will not apply to Vista.

More Information:

http://www.theregister.com/2005/09/02/vista_trusted_computing_controversy/

http://en.wikipedia.org/wiki/Bait_and_switch

http://www.microsoft.com/resources/ngscb/default.mspx

http://news.com.com/Something+fishys+going+on/2010-7350_3-5844412.html

http://it.slashdot.org/it/05/09/01/1419222.shtml?tid=172&tid=109

Firefox Security Flaw

It isn't only Internet Explorer that has security flaws. Peter Zelezny has found one for Firefox. Users should upgrade to version 1.0.7.

http://www.theregister.com/2005/09/21/linux_firefox_security_bug/

http://www.mozilla.org/products/firefox/

Potter and Security

J. K. Rowling's books about the young wizard, Harry Potter, come under the critical eye of security analysis. Encouraging people to think, even in an area where the author is not an expert, is surely a useful function of literature.

The discussion on transitive betrayal of trust is wrong to put forwards the death of Harry's parents as an example. Sirius Black did not make Peter Pettigrew the Potter's Secret Keeper, he persuaded the Potters to do so – the trust was direct, the advice was flawed. In fact, the Fidelius Charm appears capable of entirely preventing transitive betrayal of trust – in the "Order of the Phoenix", Snape and Kreacher are unable to name the location of the Order's Headquarters. Even more astounding, Voldemort's followers are unable to deduce its location from the facts

that Kreacher has seen certain Order members, and Kreacher is a house elf, normally limited to a single location, that some of Voldemort's followers have undoubtedly visited previously. The power of the charm is demonstrated in the scene when Harry arrives at the Headquarters – until the Secret Keeper tells him the location, it simply does not exist for him.

Fred Cohen notes that limited transitivity is one of the three perfect defences against computer viruses. Limited transitivity is also a requirement of unbreakable DRM. A working Fidelius Charm would therefore be extremely valuable.

More information:

http://www.veryard.com/trust/potter.htm

http://ritestuff.blogspot.com/2005/08/harry-potter-and-half-assed-security.html

What is friendship worth?

About US$0.02, judging by a recent spam message (see text box).

```
From: NOT SPAM <***@***>


Hey man/woman,

 I'm here to tell you that ************* is a REALLY
great website and you should please visit them
today!!!! Visit us today, fullfilling your PHP needs!!!
***

Please spread the word about our website and our
scripts!!! Forward this email to 250 people and we'll
pay you $5.00 US dollars via paypal.


Thank you,

Patatten Boerken

***

NOTE: THIS MESSAGE IS NOT SPAM and your email was
obtained from legal sources.
```

The sender is apparently trying to co-opt people as spammers for a payment of just US$5 for 250 contacts. Aren't your contacts worth more than that?

It seems likely that even this derisory offer is insincere. It is too similar to the well-known Bill Gates giveaway hoax (see Snopes, Vmyths and Urban Legends for details) and the same questions arise: how is it possible to verify who forwarded the message, and why would anyone pay money for an unverifiable claim?

The message also shows two common spammer misconceptions (or, in all likelihood, something the spammer does not believe, but they would like the recipients to believe it):

i) It is not spam if it shows the words "not spam" (with extra effectiveness for using ALL CAPS, repeating the phrase *and* repeating the phrase).

ii) Obtaining an address by "legal means" automatically makes a message wanted.

Critical Vulnerabilities

Microsoft has announced that there is a critical vulnerability in Windows, but has had to delay release of the patch to fix it because of "quality issues".

More information:

http://www.theregister.com/2005/09/14/secfocus_patches/

Airport Lounge Security

Curiosity and boredom prompted, Scanit, a company that specializes in network security audits, to examine what had been left on public access terminals in airport executive lounges. They found confidential emails, and valuable contract documents. Some were also infected with backdoors. The lounge staff said they were not responsible for the machine's security.

More information:

http://www.theregister.com/2005/09/21/airport_pc_security_lax/

"We Know Where to Find You"

The NSA has patented (US patent 6,947,978) a method for locating Internet users based on their IP address by using the latency of connections with a network topology map. The highly secretive US Government agency cites geographically targeted advertising, disabling use of a password from a computer located outside of a specified area and signals intelligence as possible applications.

Depending on the accuracy, the technology might also be useful for tracing the origin of emergency phone calls over VOIP connections.

More information:

http://www.theregister.com/2005/09/22/nsa_geolocation_patent/

http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=6,947,978.WKU.&OS=PN/6,947,978&RS=PN/6,947,978

Cardtrap Infects Phones and PCs

SymbOS/Cardtrap.A is otherwise unremarkable Symbian trojan, except that it also tries to infect users PC if user inserts the phone memory card to PC. Currently, many corporate malware outbreaks occur when a user connects an infected laptop to the internal network, bypassing the strong perimeter defences. In future, the problem might be users with phones.

More information:

http://www.f-secure.com/v-descs/cardtrap_a.shtml

http://www.theregister.com/2005/09/22/pc_hopping_symbian_trojan/

http://www.f-secure.com/weblog/archives/archive-092005.html#00000659

http://www.sarc.com/avcenter/venc/data/symbos.cardtrp.a.html

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=SYMBOS%5FCARDTRP%2EB

Profiling for Terrorists Catches Techie

London Police arrested David Perry, computer and telecoms enthusiast and former editor of EXE for suspicious behaviour including wearing a rucksack containing a laptop and fiddling with a mobile while waiting for the tube. David comments, "at least I'm still alive".

Meanwhile, Hong Kong Police are making careful security preparations for the Hong Kong Ministerial Conference of the World Trade Organization, to be held in Wan Chai in December. Wan Chai also contains two busy computer malls, the offices of numerous technology companies and an MTR station. Naturally, the Police are liasing with their counterparts in other

countries, including Britain. Hopefully that means learning from their mistakes, not simply applying the same, flawed methods.

More information:

http://digital.guardian.co.uk/guardian/2005/09/22/pages/ber1.shtml

http://gizmonaut.net/bits/suspect.html

http://www.theregister.com/2005/09/23/terror_profile_techies/

http://gizmonaut.net/bits/profiling.html

http://www.wtomc6.gov.hk/eng/home/welcome.html

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/