# THE MICROSOFT SECURITY CHRONICLES

CSS SECURITY WORLDWIDE PROGRAMS

March 31, 2011

## INSIDE THIS ISSUE

## MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

Microsoft Security Sites Worldwide

## Junk Mail Down 1/3 Since Rustock Botnet Takedown

*The Register*

Global spam volumes dropped by a third following the takedown of the infamous Rustock botnet earlier this month, according to MessageLabs.

Prior to the dismantling of its command and control servers on a takedown operation led by Microsoft, Rustock accounted for 13.82 billion spam emails daily, the majority of which advertised unlicensed pharmaceutical websites..

Analysis:

*According to Symantec's blog post, spam sent via the Rustock botnet virtually disappeared on March 16, 2011. It was reported later that Microsoft and federal law enforcement agents seized computer equipment from Internet hosting facilities across the U.S. in a sweeping legal attack (Operation b107) designed to cripple Rustock, the leading source of junk email on the Internet. Microsoft launched the raids as part of a lawsuit (PDF) filed in federal court in Seattle against Rustock's unnamed operators.*

*Microsoft's Digital Crime Unit (DCU) reported that Rustock has been among the world's largest spambots, at times capable of sending 30 billion spam emails per day. A single Rustock-infected computer could send 7,500 spam emails in just 45 minutes – a rate of 240,000 spam mails per day. There may be close to 1 million computers infected with Rustock malware.*

*In February 2010, Microsoft had taken down the Waledac botnet in a similar legal operation (Operation b49). It was reported that the primary tool in dismantling Waledac was the seizure of some 277 domain names that Waledac clients used to locate control servers. However, Microsoft did not*

## SECURITY CALENDAR

**April 2011**

05 BlueHat Security Forum Brazil 2011

07 Hackito Ergo Sum 2011 - Paris

07 Microsoft Bulletin Advance Notification

11 ISO Spring 2011 - Singapore

12 Microsoft Security Bulletin Release

16 Infiltrate 2011 - Miami

20 SOURCE Conference Boston 2011

22 Thotcon – Chicago

28 SyScan 2011 - Singapore

**May 2011**

05 Microsoft Bulletin Advance Notification

10 Microsoft Security Bulletin Release

15 AusCERT2011 – Australia

16 YStS – Brazil

24 HITB Amsterdam

*have the ability to seize control servers and analyze their contents. With Rustock, Microsoft's legal approach included allegations of trademark infringement and the Lanham (Trademark) Act includes specific provisions to seize infringing material.*

*Rustock's takedown had a significant impact on global spam volumes. Symantec reported in its March 2011 Intelligence Report (PDF) that global spam had dropped by one-third after Rustock was dismantled. In March 2011, prior to its takedown, Rustock had been sending approximately 13.82 billion spam emails daily, accounting for an average of 28.5 percent of global spam sent from all botnets in March.*

*Microsoft is continuing its work with both CERTs and ISPs around the world to reach out to those whose computers are infected and help clean them of viruses. Support information for cleaning infected computers is available at http://support.microsoft.com/botnets. Microsoft also provides an intelligence report on botnets in the latest edition of its Security Intelligence Report V9.*

## White House Backs Online 'Privacy Bill of Rights'

*Google News*

The [U.S.] White House urged Congress on Wednesday [March 16, 2011] to approve a "consumer privacy bill of rights" to govern the collection and use of personal data on the Internet.

Assistant Commerce Secretary Lawrence Strickling called for the legislation at a hearing on online privacy held by the Senate Committee on Commerce, Science and Transportation.

*Analysis*:

*The cover story on the March 21, 2011, edition of Time magazine reported that companies mine a significant amount of personal and behavioral data about consumers and sell it to advertisers. A Wall Street Journal investigation last year also reported that one of the fastest-growing businesses on the Internet is the business of spying on consumers.*

*The FTC has called for the development of a "Do Not Track" system that would enable people to avoid having their actions monitored online. On March 16, 2011, the U.S. government supported the creation of a "privacy bill of rights" to help regulate the commercial collection of consumer data online. The* *government's report emphasized that consumers should have stronger privacy protections and the companies that run the Internet economy should have clearer rules to guide their uses of data about consumers. It proposed that:*

1. *There should be a "consumer privacy bill of rights" with legislation to baseline consumer data privacy protections.*
2. *The FTC should have the authority to enforce any baseline protections.*
3. *A framework that provides incentives for the development of codes of conduct as well as continued innovation around privacy protections should be created.*

*The European Union (EU) is also moving forward with online privacy legislation. On March 17, 2011, the EU confirmed that it will seek a law on the "right to be forgotten" ensuring that consumers' data is erased if they so wish. Proposals will be unveiled soon to force Facebook and other social networks to make stringent data privacy settings the default position for users and to give them control over their own information. It was reported that the U.S. and EU are converging in their web privacy positions, although differences remain in their approach.*

*Note: Microsoft released Internet Explorer 9 in February 2011 with a new privacy feature, Tracking Protection, to help consumers be in control of potential online tracking as they move around the web.*

## RSAs Secure IDs Hacked; What to Do

*Gadgetwise*

RSA Security, a division of EMC Corporation, said on Thursday that it suffered a sophisticated hacker attack that resulted in the theft of sensitive information related to its popular SecurID two-factor authentication products.

Analysis:

*There have been several reports of enterprise hacking incidents in the past few weeks. Some of the key ones include:*

1. *Hackers broke into the MySQL.com and Sun.com websites using a SQL injection technique.*
2. *The European Commission and the European Parliament were hacked in separate incidents.*

3. *The RSA suffered a sophisticated data breach, potentially compromising computer security products widely used by corporations and governments.*
4. *Comodo suffered an attack in which a hacker fraudulently obtained digital certificates for some major websites that could have been used to impersonate those sites. Microsoft issued an advisory on this issue.*
5. *Bank of America accounts were hacked in a major security breach this week.*
6. *Hackers repeatedly penetrated the computer network of the company that runs the Nasdaq Stock Market during the past year.*
7. *McAfee had reported (PDF) in February 2011 that hackers had waged attacks, dubbed Night Dragon, against global oil, gas, and petrochemical companies.*
8. *Security researchers discovered 45 vulnerabilities in the software used to control facilities such as nuclear plants and oil refineries this week.*

*The number of hacking attacks and the seriousness of the possible consequences continue to rise. A new report (PDF) from McAfee found that the latest "cyber crime currency" is intellectual capital and sensitive corporate data such as trade secrets and marketing plans. It found that:*

1. *The value of intangibles is estimated at around 81 percent of S&P 500 companies' value – a significant portion of which is represented by patented technology, trade secrets, proprietary data, business processes, and go-to-market plans.*
2. *More than 25 percent of organizations assess the threats or risks posed to their data twice a year or less often.*
3. *Almost 50 percent of respondents surveyed in the report said that they would take particular data off the network in order to protect it from being leaked.*
4. *62 percent of respondents identified securing mobile devices as a challenge.*
5. *The admission of a significant vulnerability could flag other attackers so very few companies are willing to be public about intellectual capital losses.*
6. *One in seven organizations has not reported data breaches and/or losses to outside government agencies or authorities, or stockholders. Only three in ten organizations report all data breaches/losses suffered, while one in ten organizations will only report breaches/losses that they are legally obliged to, and no more.*

7. *Only 25 percent of organizations conduct forensic analysis of a breach or loss, and only 50 percent take steps to remediate and protect systems for the future after a breach or attempted breach.*
8. *More than 50 percent of organizations have, at some point in their history, decided not to further pursue or investigate a security incident because of the cost of such an investigation/pursuit.*
9. *The most significant threat reported by organizations when protecting their sensitive information was data leaked accidentally or intentionally by employees.*

*According to McAfee's report, some emerging trends that are changing the ways companies are defying sophisticated attacks and insider leaks include:*

1. *Deep Packet Inspection (DPI): A DPI solution acts as a highly flexible complement to existing security architecture, performing inline, full packet analysis in near real-time of all packets.*
2. *Human Behavior Based Network Security: These solutions are a step ahead of the hackers or insiders as they detect intent through the activities taken on the network.*
3. *Insider Threat Tools: Tool suites can be deployed on systems to monitor hundreds to thousands of inside users simultaneously, tracking their actions and identifying traits inherent in those actions that should be cause for alert.*
4. *Advanced Forensics: Every digital device is traceable through a trail of "digital DNA" uncovered through sophisticated computer and network analysis.*
5. *Advanced Malware Analysis: It is now possible to discover zero-day malware that will use or is using network exploits to attack a network.*

## Rise in Federal Cyberattacks Partly Due to Better Monitoring

*SC Magazine*

The number of cyber incidents affecting U.S. federal agencies shot up 39 percent in 2010, according to a new report [PDF] from the Office of Management and Budget (OMB), but experts said the increase is partly a reflection of improved discovery capabilities within government.

Analysis:

*The U.S. federal government's responsibility of maintaining the safety, security, and resilience of its IT infrastructure is codified in the Federal Information Security Management Act of 2002 (FISMA). In its Fiscal Year 2010 FISMA Report to Congress (PDF), the federal government reported the following trends:*

1. *In FY2010, federal cyber security incidents increased by almost 39 percent from FY2009.*
2. *Malicious code through multiple means (e.g. phishing, virus, logic bomb) continues to be the most widely used attack approach (30.8 percent).*
3. *There were repeated attacks on zero-day vulnerabilities through social engineering. Exploit codes for these vulnerabilities often became publicly available, which placed federal agencies, private organizations, and individuals at increased risk. (Note: Microsoft supports coordinated vulnerability disclosure as a shared responsibility in the security community.)*
4. *66 percent of IT assets at agencies are being managed with an automated asset management capability and 51 percent are being managed with an automated vulnerability management capability.*
5. *54 percent of government-wide portable computing devices are encrypted with FIPS 140-2 (PDF) encryption.*
6. *On average, it takes agencies almost 9 hours to determine whether anomalous behavior is an actual incident. The time between detection and reporting is on average 20 hours.*
7. *Specialized cyber security training for agency users with significant security responsibilities averages 88 percent across all federal agencies. 73 percent of new users were given security awareness training prior to being granted network access.*
8. *In FY2010, 15.6 percent of agencies' IT spending was spent on IT security. The main categories of security spending were personnel (74.4 percent), security tools (8 percent), NIST 800-37 implementation (7 percent), security testing (7 percent), and security training (3 percent).*

*The federal government will continue focusing on having information security as a key enabler in harnessing technological innovation in FY 2011.*

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.