THE MICROSOFT SECURITY CHRONICLES

CSS SECURITY WORLDWIDE PROGRAMS

May 12, 2011

INSIDE THIS ISSUE

MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

Microsoft Security Sites Worldwide

Hackers Stole Personal Data from PlayStation Network

MSNBC

In a post to the official PlayStation blog Tuesday afternoon, Sony of America's director of communications said that "an illegal intrusion" in their system has caused a "compromise of personal information." And while Sony officials don't believe credit card information was taken, they say that hackers may have taken names, addresses, email addresses, birthdates and passwords among other things.

Analysis:

Personal information of an estimated 70 million users of Sony's PlayStation Network was reported to have been stolen in a data breach incident that occurred between April 17 and April 19, 2011. Sony confirmed in a blog post on April 26, 2011 that user account information was compromised in an illegal and unauthorized intrusion into its network. Sony said it took the following steps in response to the intrusion:

1. *Temporarily turned off PlayStation Network*
2. *Engaged an outside, recognized security firm to investigate the intrusion*
3. *Took steps to enhance security and strengthen its network infrastructure*

On May 06, 2011, Sony acknowledged in a blog post that approximately 2,500 names and addresses of individuals who had entered a 2011 product sweepstakes had been posted online and it had taken steps to shut down the website.

SECURITY CALENDAR

May 2011

15 AusCERT2011 – Australia

16 YStS – Brazil

17 HITB Amsterdam

21 ICSE Honolulu

June 2011

12 FIRST - Vienna

14 Hack in Paris

16 SOURCE Seattle

18 ToorCon Seattle

27 ISACA

27 STM'11 - Copenhagen

In a letter (PDF) to the U.S. Congress, Sony listed the new security measures being implemented to prevent future data breaches. The PlayStation Network remained turned off since the day of the intrusion. It was reported but not confirmed that the services could be online by May 31, 2011.

Reports of data breach incidents continue to be in the news. On April 01, 2011, in a data breach considered to be the largest breach in U.S. history, email marketing company, Epsilon had announced that an incident was detected where a subset of Epsilon clients' customer data was exposed by an unauthorized entry into Epsilon's email system. On May 05, 2011, it was reported that hackers broke into the databases of online password management company, LastPass and stole information of an estimated 1.25 million accounts. LastPass confirmed that it had seen a network traffic anomaly and enforced change of users' master passwords.

An article on exfiltration or the illegal removal of data from a system, discussed how hackers extract data without being detected. Hackers may store data in temporary password-protected folders or files, which can often go unnoticed. Breaches by malware, such as keystroke loggers' data exfiltration, most often used FTP and email capabilities. A report (PDF) on 218 investigations in 24 countries, conducted in 2009 found that an average of 156 days lapse between initial data breach and its detection. Recent studies have indicated that source code or other intellectual capital (PDF) may be the top "cyber currency" that hackers look for in data breaches.

A benchmark study of 51 U.S. companies by Ponemon Institute – U.S. Cost of a Data Breach – found that data breaches in 2010 cost their companies an average of US$214 per compromised record.

According to a report, the U.S. Congress has been called upon to pass new data security regulations for businesses in response to these data breaches at Sony, Epsilon, and other companies.

Fake Antivirus for Mobile Platform Spotted

ZDNet

Security researchers from CA have spotted a bogus mobile antivirus scanner using the Kaspersky brand. Spreading through social engineering, and relying on hardcoded results, the rogueware attempts to trick users into thinking they're malware-infected.

Analysis:

Security and privacy are top concerns in the mobile platform space today. The McAfee Threats Report: Fourth Quarter 2010 (PDF) reported recently that threats to mobile platforms are growing. A report on a study by the Nelsen Company shows that the majority of mobile app users are wary about privacy and are cautious about sharing their locations via mobile phone.

On May 10, 2011, Juniper Networks released its Malicious Mobile Threats Report 2010/2011 (registration required) on the current mobile threat landscape. It found that malware developers are capable of researching, uncovering, and leveraging weaknesses in mobile platform security models, as well as inherent weaknesses in app stores and open ecosystems. As mobile device usage increases, the absence of installed mobile security products is playing an enabling role in the vulnerability of mobile devices and the exploitation of sensitive data and personal identifying information (PII).The report's key findings include the following:

1. *There has been a 400 percent increase in Android malware since summer 2010.*
2. *A SANS survey found that 85 percent of smartphone users were not using an antivirus solution on their mobile device to scan for malware. Of the 15 percent respondents who were using antivirus products on their smartphones, one in five reported having been infected with a malicious application.*
3. *Spyware capable of monitoring communication to and from a mobile device accounted for 61 percent of all reported Juniper Networks mobile customer infections.*
4. *17 percent of all reported infections were due to SMS trojans that sent SMS messages to premium rate numbers, often at irretrievable cost to the user or enterprise.*
5. *One in 20 mobile devices is lost or stolen, risking loss of confidential and sensitive data.*

The report's recommended security measures for mobile devices that can be implemented by enterprises, government agencies, and small and medium sized businesses (SMBs) include:

1. *On-device antimalware to protect against malicious applications, spyware, infected SD cards, and malware-based attacks to the device*
2. *On-device firewall to protect device interfaces*

3. *SSL VPN clients to protect data in transit, and to ensure secure and appropriate network access and authorization*
4. *Centralized remote locate, track, lock, wipe, backup, and restore facilities for lost and stolen devices*
5. *Centralized administration to enforce and report on security policies across the entire mobile device population*
6. *Support for all major mobile platforms and management capabilities to enforce security policies*
7. *Device monitor and control, such as the monitoring of messaging and control of installed applications*
8. *A solution that integrates with network-based technologies to ensure the security of mobile devices*
9. *Ability for an administrator to monitor device activity for data leakage and inappropriate use*

Federal CISOs remove the 'human element', Focus on Known Risk

Fierce Government IT

Cyber security is about assessing risk, not just vulnerabilities, and often federal agencies' biggest risks lie within the workforce, according to a [U.S.] National Security Agency official.

Analysis:

According to a report on the Government IT Leadership Forum held on May 05, 2011, cyber attacks at the U.S. State Department quadrupled between 2008 and 2010, reaching 8,000 last year. The department took a census of the attacks and assigned numeral values ranging from zero to 10 to each, creating a "risk market" or "monetizing risk" approach. The strategy was built on National Institute of Standards and Technology guidance and was enhanced with additional metrics. By concentrating on known vulnerabilities and containment, the pace of patching could be accelerated. Several State Department offices, located overseas, went from zero to 84 percent patch coverage in 7 days and to 93 percent in 30 days.

In another report on cyber security, an audit (PDF) that reviewed the U.S. Federal Bureau of Investigation's (FBI) ability to address the national security cyber intrusion threat was published. A computer intrusion is defined as the actual or attempted unauthorized access of a protected computer, which *includes any computer connected to the Internet or any computer connected to a network that is connected to the Internet. A national security intrusion is one conducted by foreign powers for intelligence or terrorist purposes. The audit found that:*

1. *36 percent of the FBI field agents interviewed reported that they lacked the networking and counterintelligence expertise to investigate national security intrusion cases.*
2. *The FBI's rotation policy, which rotates agents among different offices, hindered the ability to investigate these intrusions.*
3. *The forensic and analytical capability in field offices was inadequate to support national security intrusion investigations.*
4. *Interagency access to and sharing of information about cyber threats had many ongoing challenges.*

It was later reported that the FBI disputed some of the findings of the audit.

Facebook Applications Accidentally Leaking Access to Third Parties

Symantec

Third parties, in particular advertisers, have accidentally had access to Facebook users' accounts including profiles, photographs, chat, and also had the ability to post messages and mine personal information.

Analysis:

According to a Symantec report on May 10, 2011, Facebook IFRAME applications inadvertently leaked access tokens to third parties like advertisers or analytic platforms. Access tokens are like "spare keys" granted by Facebook that applications can use to perform certain actions on behalf of the user or to access the user's profile. Each token is associated with a select set of permissions. Symantec estimated that as of April 2011, close to 100,000 applications were enabling this leakage. These third-parties may not have realized their ability to access this information. Symantec reported this issue to Facebook and corrective action was taken.

The need for raising user awareness on security and privacy in social networking continues to rise. On May 04, 2011, it was reported that a study from the U.S. National Cyber Security Alliance (NCSA), sponsored by Microsoft, *found that U.S. schools are ill-prepared to teach students the basics of online safety, security, and ethics.*

Cyber ethical issues include promoting academic integrity, combating and detecting plagiarism, rules for respecting copyright and downloading, etc. Cyber safety issues include safer and best practices for social networking sites, dealing with inappropriate content, etc. Cyber security issues include phishing, hacking, malware, identity theft, etc. The study (PDF) found that:

1. *51 percent of teachers agreed that their school did an adequate job of preparing students regarding cyber ethics, online safety, and computer security issues.*
2. *Roughly 30 percent of teachers agreed that their school required cyber ethics, cyber safety, and cyber security curriculum be taught in the classroom setting.*
3. *57 percent of teachers said they felt they were prepared to talk about cyber bullying.*
4. *One-third of the teachers reported teaching about the risks tied to social networking sites and about making decisions on sharing personal information on the Internet.*
5. *36 percent of teachers spent zero hours and 40 percent spent 1-3 hours in training provided by the school on cyber ethics, cyber safety, and cyber security. 44 percent teachers spent zero hours and 32 percent spent 1-3 hours on training in these areas in their own time.*

Microsoft recently published a paper - Personal Safety in the Cloud (PDF) - that examines online safety issues and identifies a number of ways that policymakers can help protect individuals online , including enacting stronger laws against cyber crime and child exploitation, supporting industry self-regulatory principles, promoting Internet safety education in schools, and funding research on online risks.

The material in the Microsoft Security Chronicles is provided for informational purposes only. References to third party products, services or websites are provided only as a convenience to you and should not be considered an endorsement by Microsoft. Microsoft makes no warranties, express or implied, as to any third party products, services or websites. The views expressed in the linked articles are strictly those of the individual authors and/or publications.