



June 16, 2011

INSIDE THIS ISSUE

[Citigroup Breach Exposed Data on 210,000 Customers](#)

[Can RSA Repair the Broken Trust?](#)

[Microsoft Prepares to Out Rustock Operators](#)

[Cyber Security Agency ENISA Maps Good Practice in Europe](#)

MICROSOFT RESOURCES

[Microsoft Security Home](#)

[Microsoft Trustworthy Computing](#)

[Microsoft Security Sites Worldwide](#)

[Citigroup Breach Exposed Data on 210,000 Customers](#)

CIO

Citigroup admitted on Wednesday [June 08, 2011] that an attack on its website allowed hackers to view customers' names, account numbers, and contact information such as email addresses for about 210,000 of its cardholders.

Analysis:

The list of organizations suffering hacking intrusions continues to grow. On June 09, 2011, it was [reported](#) that account information of approximately 210,000 Citi North America customers was stolen. The breach was discovered in May during routine systems maintenance.

More attacks on Sony's website were also [reported](#). A hacking group called LulzSec claimed that it had breached the Sony Pictures website via a SQL injection attack and compromised more than 1 million users' personal information. Attacks on Nintendo's servers in the U.S. were also [reported](#). The company said consumers' information was not compromised in the attacks.

The website of InfraGuard, a U.S. private sector affiliate of the Federal Bureau of Investigation, was also [compromised](#) and nearly 180 passwords were stolen and posted online. The International Monetary Fund (IMF) was [reportedly](#) hit by a large and sophisticated cyber attack as well. The concern about the attack was so significant that the World Bank, an international agency focused on economic development, whose headquarters is across the street from the

SECURITY CALENDAR

June 2011

- 18 [ToorCon Seattle](#)
- 27 [ISACA](#)
- 27 [STM'11 - Copenhagen](#)

July 2011

- 06 [EWNI 2011 - Amsterdam](#)
- 07 [Microsoft Bulletin Advance Notification](#)
- 08 [REcon - Montreal](#)
- 12 [Microsoft Security Bulletin Release](#)
- 19 [Privacy Security Trust - Montreal](#)
- 21 [SyScan 2011 – China](#)
- 30 [Black Hat USA – Las Vegas](#)

IMF in downtown Washington D.C., cut the computer link that allows the two institutions to share information. The incident is under investigation.

In another major hacking [incident](#), hundreds of personal Gmail accounts, including those of some senior U.S. government officials, were hacked in a massive phishing scheme. Google [said](#) on June 01, 2011, that the attacks originated from Jinan, China. The goal of this effort seems to have been to monitor the contents of these users' emails, with the perpetrators apparently using stolen passwords to change peoples' forwarding and delegation settings.

Companies targeted in hacking attacks often explain that sensitive customer information such as social security numbers was not stolen in the attacks. However, the information that was exposed could be used in phishing attacks. The black market for selling confidential data is also expanding. As noted in this Panda Security [report](#) (PDF), cyber crime organizations have an established process for selling sensitive data. Credit card details, for example, typically sell from US\$2 to US\$90. These types of markets operate in line with the normal laws of supply and demand. Any customer information that is compromised in an attack can be sold and exploited for profit.

[Can RSA Repair the Broken Trust?](#)

Help Net Security

Despite Art Coviello's [open letter](#) offering to replace tokens for customers, we are still none the wiser as to what assets within RSA were compromised during the breach they suffered in March.

Until RSA is more forthcoming with facts as to what was compromised, when it was compromised and the impact that can have on its customers, we will be subjected to ongoing speculation as to the exact impact of the breach, which will result in a continuing erosion of confidence in its products. And a replacement token does not make up for broken trust.

Analysis:

RSA suffered a sophisticated [data breach](#) in March 2011, resulting in information about RSA's SecurID authentication tokens used by millions of people, including government and bank employees, being stolen. The company acknowledged the breach in a [letter](#) to its customers.

In April, RSA provided a [blog post](#) explaining how the hacking attack had worked. The company's investigation revealed that the attack was in the category of Advanced Persistent Threat (APT). The attacker sent two different phishing emails over a two-day period to two small groups of employees. The email attachment was an Excel file containing a zero-day exploit that installs a backdoor through an [Adobe Flash vulnerability](#). The attacker then installed a remote administration tool that allowed control of the machine and access to other servers. With this access, the attacker stole confidential data.

There were concerns that SecurIDs stolen in this breach could be used to compromise other organizations that used SecurIDs. On May 31, 2011, a major online attack was [reported](#) on the networks of Lockheed Martin, the largest defense contractor in the U.S. Hackers reportedly exploited Lockheed's VPN access system, which allows employees to log on remotely by using their RSA SecurID hardware tokens. Attackers apparently possessed the factory-encoded random keys used by at least some of Lockheed's SecurID hardware, as well as serial numbers and the underlying algorithm used to secure the devices. Lockheed Martin was able to detect the intrusion and take swift steps to prevent any data loss.

RSA acknowledged that the attack on Lockheed Martin used information taken from RSA in March 2011. RSA offered to replace SecurID tokens for customers and implement risk-based authentication strategies to assure customers' confidence.

These events highlight the seriousness and widespread impact that a data breach incident can have on organizations.

[Microsoft Prepares to Out Rustock Operators](#)

CIO

Microsoft plans to take its next step against the operators of the Rustock botnet in coming weeks, revealing information about cyber criminals' identities.

Analysis:

In March 2011, Microsoft took legal action to take down the [Rustock](#) botnet and earlier, in February 2010, it had taken legal action to bring down the [Waledac](#) botnet. In another legal action in April 2011, the U.S. Department of Justice (DOJ) and the U.S. Federal Bureau of Investigation (FBI) [announced](#) that

they had undertaken a legal and technical operation to take down the [Coreflood](#) botnet.

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 13.8 billion spam emails daily, accounting for an average of 28.5 percent of global spam sent from all botnets in March.

On June 06, 2011, Microsoft [reported](#) that Rustock had remained dead since its takedown. The [Microsoft Digital Crimes Unit](#) continued to follow this case. Based on evidence gathered in the case (which can be found at <http://www.noticeofpleadings.com>, which was set up by Microsoft specifically for this case, there is reason to believe that the people behind the Rustock botnet either have operated or are operating out of Russia. Consequently, Microsoft has placed advertisements in two mainstream Russian newspapers to honor its legal obligation to make a good-faith effort to contact the owners of the IP address and domain names that were shut down when Rustock was taken offline. If the owners do not respond, Microsoft will continue to pursue this case, including possibly within the Russian judicial system, if necessary. Microsoft remains firmly committed to taking action against not just the perpetrators of this botnet, but to disrupt digital crime globally to make the Internet safer for everyone.

Microsoft has a [dedicated website](#) to provide free information and tools to help people get rid of botnet malware. Microsoft also provided intelligence analysis on [botnets](#) in the latest edition of its [Security Intelligence Report](#).

[Cyber Security Agency ENISA Maps Good Practice in Europe](#)

PR Newswire

The European Union Agency, ENISA (European Network and Information Security Agency), has today launched online an updated edition of its "[Country Reports](#)" on network and information security (NIS) in the member states and other European countries.

Analysis:

With the number of incidents of data breaches on the rise, a bill — The Personal Data Privacy and Security Act — was [introduced](#) in the U.S. Senate on June 07, 2011. The bill proposes establishing a national standard for data breach notifications and would make concealing data breaches a crime. A similar [proposal](#) was also released by the U.S. government in May 2011. Its [fact sheet](#) included proposals for standardizing national data-breach reporting and penalties for computer criminals.

It was [reported](#) on June 10, 2011, that the European Union (EU) countries had agreed on tougher sanctions against people conducting cyber attacks. Under the new rules, which have to be agreed to by the European Parliament, hackers would face a sentence of at least five years if found guilty of causing serious damage to IT systems. Tougher penalties would also affect perpetrators of attacks through botnets — networks of infected computers programed to send spam emails — and target identity theft. Illegally intercepting data would become a criminal offence in the EU.

ENISA's [report](#) (PDF) finds that:

- 1. European countries are highly varied in how prepared they are for dealing with cyber crime, network attacks, and network resilience.*
- 2. More countries are establishing centralized cyber security authorities (in the United Kingdom, France, The Netherlands, etc.). In other countries, the need for such centralized bodies is often recognized by private or public sector stakeholders, even though it has not yet led to concrete implementation.*
- 3. Increasing presence of national and governmental CERTs. In most of the countries that were the subject of this study, information security incidents are reported and handled via the national/governmental CERTs.*
- 4. The level of information reported and of support given by the CERT varies depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and CERT resources available. Special attention is generally given to issues affecting critical infrastructure.*
- 5. Best practice information on the resilience of eCommunications networks is usually collected by different authorities, while there is no central repository in place.*
- 6. The Data Protection Directive has been implemented by the countries and at least one competent national regulatory authority on this matter is in place and responsible for the enforcement of the locally-implemented Data Protection Act.*

7. *An increasing awareness toward spam and/or malware was noted in the study.*

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.

©2011 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Privacy Statement](#) | [Microsoft Trademark List](#)