Yui Kee Computing Ltd.

Newsletter

December 2004

Contents

Editors Notes

It seems petty and irrelevant to write about information security shortly after an enormous natural disaster, but I am sure the readers of this newsletter are capable of making their own compassionate decisions. Rob Rosenberger has some comments (http://www.vmyths.com/rant.cfm?id=697&page=4) about companies that issue special press releases for unrelated news events.

Incident Update

- Thu Dec 2 14:46:31 2004 TREND: MS04-039_ISA_SERVER Medium
- Thu Dec 2 17:01:53 2004 TREND: MS04-040_INTERNET_EXPLORER High
- Mon Dec 13 17:31:44 2004 TREND: WORM_NETSKY.P Medium
- Mon Dec 13 18:31:54 2004 TREND: WORM_SOBER.I Medium
- Tue Dec 14 22:01:56 2004 FSC: Zafi.D sends fake Christmas Cards 2
- Tue Dec 14 22:46:41 2004 NAI: W32/Zafi.d@MM Medium
- Wed Dec 15 00:02:21 2004 NORMAN: Nocard.A Medium
- Wed Dec 15 00:31:48 2004 TREND: WORM_ZAFI.D Medium
- Wed Dec 15 02:02:19 2004 NORMAN: Zafi.D Medium
- Wed Dec 15 10:16:29 2004 SARC: W32.Erkez.D@mm L3
- Wed Dec 15 12:01:53 2004 TREND: MS04-043_HYPERTERMINAL High
- Wed Dec 15 13:16:30 2004 TREND: MS04-041_WORDPAD High
- Wed Dec 15 15:01:47 2004 TREND: WORM_ZAFI.D Medium
- Wed Dec 15 19:46:32 2004 TREND: MS04-045_WINS High
- Fri Dec 17 13:46:39 2004 TREND: MS04-044_KERNEL_AND_LSASS Medium
- Fri Dec 17 13:46:39 2004 TREND: MS04-042_DHCP Medium
- Tue Dec 21 12:16:39 2004 TREND: WORM_MUGLY.C High
- Wed Dec 22 02:46:35 2004 FSC: New worm defacing phpBB forum sites 2
- Thu Dec 30 07:02:08 2004 CA: Win32.Netsky.Z

CPCNet Attempts to Block Yui Kee's Communications

Not satisfied with threatening to cut Yui Kee's leased line connection to the Internet, CPCNet also tried to stop Yui Kee communicating with the Press. On 14 December, Yui Kee received a letter from CPCNet's solicitors, claiming that Yui Kee's 23 November Press Release (titled 'Yui Kee Warns: CPCNet Puts Customers At Risk; OFTA Adopts a "Hands Off" Position') was "untrue, unfair and probably defamatory". Allan Dyer rejected the accusation, writing in a letter to CPCNet's solicitors on 15 December, "The press release is a true and fair representation of the situation on 23rd November, and of my opinions about the situation."

Although the solicitors wrote in the 14 December letter that CPCNet would consider immediate legal action if Yui Kee did not withdraw the press release, nothing further has been received on this matter. Dyer commented, "This looks like an intimidation tactic, they would be unwise to proceed because their claim has no validity."

CPCNet did, however, cut Yui Kee's leased line shortly after 18:00 on 31 December 2004. Yui Kee still regards this as outside of their contract terms with CPCNet, and a possible violation of the Telecommunications Ordinance. OFTA did suggest that Yui Kee should take the case to arbitration, but the Hong Kong International Arbitration Centre can only become involved if the parties agree to arbitration. "We did ask CPCNet to go to arbitration, but they gave no response before terminating the connection. I guess that is a non-verbal response", explained Dyer.

However, if CPCNet's aim was to isolate Yui Kee, the attempt has failed, as receipt of this electronic newsletter demonstrates. "Our aim was to replace our leased line connection with multiple broadband connections, so we already had an alternate route in place", Dyer explained. Although connectivity was maintained, it was still necessary to update records at the Hong Kong Domain Name Registry, delete obsolete routes, and remove obsolete IP addresses from host configurations.

Although the impact on Yui Kee's communications was minimal, there is still the issue of the effect of CPCNet's terms and conditions on other customers. "Essentially, CPCNet's standard terms and conditions prohibit effective communications with anti-virus suppliers. Organisations should consider moving to other ISPs before they find themselves caught in a choice between sending an urgent sample by snail mail, or sending it quickly and having CPCNet terminate their connection", concluded Dyer.

Test Your Website Design

SiteScore (http://sitescore.silktide.com/) tests and scores the design of your website. Some sample scores for your amusement:

http://www.ofta.gov.hk/	6.6
http://www.cpcnet-hk.com/	6.0
http://www.sophos.com/	8.3
http://www.yuikee.com/.hk	6.1
http://www.microsoft.com	8.9
http://www.cpan.org	8.3
http://www.opera.com	9.5
http://sitescore.silktide.com/	8.4

However, providing disabled access appears to be difficult, every site seemed to get "This website appears to be in violation of the British Disability Discrimination Act" in its report - including Silktide itself.

Dutch advertising board Explains Viruses to AMD

Reclamecode Commissie, the Dutch advertising board, says that AMD's adverts, which claim users of its Athlon 64 processors don't have to worry about viruses, are misleading.

http://www.theregister.com/2004/12/24/amd_dutch_ads/

Network World selects Sophos PureMessage as a favourite among dozens of leading spam solutions

Network World, a leading US IT Magazine, has selected Sophos PureMessage as a 'favourite' among the leading anti-spam software providers in the publication's recent "Spam in the Wild, The Sequel" review.

The product review compared anti-spam software products, managed services, and appliances from 35 different companies to determine which solutions were most effective at stopping spam and keeping legitimate email flowing. The test looked at four key areas: spam-oriented features, per-user features, anti-virus and policy-based filtering, and logging and management.

Looking closely at policy-based controls, "The clear king of email policy is Sophos PureMessage. Beautifully integrated with Sophos's virus-scanning tools, PureMessage lets you construct any policy you want. For example, if you want to completely drop some of your incoming virus-infected email but try to clean or quarantine others, you can do it. No other product comes close to this functionality."

Each product or service tested filtered more than 10,000 emails and was measured for accuracy of spam filtering technology and rate of false positives. Of the top products tested, Sophos PureMessage offered a .04% false positives rate, sharing the top spot with just one other vendor.

"The network security landscape is certainly far more complicated than ever before," said Steve Munford, president of Sophos Inc. "As a global provider of integrated security software to businesses, Sophos offers a unique combination of expertise and leading anti-virus, anti-spam and email policy solutions, allowing organizations to stay one step ahead of evolving and intensifying threats to network security."

Sophos PureMessage is available from Yui Kee, please contact us to arrange an evaluation.

More Information:

http://www.nwfusion.com/reviews/2004/122004spamanalysis.html

http://sophos.com/pressoffice/pressrel/us/20041223network.html

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

•Content & Curriculum Development

•Training

Education

•Project Development & Management

•Educational Software Distribution

http://education.yuikee.com.hk/