NewsBriefs

BRANDI ORTEGA

Security

Enterpriseing organized crime gangs are now offering malware subscription services complete with technical support. Dubbed “managed exploit providers” by Gunter Ollmann, director of security strategies at IBM’s Internet Security Systems X-Force team, they offer malware subscriptions for as little as US$20 per month to spyware distributors and spammers. Additionally, the hacking gangs offer services such as detection monitoring, in which they’ll monitor antivirus products for new signatures and alert subscribers so they can release new malware variants.

A security researcher at Juniper Networks has discovered a new class of attacks that could let attackers run malicious software on network devices and steal sensitive information from mobile phones or redirect Internet traffic on routers. The attack’s developer, Barnaby Jack, says the vulnerability lies in the ARM and XScale microprocessors in embedded devices such as mobile phones and routers.

Described as “out of character” by security researchers such as Qualys’s Jonathan Bittle, Microsoft recently discussed the Windows animated (ANI) cursor vulnerability on its new security development life-cycle blog (http://blogs.msdn.com/sdl/archive/2007/04/26/lessons-learned-from-the-animated-cursor-security-bug.aspx). The vulnerability, which lets attackers take over PCs after they’ve been infected from visiting malicious sites or opening up malicious email attachments, was severe enough to prompt Microsoft to issue an out-of-cycle patch. On the blog, Michael Howard, Microsoft’s security program manager, outlined how the vulnerability found its way into Vista and the company’s development tools and processes.

In April, Laurent Butti, a security researcher at France Telecom Orange, unveiled a vulnerability in a major Linux Wi-Fi driver that could let attackers control machines, even when they’re not connected to a Wi-Fi network. The flaw affects the MadWi-Fi Linux kernel device driver for Atheros-based Wi-Fi chips. The MadWi-Fi development team released a patch for the flaw, and Butti advises users to manually patch their drivers.

F-Secure recently identified a worm that targets the Skype voice-over-IP (VoIP) application. Infected machines send instant messages (IMs) to users’ contact lists with a link to an executable file that downloads a Trojan; the worm also blocks incoming calls by setting Skype to “do not disturb” status, thus preventing users from responding to IMs. Users are advised to update and run their antivirus programs.

In April, researchers at the HotBots conference in Cambridge, Massachusetts warned of increasingly resilient botnets that take advantage of P2P architectures. Jose Nazario, a security engineer at Arbor Networks, calls P2P botnets, “the biggest challenge we’re facing.” P2P botnets aren’t new, but in a paper presented at the event, Julian Grizzard and his coauthors predict that “P2P botnets will mature to a level in which they might become more widespread than traditional decentralized C&C [command and control] architectures.”

In January, the TJX Company revealed that hackers stole at least 45 million credit- and debit-card numbers from its Marshalls, T.J. Maxx, HomeGoods, and A.J. Wright stores. In addition to financial data, hackers scored the driver’s license numbers, military service information, and social security numbers (SSNs) of 451,000 customers. Investigators believe the entry point into TJX’s computer systems was Wired Equivalent Privacy (WEP). Internal auditors also found that the company failed to install firewalls and data encryption on several wireless networks and incorrectly installed security software. The company admits that the exact amount of card numbers stolen will never be known because it deleted its own copies of the stolen records and has yet to crack the encrypted files the hackers left in the system. TJX is, of course, “sorry” and offers credit-monitoring protection to those whose SSNs were stolen.

According to a recent survey conducted by Centennial Software, roughly 38 percent of IT professionals viewed portable storage devices such as thumb drives and MP3 players as their number one security concern. Only 8 percent of the respondents reported a total ban on portable devices at their organizations; 80 percent reported that their organization had no control measures in place to counter unauthorized use of such devices. However, 65 percent of the IT managers used USB flash drives on a daily basis.

In July 2007, the Australian government will launch its National Filter Scheme, which will let Australian residents download free content-filtering software from five
vendors. Users will be able to download the software until June 2009. As part of the plan, vendors will be required to provide technical support until June 2010 and set up call centers to support the program’s launch. The government plans to cover the vendors’ support costs if their products reach an agreed-to level of adoption among downloaders.

**Privacy**

- Some employees using Google Calendar—JPMorgan Chase, for example—leaked sensitive corporate information such as the date and time of meetings and names of projects in the works. Google Calendar was released last year as part of the company’s continuing stretch into Web-based applications. Users can choose to keep their calendar entries private or public; the default setting is private. Additionally, Google says that the calendar application can be deployed through Google Apps, allowing IT administrators to define corporate user settings.

- South African security researcher Roelof Temmingh has created a new search tool—Evolution—that searches across Web sites, search engines, and social-networking sites to gather personal data. Typing in an individual’s email address, for example, could connect it to an IP address or home phone number by searching through a domain registration site or a social-networking site.

- While surfing a searchable database on a US Census Bureau Web site, a bored farmer in Illinois discovered the names and social security numbers (SSNs) of 63,000 people who had received federal financial aid. The information has since been removed, and an internal investigation is ongoing to determine whether other related agencies might have exposed the same personal information. The US Department of Agriculture, which oversees the aid program, is offering free credit monitoring to those affected.

- The WHOIS Taskforce recently submitted its final report on a proposal to let domain name registrants list third-party contact information instead of their own personal information. Some domain name owners use a proxy service that lets them list the proxy instead of their information. The proposal, known as Operational Point Of Contact (OPOC), is facing opposition from law enforcement, businesses, and intellectual-property lawyers. The Generic Names Supporting Organization (GNSO) Council is deliberating whether to recommend the proposal to the ICANN Board for a formal vote.

- In its House Appropriation Committee report, the US Government Accountability Office (GAO) says the Department of Homeland Security (DHS) has overlooked the need for a privacy impact assessment for its developing data mining program. The program—Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE)—uses software that sifts through information and identifies
patterns or relationships that might be potential threats. The GAO points out that privacy risks should be evaluated early in the development process to avoid costly retrofitting later to add privacy controls.

- A CD containing the personal data, including social security numbers, of 2.9 million Georgia residents was lost by a Dallas-based firm handling the state’s health care claims. According to the Georgia Department of Community, the CD was lost in transit. The company responsible for the loss, Affiliated Computer Services, has notified those affected by mail and is offering free credit monitoring. To date, no evidence of fraudulent activity has occurred.

### Policy

- In April, the European Court of Human Rights ruled in favor of a UK resident in her suit against the UK government for monitoring her Internet and telephone usage while at her public-sector job. The suit was brought under EU human rights legislation rather than UK law. The court ruled that an employee’s private use of company’s Internet and telecommunications might be protected if the company fails to inform employees that their communications will be monitored under a personal-use policy.

- In April, the European Court of Human Rights ruled in favor of a UK resident in her suit against the UK government for monitoring her Internet and telephone usage while at her public-sector job. The suit was brought under EU human rights legislation rather than UK law. The court ruled that an employee’s private use of company’s Internet and telecommunications might be protected if the company fails to inform employees that their communications will be monitored under a personal-use policy.

- In April, the US House of Representatives Committee on Government Oversight released its computer security report card and the Department of Homeland Security (DHS) managed to dig itself out of a failing grade for the first time with a D. Other agencies requiring more studious attention to the security requirements of the Federal Information Security Management Act of 2002 (FISMA) include NASA, with a D-minus, and the Departments of Education and Defense, both with Fs. However, some did make the honor roll, including the Department of Justice with an A-minus and the Department of Housing and Urban Development with an A-plus.

- The Internet Security Alliance (ISA), a consortium of IT vendors and customers, released a white paper in April that calls on the US government to abandon its regulatory approach to cybersecurity and adopt industry-outlined best practices. The group advocates incentives to encourage companies to invest in cybersecurity, including enticements to reduce implementation costs. Larry Clinton, the ISA’s president, says, “Government regulations can’t keep up with Internet threats, but the profit motive can.” Other suggested incentives include limited legal liability for companies following industry-approved best practices and creating new business opportunities for companies that follow the best practices.

- In May, Digg, the social news site, found itself in a pickle when it complied with cease-and-desist letters filed under the US Digital Millennium Copyright Act (DMCA) and removed posts containing the cracked encryption key that lets users circumvent digital rights management (DRM) on high-definition (HD) DVDs. In an effort to curtail piracy, the consortium that holds ownership rights to the key—the Advanced Access Content System (AACS)—began sending DMCA take-down letters to blogs and Web sites that published it. Digg users responded by overloading the site with posts containing the key, which spread to other blogs as well, eventually making appearances in Photoshopped images and on T-shirts. Digg gave in and stopped removing the posts.

- In May, Digg, the social news site, found itself in a pickle when it complied with cease-and-desist letters filed under the US Digital Millennium Copyright Act (DMCA) and removed posts containing the cracked encryption key that lets users circumvent digital rights management (DRM) on high-definition (HD) DVDs. In an effort to curtail piracy, the consortium that holds ownership rights to the key—the Advanced Access Content System (AACS)—began sending DMCA take-down letters to blogs and Web sites that published it. Digg users responded by overloading the site with posts containing the key, which spread to other blogs as well, eventually making appearances in Photoshopped images and on T-shirts. Digg gave in and stopped removing the posts.

- Network and Information Security Agency (ENISA), is conducting a feasibility study on how to efficiently collect and distribute security information to small- and medium-sized businesses (SMBs) in Europe. One current project under consideration is the European Information Sharing and Alert System (EISAS), which would alert businesses to security threats. ENISA is expected to release the results of its study in June.