Yui Kee Computing Ltd.

Newsletter

October 2005

Contents

Incident Update

- Mon Sep 19 23:31:24 2005 FSC: Bagle variant spammed as TEXT.EXE 2
- Thu Oct 6 11:01:19 2005 NAI: W32/Sober.r@MM Medium
- Thu Oct 6 15:46:26 2005 CA: Sober.P Medium
- Thu Oct 6 19:01:21 2005 FSC: Sober seeded worldwide 2
- Thu Oct 6 22:01:22 2005 TREND: WORM_SOBER.AC Medium

Social Engineering Variants: Sober Distribution

At one time, social engineering in malware meant, "claiming a dangerous email attachment contains pictures of a beautiful woman". The criminals behind the Sober family of malware seem determined to expand this definition as much as possible, previously, Sober.N posed as an offer for soccer World Cup tickets and this month Sober.O has claimed to be a message from an old school friend. Some variants of Sober have been used to distribute neo-Nazi spam.

More information:

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

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

http://www.theregister.com/2005/10/06/sober_schoolfriend_pic_viral_ruse/

http://www.sophos.com/virusinfo/articles/sobero.html

Reptile Fashion

Recognising the value of publicity, the tiny Cornish village of St Blazey has acquired a rouge reptile, apparently in emulation of Hong Kong's own crocodile, Pui Pui. There are no reports of the two-foot caiman's capture.

Will this become a fashion for publicity-seeking towns?

More information:

http://www.theregister.com/2005/10/06/cornish_gator_alert/

http://news.bbc.co.uk/1/hi/england/cornwall/4309590.stm

http://www.ananova.com/news/story/sm_1561232.html

http://www.rspca.org.uk/servlet/Satellite?pagename=RSPCA/RSPCARedirect&pg=NewsFeature&articleId=1128415205528&marker=1

http://www.info.gov.hk/gia/general/200408/12/0812113.htm

http://www.info.gov.hk/gia/general/200406/23/0623141.htm

Taiwan vs. Google vs. China

First Taiwan noticed that Google Earth labeled the island a "province of China", and complained. Google changed the label. Then, naturally, China (through Peng Keyu, consul general of the Chinese consulate in San Francisco) complained that the label had been changed.

Maps should reflect reality, and the reality is that the Taiwan Straits are significantly different to any other boundary between Chinese provinces, certainly in terms of travel restrictions. Now, how do you say that without offending anyone?

More information:

http://www.theregister.co.uk/2005/10/04/taiwan_google_earth/

http://www.theregister.co.uk/2005/10/20/china_google_strop/

http://www.taipeitimes.com/News/front/archives/2005/10/04/2003274363

http://www.pekingduck.org/archives/003025.php

http://www.20six.co.uk/Angrychineseblogger/archive/2005/10/05/w24o72zj96xd.htm

http://www.physorg.com/news7400.html

http://www.pandia.com/sew/98-on-googles-taiwan-blunder.html

Virus Naming

US-CERT has launched its Common Malware Enumeration initiative. The initiative aims to:

- Reduce the public's confusion in referencing threats during malware incidents.
- Enhance communication between anti-virus vendors.
- Improve communication and information sharing between anti-virus vendors and the rest of the information security community.

It will work in a similar manner to the existing Common Vulnerabilites and Exposures (CVE) initiative. Each major threat will receive a unique tag, of the form CME-*number*.

Many developers, including Sophos and F-Secure, have started listing the CME identifiers in their virus descriptions.

Virus naming inconsistencies have plagued developers and users for years, and this identifier will not solve the problem, though it might mitigate it. Detractors, including David Perry of Trend Micro, say it might just make things more confusing.

More information:

http://cme.mitre.org/

http://cme.mitre.org/community/prod_serv.html

http://www.theregister.com/2005/10/06/virus_naming/

Is SPF “Worse Than Usless”?

Heavyweight anti-virus researchers Nick Fitzgerald and Vesselin Bontchev have clashed at the Virus Bulletin Conference in Dublin over the utility of SPF (Sender Policy Framework). Nick attacked SPF as “broken” as an anti-spam measure because it is trivial to break and that it tells us nothing about the actual sender or “spaminess” of the message. He also pointed out that botnets could easily be used to send SPF-compliant spam.

Vesselin Bontchev pointed out that that would only work for organizations that do not filter their outgoing mail and that ISPs could use the information to identify compromised PCs.

Our Chief Consultant, Allan Dyer, gives his opinion:

I think Vesselin is missing a trick by bringing in the ISP - Nick is right, ISP's don't have the motivation or margin to follow up these cases (see related story, “Déjà vu: HKISPA Gets Tough on Spam?”, below).

The reason why an organisation should want to publish an SPF record is to protect its reputation; email "rom" their domain, arriving from an unlisted IP address is bogus. If the organisation becomes infested with zombies, with the result that the listed mail servers are sending out spam in the organisation's name, they have extremely high motivation to clean up immediately. Recipients can contact the domain's postmaster, and expect immediate response, or conclude that the spam is authorised from the organisation.

The second reason to publish an SPF record is the hope of reducing the number of bounce messages to non-existent users - if the receiving mail server had checked the SPF record, the reject message would not have been sent.

Some anti-spam developers refuse to implement SPF checking in their products, saying that it is easily broken, not very effective, and will not do much to improve their already excellent spam detection accuracy.

I disagree. It is comparable to the MX record in strength. It is effective at preventing machines outside of your domain pretending to be you (Nick's objection is that it does not defend against spam being sent from your machines, when they have been compromised by zombies - if that is the case, you have a massive security breach, and sending spam is just one of your problems).

The effectiveness is limited by its adoption. Publishing an SPF record is cheap (a simple DNS update), and anti-spam vendors could make a major difference to its adoption in receiving servers.

The argument that it will not do much to improve “already excellent” spam detection accuracy is empty – these products use many techniques to give a final result better than any individual technique. So the same argument could be made against any other technique - it could be removed from the cocktail with very little effect on the final result.

Two questions:

As a domain owner, you can make a one-line change in your zone file to allow recipients to easily identify forged mail supposedly from your domain. What is your justification for not doing so?

For the anti-spam developers, some domains are choosing to publish information to help recipients identify which messages are from authorised servers, why are you choosing to ignore that information?

More information:

http://www.theregister.co.uk/2005/10/10/spam_user_authentication_is_ineffective/

http://news.zdnet.co.uk/internet/security/0,39020375,39228023,00.htm

http://www.emailbattles.com/archive/battles/spam_aabhifdicc_ji/

Self-Replicating Code is Dangerous

Players in the "World of Warcraft" online game have suffered a demonstration of the dangers of self-replicating code. The designers of the game added a monster that could inflict a self-propagating disease on player characters, but did not limit the ability of the disease to spread. Consequently, the disease spread out of control, making the whole game almost unplayable, and spoiling the fun of many players.

The game's developer, Blizzard Entertainment, modified the disease so that spread was limited to certain game areas, thus stopping the epidemic.

This incident takes place in a game and stretches the limits of the definition of a computer virus, but it is a reminder of the dangers of any self-replicating code.

More information:

http://www.securityfocus.com/news/11330

F-Secure DoS

On October 18, F-Secure's external web site www.f-secure.com experienced a denial of service attack. The attack lasted for a few hours but F-Secure was succesfully able to control it.

http://www.f-secure.com/news/items/news_2005101800.shtml

DNS Security

A survey by the Measurement Factory has found that 84% of authoritative Domain Name Servers might be vulnerable to attack by DNS cache poisoning or domain hijacks.

More information:

http://www.theregister.com/2005/10/24/dns_security_survey/

http://dns.measurement-factory.com/surveys/sum1.html

http://www.measurement-factory.com/press/20051024.html

Define Spyware

The Anti-Spyware Coalition (ASC) has defined what it is about. The group of software companies, security firms and consumer groups considers spyware as deployed without appropriate user consent and/or implemented in ways that impair user control over: material changes that affect their user experience, privacy, or system security; use of their system

resources, including what programs are installed on their computers; and/or collection, use, and distribution of their personal or other sensitive information.

http://www.theregister.com/2005/10/28/anti-spyware_defs/

Virus Writers Jailed

Newcastle Crown Court has jailed Andrew Harvey (23) from Durham and Jordan Bradley (22) from Darlington for conspiring to "effect unauthorised modifications to the contents of computers with the intent to impair the operation of those computers". They pleaded guilty to the offences related to writing the “TK Worm”, and early botnet client, in 2003. The pair were members of a gang called “THr34t Krew".

More information:

http://news.bbc.co.uk/2/hi/uk_news/england/4319942.stm

http://www.nationalcrimesquad.police.uk/media/article.jsp?id=126

http://www.evalu8.org/staticpage?page=review&siteid=9614

http://www.f-secure.com/weblog/archives/archive-102005.html#00000673

Déjà vu: HKISPA Gets Tough on Spam?

The Hong Kong Internet Service Providers Association issued an Anti-Spam Code of Practice in June 2005. Widely unreported, this is, in fact, the second version of this Code. However, unlike the previous version, this has resulted in positive action: at least one ISP (namely, Pacific Internet) has sent a letter to its customers stating that it will carry out a series of security measures to comply with the Code.

Version one of the Code, published February 2000, received significant press coverage, but there was no evidence of any action. In fact, although the Code stated that a list of compliant ISPs would be posted on the HKISP website, the list was never published, and there was no response to repeated requests for the list. Version 2 also includes provision for:

“A web site run by the HKISPA showing this Code of Practice and the parties that are in compliance.”

But, to date, there is no sign of the list.

The Code includes these technical measures:

1. Mail servers shall not be allowed to relay mail from third parties.
2. There shall be a restriction on the amount of outgoing mail provided for web e-mail and pre-paid accounts.
3. All clients using switched access shall not have outgoing TCP access to the Internet on port 25 (SMTP). An SMTP server shall be provided by such accounts; if possible the users outgoing SMTP connection will automatically be redirected to such server.

The first two are “no-brainers”, the third uses the term “switched access”, possibly using the term in the telecoms industry sense of an occasionally connected circuit. However, the wording used in the ISPA’s Implementation Guidelines is “switched dialup access”, is this an intentional change, indicative of a change in the Code? On the one hand, nowadays restricting port 25 access for dialup connections is fairly irrelevant – most spam is sent via zombies on broadband connections, so extending the coverage to other connections is sensible. On the other hand, is restricting port 25 access an unfair limit on competition? Will ISPs coerce users into using their mail servers for their domains on the pretense of “security”? A reasonable solution that allows competition without compromising security is to block port 25 by default, but to open it, at no charge, on a signed request from the customer. The ISPs can then contribute to the fight against

spam by blocking spam from the machines most likely to be zombie-infected, while allowing customers who can take responsibility for their systems the freedom of choice.

More information:

http://www.hkispa.org.hk/antispam/cop.html

http://www.hkispa.org.hk/antispam/guidelines.html

http://www.pco.org.hk/english/infocentre/press_20000215.html

http://www.info.gov.hk/gia/general/200002/15/0215135.htm

http://www.ofta.gov.hk/en/junk-email/main.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/