Theft of Personal Data Could Affect 40 Percent of South Korea's Population

Officials have arrested a man for the alleged theft of credit card data for up to 20 million people in South Korea, about 40 percent of the country's population of 50.2 million. This was the largest personal privacy breach in the nation's history.

The suspect reportedly worked for the Korea Credit Bureau, which several South Korean credit card companies hired to help them better protect client data by creating forgery-proof cards.

Between May 2012 and December 2013, he allegedly stole personal information from 104 million credit cards—many South Koreans have multiple cards—that the KB Financial Group, the NongHyup Financial Group, and Lotte Card issued.

The stolen data included credit card numbers, as well as account holders' names, phone numbers, South Korean social security numbers, home and email addresses, and salaries, according to the country's Financial Supervisory Service.

Among the victims were South Korean President Park Guen-hye and United Nations Secretary-General Ban Ki-moon.

Regulators have said the stolen data wasn't encrypted.

Officials subsequently accused two marketing company managers of buying stolen data from the alleged thief.

However, investigators say, nothing indicates the data was distributed more widely or used for malicious purposes.

Nonetheless, many South Koreans have expressed fear this will eventually happen. About 2.28 million requested that the three affected businesses cancel their accounts, and 3.84 million demanded new cards. Some customers filed lawsuits against the companies.

The businesses say they will compensate people who lose money because of the theft, and several top executives have offered to resign.

South Korean regulators ordered the companies to not add new cardholders and to not market insurance policies or travel products for three months. Services to existing clients will continue.

Microsoft Chooses New CEO

Microsoft's Board of Directors has chosen longtime employee Satya Nadella to be the third CEO in the company's 39-year history. He replaces Steve Ballmer, who announced last August that he would step down as chief executive, a post he held since 2000.

The company also announced that founder and former chief executive Bill Gates will no longer serve as board chair but instead will act as Nadella's technology adviser.

John Thompson—former CEO of security vendor Symantec and current chief executive of infrastructure performance–management vendor Virtual Instruments—will be the new board chair.

Nadella, 46, was executive vice president of Microsoft's Cloud and Enterprise Group, one of the company's fastest growing divisions. In addition, he played an important role in Microsoft's successful cloud strategy and helped make its software development process quicker and more flexible.

One of his key challenges will be helping Microsoft adapt to a world in which mobile technology is growing rapidly in popularity and the PC—once key to the company's business—is less important.

Some industry observers predicted that Microsoft would look outside the company for its new chief executive, to shake things up. The company has faced a variety of problems in the past few years.

For example, its market value has plummeted and its consumer business is struggling. Also, the company hasn't developed a successful mobile strategy, and its Windows 8 operating system was widely criticized.

Because of these issues, some investment and market analysts expressed disappointment that Microsoft hired its new CEO from inside the company.

Nadella, who holds an MBA and an MS in computer science, has worked for Microsoft for 22 years.

Hackers Conduct First Internet of Things Attack

Smart TVs, wireless speakers, set-top boxes, home networking routers, multimedia centers, and a refrigerator were among the everyday objects used in the first reported cyberattack involving the Internet of Things, according to security firm Proofpoint.

This incident is important because manufacturers are increasingly enabling their everyday products to go online and thereby become part of the Internet of Things.

In the recent attack, hack-

Published by the IEEE Computer Society
0018-9162/14/$31.00 © 2014 IEEE

ers penetrated home networks and accessed 100,000 connected devices, according to Proofpoint, which declined to name the brands of appliances that were compromised.

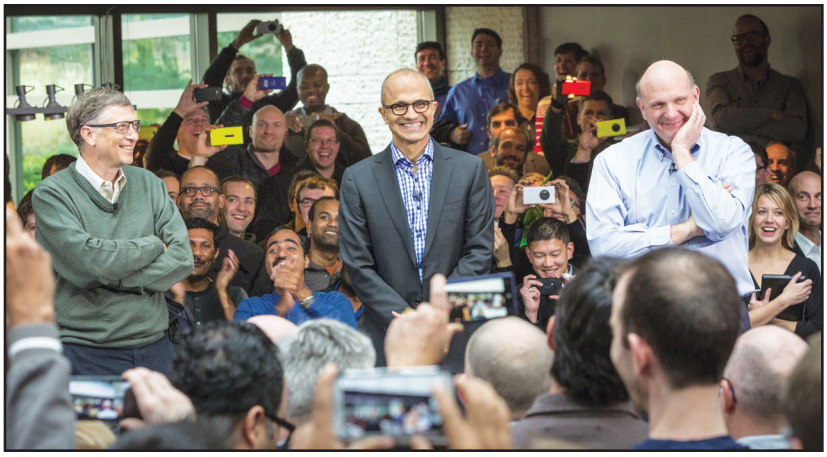
The security vendor says the hackers sent malware to the devices and turned them into a botnet of email clients that sent 750,000 phishing and spam messages to companies and individuals between 23 December 2013 and 6 January 2014. They sent bursts of malicious email, often 100,000 messages at a time. However, they initiated no more than 10 messages from a single IP address, making it difficult to blunt the onslaught by shutting down individual computers.

The botnet's creators targeted networked appliances that used an insecure default configuration or easy-to-find default passwords.

In the Internet of Things, everyday objects connect to the Internet, and then dynamically discover, send data to, and otherwise communicate with one another. Proponents say this makes controlling and using these items more convenient.

However, many of the connected objects are neither monitored nor well secured. Moreover, their owners know little about security. Thus, Proofpoint says, they are likely attack targets.

"Botnets are already a major security concern, and the emergence of thingbots may make the situation much worse," said David Knight, general manager of Proofpoint's Information Security Division.



Microsoft has chosen Satya Nadella (center) to be its third CEO. He is flanked by company founder and first chief executive Bill Gates (left) and second CEO Steve Ballmer (right).

Chinese Internet Traffic Accidentally Redirected to Two Small US Companies

For several hours, much of China's huge volume of Internet traffic was redirected to two small US companies, apparently caused by the unintentional actions of Chinese censors.

According to Web-performance–monitoring firm Compuware, users in most regions of China—which has 600 million people online, more than any other country—couldn't download websites with the .com, .net, or .org domains for about eight hours.

The problem affected about three-quarters of the country's Domain Name System servers.

It also redirected traffic intended for Chinese social networking sites and search engines to Internet addresses registered to Wyoming-based Sophidea and North Carolina-based Dynamic Internet Technology.

Sophidea offers traffic redirection services, which some people use to evade Chinese Internet censorship. Dynamic Internet Technology sells anticensorship software to customers, including content providers.

China typically blocks traffic to both companies.

The China Internet Network Information Center claimed hackers likely caused the traffic redirection problem.

However, many experts contend Chinese Internet censors were probably to blame.

They say it appears that Chinese censors were trying to block communications with Sophidea and Dynamic Internet Technology but accidentally rerouted large amounts of traffic to the companies.

Court Overturns US's Controversial Net Neutrality Policy

The US Court of Appeals in Washington, DC, has rejected controversial US Federal Communications Commission (FCC) rules on Net neutrality.

The Net neutrality policy, which the commission adopted in 2011, says ISPs should provide equal access and service to all traffic, regardless of volume, source, content, or platform.

Proponents say this is necessary to ensure that providers don't block certain traffic to, for example, stymie competition.

Without Net neutrality, supporters add, large carriers could also charge companies more for providing faster data rates. Only the biggest content providers could afford this, they say, so other companies would be relegated to slower service and a competitive disadvantage, making the Internet less open in the process.

Verizon Wireless challenged the FCC rules, saying it

HIGH-TECH HEADSET MEASURES USER ALERTNESS

A small startup has developed a headset designed to identify when users are becoming less alert and then "nudge" them electronically to increase their attentiveness.

Vigo (http://wearvigo.com) says its headset could help drivers, students in class, workers in meetings, machinery operators, and others who need to be as awake as possible.

The company's headset, also called Vigo, works with Android and iOS smartphones and tracks a wearer's blinking patterns and head movements to evaluate alertness in real time.

The Vigo device—which can also serve as a Bluetooth headset for use with mobile phones—tracks about 20 blink-related variables over time and watches how they change. The system then uses an algorithm that combines this data with information about time, user activity, and head motions to gauge alertness and identify attentiveness patterns throughout the day.

Wearers could use this information, along with recommendations from the system, to determine the best times to do tasks of varying complexity.

When Vigo senses that users are becoming less alert, it counters with either a flashing light, a vibration in the earpiece, or an alarm.

The 20-gram device contains an infrared sensor that detects eye and eyelid movements, an accelerometer and a gyroscope to track head movements, a Bluetooth 4.0 chip, and an ARM Cortex-M0 16-MHz processor that runs the alertness algorithm.

Users could adjust the algorithm's sensitivity to enable various target alertness levels.

Vigo hopes to begin shipping the $79 headset in May.

The Vigo headset tracks wearers' eyeblinks and head motions to determine if they are becoming less alert. If so, the device tries to get users to focus via a flashing light, earpiece vibrations, or an alarm.

and other providers should be able to manage traffic on their own networks as they see fit.

The Court of Appeals said that the FCC has the right to regulate the Internet. However, it ruled, the commission currently classifies Internet access as an information service rather than a telecommunications utility, which exempts ISPs from regulations such as Net neutrality.

The FCC said it might appeal the Court of Appeals ruling. The commission could also try to reclassify ISPs as utilities so that it could regulate them more closely.

Connected Cars Raise Privacy Concerns

Automobiles are becoming more and more connected to the outside world and are increasingly gathering data about themselves and their drivers.

Many vehicles have computers, Web browsers, cellular telephones, GPS devices, and black-box information collection systems.

Proponents say these features provide convenience to drivers—such as directions and Internet connections—and information that automakers can use to improve their vehicles.

However, these capabilities are also raising privacy concerns.

For example, privacy advocates say police officials shouldn't be able to access car-collected data to look for driving violations.

They also say authorities shouldn't be able to gather information that would let them determine where drivers live, shop, visit friends, take children to school, or otherwise spend time.

The General Accountability Office—the US Congress's audit, evaluation, and investigative arm—reported that the automakers, GPS-device manufacturers, and application developers it studied don't follow all industry-recommended privacy practices. It also said consumers often don't understand the privacy ramifications of using in-car services.

Several US senators have expressed concerns about such matters and say they plan to introduce legislation to address them.

New Product Adds Physical Buttons to Touchscreens

A new product uses microfluidics to create a physical keyboard on the flat surface of a touchscreen. The provision of physical buttons provides users with tactile feedback and also lets them rest fingers not being used for typing.

Manufacturer Tactus Technology says this would make smartphones, tablets, and other machines with only virtual keyboards easier to work with and address the frequent complaints many users have about trying to type on the devices.

The tactile user interface is a 1-millimeter-thick microfluidics panel that sits on devices' LCD in place of the standard plastic or glass.

Holes in the panel would let fluid enter and raise parts of the flexible polymer surface to form buttons when a user activates it. When the user disables the buttons, they

recede completely into the screen, leaving a flat viewing surface.

Via a tactile controller, users can generate buttons in various sizes, shapes, and degrees of rigidity.

Tactus says its system will enable images to pass through the microfluidics panel and liquid and thus still be visible on the screen.

The company provides an API to enable development of applications that work with its system.

Tactus Technology's new product generates a physical keyboard on a touchscreen's normally flat surface.

Google Plans Smart Contact Lenses

Google is developing a contact lens—complete with a processor and sensors—designed to monitor the level of glucose in diabetics' tears and alert wearers if their blood-sugar levels are too high.

This could eliminate the ongoing, intrusive blood testing that diabetics currently must perform.

Diabetes sufferers—one of every 19 people in the world—have high blood-sugar levels because either their pancreas doesn't produce enough insulin or their cells don't respond to the insulin it produces.

When diabetes gets out of hand, people can suffer multiple health problems, including eye, kidney, and heart damage.

Currently, diabetics monitor their blood-sugar level by pricking their finger and smearing a bit of blood onto a test strip, which they then insert into a reader.

The device that Google researchers are working on would consist of a tiny wireless communications chip and glucose sensors—which would take readings once per second—embedded within a lens.

A nearby transmitter would remotely power the embedded electronics by sending RF energy to a 5-millimeter-long antenna in the lens.

The scientists are working on putting LED lights inside the lens that would flash when blood-sugar levels are too high.

Google is testing the device, conducting research studies, and working with the US Food and Drug Administration. It is also looking for companies to market the product.

Researchers Develop Ultrahigh-Density Storage

UK researchers have developed a technology using quartz glass that can store huge volumes of data in a very small space for hundreds of years.

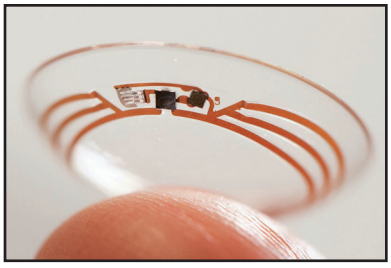
High-density storage is an important goal as a way to cope with the growing volumes of data that organizations are collecting.

The new system, developed at the University of Southampton, stores data by putting tiny marks on the quartz glass in ways that a reading device can detect. The technology increases capacity by creating additional storage dimensions using optical techniques based on the multiple ways that quartz refracts light.

This enables storage densities of up to 360 Tbytes per disc, which is thousands of times more than today's high-capacity Blu-ray discs.

However, users need an electron microscope to read the data the system contains. And accessing the information is no faster than with today's storage technology. This would be a problem when people need to access data quickly. In these cases, users currently employ flash memory, hard drives, or dynamic RAM.

Quartz's durability would allow data to be stored for centuries, according to the researchers. They say this would eliminate the time and money currently spent on copying data to new media over time as old media deteriorate.



Google is designing a contact lens with a chip and sensors to monitor the blood-sugar level in diabetics' tears.

The new technology could work well for information that must be stored for long periods of time for purposes such as future analysis or compliance with government data retention regulations. However, it would have to become less expensive than magnetic tape, which is typically utilized for long-term storage.

Editor: Lee Garber, *Computer*; l.garber@computer.org