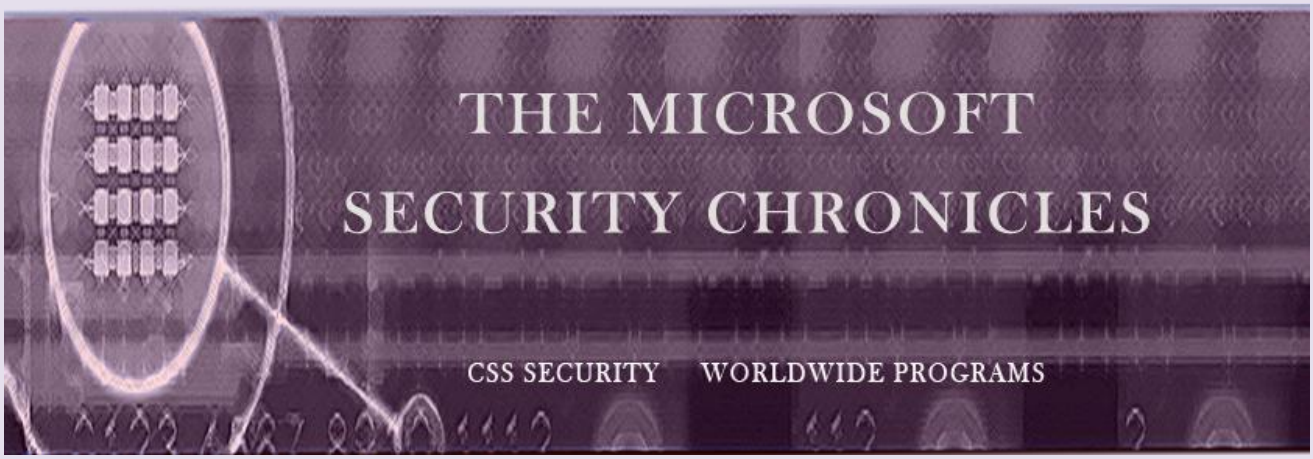

March 03, 2011

INSIDE THIS ISSUE

MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

Microsoft Security Sites Worldwide

Cybercrime: Why It's the New Growth Industry

Tech Republic

PCWorld reported earlier this month that in a struggling economy, one industry that has shown double-digit growth year after year is, like many other high growth industries, an illicit one — in this case, cyber crime.

Consequently, the cost of cyber crime — to individuals, corporations, governments, and society in general — continues to climb.

Analysis:

As noted in this article, cyber crime has been growing steadily over the last few years. According to the 2010 Internet Crime Report (PDF) released by the Internet Crime Complaint Center (IC3), online crime has become pervasive, affecting people in all demographic regions.

In 2010, the IC3 received 303,809 complaints, the second-highest since its inception, averaging 25,317 per month. IC3 also found that:

1. *The most reported offense was the non-delivery of payment or merchandise (14.4 percent), followed by FBI-related scams where a criminal poses as the FBI to defraud victims (13.2 percent), and identity theft (9.8 percent).*
2. *The highest number of complaints originated from California (13.7 percent), Florida (7.9 percent), and Texas (7.3 percent).*
3. *The top countries/regions that perpetrators resided in were United States (65.9 percent), United Kingdom (10.4 percent), and Nigeria (5.8 percent).*

SECURITY CALENDAR

March 2011

03 Microsoft Bulletin Advance Notification

07 Cloud Connect – Silicon Valley

08 Microsoft Security Bulletin Release

09 CanSecWest - Vancouver

15 Black Hat Europe - Barcelona

28 Troopers - Germany

April 2011

05 BlueHat Security Forum Brazil 2011

07 Hackito Ergo Sum 2011 - Paris

07 Microsoft Bulletin Advance Notification

12 Microsoft Security Bulletin Release

As incidents of cyber crime grow, its cost continues to climb too. The UK government recently released The Cost of Cyber Crime Report (PDF) - its first official estimate of the cost of cyber crime in the UK. It reports that:

1. *The overall cost to the UK economy from cyber crime is GBP 27 billion per year. The major part of this cost (GBP 21 billion) is borne by the business. The citizens incur GBP 3.1 billion and the government incurs GBP 2.2 billion.*
2. *Cyber crimes that cost citizens the most are identity theft (GBP 1.7 billion), online scams (GBP 1.4 billion), and scareware and fake antivirus software (GBP 30 million).*
3. *Businesses incur costs from IP theft (GBP 9.2 billion), industrial espionage (GBP 7.6 billion), extortion (GBP 2.2 billion), online theft (GBP 1.3 billion), and loss or theft of customer data (GBP 1 billion).*
4. *IP theft has the greatest economic impact, particularly on companies that create significant quantities of IP or those whose IP is relatively easy to exploit. The types of IP most likely to be stolen include copyright, ideas, designs, methodologies, and trade secrets.*

The report recommends that selected companies from within the most affected business sectors may be approached in confidence to help the government build a more accurate assessment of IP theft and espionage.

Henry Ford Tightens Security After Patient Data Lost

The Detroit News

The Henry Ford Health System is implementing more stringent security measures — warning employees they could be fired for lapses around patient data — after a security breach involving some 2,777 patients was discovered earlier this month.

Analysis:

A news article on a recent survey of U.S. patients indicated that while patients trust their physicians to keep their healthcare information private, they don't extend that same trust to computerized records systems. The survey found that:

1. *35 percent survey respondents are worried that their health information will end up widely available on the Internet.*

2. *50 percent of the respondents believe that electronic health records (EHRs) will have a negative impact on the privacy of their health data.*

A recent report (PDF) by Deloitte Center for Health Solutions on privacy and security in health care estimates that the total economic impact of data breaches on U.S. hospitals is $6 billion annually and approximately one-third data breaches result in medical identity theft.

The health care industry is particularly susceptible to data fraud and medical identity theft due to the nature and content of the data (social security numbers, insurance identification numbers, payment information, and medical provider identification numbers) involved.

The root causes of low preparedness for privacy and increased risk of data breaches and medical identity theft include:

1. *Lack of internal resources (human and capital)*
2. *Lack of internal control over patient information*
3. *Lack of upper management support*
4. *Outdated policies and procedures or non-adherence to existing ones*
5. *Inadequate personnel training*

The report suggests a basic approach to assessing a health care organization's current preparedness:

1. *Risk Management: Identify and assess data security risks to develop appropriate security controls to mitigate or avoid risk. This allows health care organizations to make informed decisions on how to allocate security resources to improve data protection.*
2. *Security and Privacy Program: Develop and implement policies, procedures, and training needed to mitigate or avoid risk. This creates baseline standards for the secure handling of sensitive patient information and creates organization-wide awareness of data privacy and security policies.*
3. *Compliance: Validate effective risk management and governance by developing and implementing policies to address identified risks, monitoring and logging data handling procedures, and compliance with established processes, etc. This reduces organizational risk, creates customer trust and confidence in an organization's protection of Personal Health Information (PHI), and reduces potential for financial penalties due to reasonable cause or willful neglect.*

As the potential for data breaches increases, stakeholders must act to prevent compromising sensitive patient data, preserve brand value, and avoid substantial financial penalties for violation.

Web Users Need More Cookie Control, Says EU Info Security Advisor

Out-Law

The European Network and Information Security Agency (ENISA) has published a report outlining how advertisers are using increasingly sophisticated varieties of cookie[s] to identify web users. The technology could breach EU laws on privacy, it said.

"In most cases users cannot easily manage cookies," said ENISA's report [PDF]. "This is particularly true for new type[s] of cookies that are not controlled by browsers and require additional management tools."

Analysis:

Microsoft released Internet Explorer 9 in February with a new privacy feature, Tracking Protection, to help consumers be in control of potential online tracking as they move around the web. Microsoft's Corporate Vice President Dean Hachamovitch, head of Internet Explorer development, and Chief Privacy Strategist Peter Cullen, explained that with Tracking Protection, consumers can filter content in a page that may have an impact on privacy and have Tracking Protection Lists to indicate what websites they would prefer to not exchange information with. Tracking Protection complements the strong set of privacy features already in IE8, like InPrivate Browsing which helps users control what their machine remembers about their browsing.

The World Wide Web Consortium (W3C) recently announced that they have formally received Microsoft's proposal on a common W3C standard for Web Tracking Protection. The submission proposes to address information gathering by third parties on the web through two different mechanisms: A filter that blocks download of third-party content and a global "Do Not Track User Preference."

The need for more user privacy for web browsing is being recognized globally. The European Network and Information Security Agency (ENISA) reported in a recent paper (PDF), that almost 80 percent of online service providers are

collecting data from cookies. Besides attributes (name, domain, expiration date, etc.), the following types of data can be stored in cookies:

1. *Credentials, such as user names and passwords and other identifiers*
2. *Preferences and interface customizations/personalization*
3. *Session data and data from the site i.e. cached data*
4. *Tracking information about users*

Due to the continuous evolution of cookies to address the needs of industries (i.e. advertising companies), they raise both security and privacy concerns. The information stored in a cookie by a website is usually coded in plain text and can be modified each time the user visits the webpage. As a result, cookies can easily be retrieved (snooped) and forged.

They can also be used by websites to track users across visits. Knowledge of the pages visited by a user allows an advertising company to target advertising at the user's presumed preferences. A study showed that not only are advertisers increasing their tracking of users, but that they can now link these traces with identities and personal information available via online social networks.

ENISA's privacy recommendations include:

1. *Greater scrutiny: As more persistent, transparent, and powerful cookies are developed that support user identification in a persistent manner, these privacy-invasive marketing practices need greater scrutiny.*
2. *More user control: The provisions for informed consent should guide the design of systems using cookies. Users must be able to find out how a website plans to use the information from the cookie and should be able to choose whether or not those policies are acceptable.*
3. *Easier management: All cookies should have removal mechanisms that are easily used by any user. The storage of these cookies outside browser control should be limited or prohibited.*

Botnets Increased Rampantly During 2010, Worse to Come – Damballa Report

ITWire

Damballa keeps track of the attacks on their clients' systems, and have just released a report indicating that 2010 saw a 650 percent increase in botnet attacks, and that six of the 2010 top 10 botnets did not exist in 2009.

Analysis:

Damballa published a report (PDF) on the performance and prevalence of botnets it most commonly encountered in the course of monitoring Internet-based threats in a user-base comprised mostly of home users and small businesses. The report found that:

1. *Six of the top 10 botnets of 2010 did not exist in 2009 and only one was among 2009's top 10 botnets. Many operators built their botnets based on popular construction kits - often changing and augmenting the kits throughout the year as their infection campaigns and fraud objectives changed.*
2. *The top 10 largest botnets in 2010 accounted for approximately 47 percent of all botnet compromised victims.*
3. *TDLBotnetA (RudeWarlockMob), a botnet associated with the TDL Gang, infected the highest percentage (14.8 percent) of all unique infected victims in 2010.*
4. *At its peak near the end of 2010, the total unique botnet victim population was 654 percent greater than the victim population at the beginning of 2010.*

The report predicts that with malware that can be repurposed, botnets that can be rented, and new and attractive targets in the proliferation of smart phones and mobile devices, 2011 will also be a challenging year.

Also see: Microsoft's latest Security Intelligence Report V9 also provides an in-depth featured intelligence report on battling botnets.