Yui Kee Computing Ltd.

Newsletter

February 2007

Contents

Vista Security

A number of security researchers have been investigating Vista's improved speech recognition features and found they could create MP3 or other audio files which would cause Vista to delete files and visit arbitrary websites. Such files could be hosted on malicious websites or P2P networks, and activated when the victim PCs are expected to be unattended. The technique could be used to download and run attack tools in a sophisticated attack.

Microsoft downplayed the scenario, saying that the exploit is technically possible but unlikely to be much of a threat in practice. Unfortunately, this is exactly how Microsoft has described previous vulnerabilities that later became a big threat. It is not possible to perform privileged functions, such as creating a user, by voice commands alone because the UAC prompt does not accept voice input *by default*. Microsoft also said that speaker and microphone placement, audio feedback and clarity of diction would make the attack difficult. Expect hackers to be well–spoken in future.

More information:

http://www.theregister.com/2007/02/01/vista_voice_recognition_attack/

Dutch Botnet Gang Sentenced

Two Dutch men, aged 20 and 28, were handed jail sentences of 18 months and 2 years and fines for creating Trojans and using them to build a botnet. As they had both served jail time, they were released at the beginning of February; however, one of the men has appealed the sentence.

The two were key members of a gang that created and distributed the Toxbot and Wayphisher Trojans in 2005, infecting millions of computers, stealing login credentials for eBay and Paypal accounts, credit card details, and blackmailing companies with DoS attacks.

Other suspects in the case have yet to be tried.

More information:

http://www.theregister.com/2007/02/01/dutch_botnet_gang_sentenced/

http://www.symantec.com/security_response/writeup.jsp?docid=2005-031012-0442-99

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

http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=22561

http://software.silicon.com/malware/0,3800003100,39165572,00.htm

http://www2.csoonline.com/blog_view.html?CID=28797

http://www.symantec.com/security_response/writeup.jsp?docid=2005-071312-5833-99&tabid=2

Spam Tracing

Outsourcing mass–mailings, or trading in address lists has risks.

Reports at The Register have traced spam sent on behalf of a large, well–known company. They found that, although the company, T-Mobile, officially had a policy of only using opt–in systems, they had outsourced the mailings to Quantum Media. Quantum Media subcontracted to Mailtrack Media, who used E-Mail Movers to send the messages, and provide the supposedly opt–in lists. E-Mail Movers got part of their list from Century Communications, which had bought the list of 200 million opted–in email addresses on eBay for £20. The seller assured them that the list was legitimate.

More information:

http://www.theregister.com/2007/02/01/t_mobile_spam/

Contact Form Attack

A UK–based security consultant has warned that the "contact us" feature on many corporate websites make it easy to launch DoS attacks on the organisation's mail servers. The situation can occur if the "contact us" feature generates an email to an internal server, an attacker can automate submissions with a script, potentially generating sufficient mail to overwhelm the mail server. Using a botnet to run the script would increase the potency of the attack.

More information:

http://www.theregister.com/2007/02/01/web_form_dos_risk/

More Vista Security

Microsoft's anti-virus product, Live OneCare, has failed to achieve a VB100 Award in the latest Virus Bulletin tests on Vista. Virus Bulletin tested fifteen products, and eleven passed. John Hawes, technical consultant at Virus Bulletin, commented, "Although many improvements have been made, Vista cannot fend off today's malware without help from security products".

More information:

http://www.theregister.com/2007/02/05/vista_security_criticisms/

http://www.virusbtn.com/vb100/archive/2007/02

Pegasus to Fly Again?

Last month's reports of Pegasus' demise appear to have been premature. Following a avalanche of messages, Pegasus author David Harris has decided to restart development with a different funding model, probably donationware.

However, IT columnist Verity Stob has urged him to “Give it up”, and possibly put it onto Sourceforge.

More information:

http://www.pmail.com/helpus.htm

http://www.theregister.co.uk/2007/01/24/pegasus_revival/

http://www.regdeveloper.co.uk/2007/02/06/pegasus_farewell/

Vista Security at the RSA Conference

Sir William Gates spoke at the RSA Conference in San Francisco, recommending IPv6 and IPsec combined with smart-card access as a better way to protect systems and users’ identities than passwords. He also announced that his company’s CardSpace system would collaborate with the OpenID initiative.

At the same conference, John Thompson of Symantec criticised Microsoft for a dangerous conflict of interest in selling both an operating system and security software. Thompson likened the conflict to combining your accountant and auditor.

More information:

http://www.theregister.com/2007/02/07/symantec_thompson_microsoft/

http://www.theregister.com/2007/02/06/gates_rsa/

DRM in Vista

Bruce Schneier has joined the debate on DRM in Vista on the side of Peter Gutmann, starting his essay with the words, “Windows Vista includes an array of "features" that you don't want.”

Full Essay:

http://www.schneier.com/crypto-gram-0702.html#8

Online Bank Heist

Swedish bank Nordea has hit the headlines as the target in what is claimed to be the world’s biggest online bank heist. It is thought that Russian organised crime managed to steal about €900,000 (HK$9,300,000) from user accounts during a fifteen–month period using specially–crafted trojans.

More information:

http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm

http://computersweden.idg.se/2.139/1.92479

http://securityblog.itproportal.com/?p=686

Chinese Police Release Fix by Fujacks Suspect

The Xinhua News Agency has reported that Hubei police intend to release a program claimed to clean up the Fujacks worm written by Li Jun, a suspect arrested for creating the worm. Li Jun claimed he wrote the anti–Fujacks program but did not release it because he feared it would lead police to him. The Fujacks worm is also known as "Xiongmao Shaoxiang".

The move has been criticised by security experts, including Graham Cluley of Sophos, citing that virus writers are untrustworthy and irresponsible. Cluley elaborated, “Additionally, the Fujacks virus left some infected files unable to run. That hardly suggests that the author took

quality assurance seriously when he constructed his malware. Our recommendation to computer users would be to clean their PCs with professional tools written by security experts."

More information:

http://www.networksasia.net/ena/article/articleDetail.jsp?id=405805

http://www.sophos.com/pressoffice/news/articles/2007/02/fujacks-fix.html

http://www.sophos.com/pressoffice/news/articles/2007/02/fujacks-arrest.html

http://www.sophos.com/pressoffice/news/articles/2007/01/fujacks.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: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/