Hackers Hit Sony with Devastating Attack

Hackers have attacked Sony Pictures with sophisticated malware as part of an assault that crashed the company’s computers for a week, wiped data from its hard drives, froze its email system, leaked its upcoming movies, and exposed confidential corporate documents and information including employee salaries and Social Security numbers.

A group calling itself the Guardians of Peace claimed credit for the attack, in which 100 terabytes of data were stolen.

US investigators say the hack was actually launched by the North Korean government, which is suspected of similar types of intrusions in the past.

That government, which has not claimed credit for the attack, has also expressed strong disapproval of a recently released Sony movie, The Interview, about a couple of US TV show hosts being asked by the CIA to kill North Korean leader Kim Jong-un.

In the recent incident, the hackers obtained copies of several major Sony movies and released them to illegal file-sharing websites. These films included the already-released Fury with Brad Pitt and Annie with Jamie Foxx. They have since been downloaded illegally 2.3 million and 278,000 times, respectively. Illegal downloads cost Sony millions of dollars in lost revenue from theater tickets, as well as DVD rentals and sales.

The attackers additionally swiped Sony personnel’s passwords and released internal communications that could prove embarrassing to the company. These include memos from employees criticizing the company’s movies as boring, unoriginal, and formulaic, and bashing actors like Angelina Jolie.

Also stolen was information about the salaries of 6,000 Sony Pictures workers, including data showing that of 17 employees making at least $1 million annually, only one is female and only one is African-American.

The hackers took and posted names, Social Security numbers, birth dates, and other personal data sufficiently sensitive to put 15,000 workers at risk of identity theft.

And they released data on personnel appraisals, firings, and layoffs, as well as confidential information, including Social Security numbers, for celebrities such as Sylvester Stallone.

The attack has been so damaging that the FBI is warning other companies about the Windows-targeting malware that was used.

Security researchers say it appears that the hackers were in Sony’s network for a while before launching their assault and that their malware was designed to spread via the company’s email server system.

To make matters worse, security researchers say Sony apparently inadequately secured its system. For example, most of the stolen sensitive information wasn’t password-protected. In addition, the hackers are sharing pilfered files using computer servers owned by Sony’s PlayStation Network.

Sony has said little so far about the attacks except that it’s working with law-enforcement agencies.

Hackers claiming to be with the Guardians of Peace later issued an implied threat, saying in an online post that people should avoid going to theaters where The Interview is playing.

Many large US cinema chains decided not to show the movie during its scheduled Christmas weekend opening, so Sony cancelled that release date.

Big E-Commerce Websites Crash under the Weight of Holiday Shopping Traffic

In the US, the day after the Thanksgiving holiday—which occurs on the fourth Thursday of November—is one of the busiest cybershopping days of the year.

The day—called Black Friday because it’s the time many businesses move from being in the red (losing money) to being in the black (profitable) for the year—lived up to its reputation.

In fact, it produced so much traffic that the websites of several major e-tailers—including electronics giant Best Buy, tech stalwart Hewlett-Packard, and office retailer Staples—crashed or suffered slowdowns.

On a blog published by Dynatrace—a division of the Compuware Corp. that
focuses on application performance management—technical evangelist David Jones said factors such as internal technical problems, site complexity, and a spike in mobile traffic caused the website malfunctions.

The issues occurred even though many companies are using multiple content-delivery networks to handle traffic regionally and thereby reduce the overall amount of traffic hitting any single e-commerce site.

Hewlett-Packard’s HP Shopping site crashed due to a problem with the company’s internal cloud system. This is potentially embarrassing because the company is promoting itself as a major cloud-service provider.

Best Buy’s website—which initially performed normally—went offline briefly due to an unidentified internal error. However, the site refreshed itself and returned to normal operations in a couple of hours.

Staples’ website suffered several slowdowns. Shoe retailer Foot Locker also experienced Black Friday e-commerce woes, apparently because of problems with the configuration that a content-delivery network provider used.

The website for Cabela—which sells hunting, fishing, and outdoor gear—experienced brief instability and outages through Black Friday due to unidentified internal factors. The company solved the problems fairly quickly and operations returned to normal.

Lawmakers Approve Plan that Could Break Up Google in Europe

In a move apparently aimed at Google, the European Parliament has adopted a proposal that supporters say would increase competition by forcing companies to separate their search-engine operations from their other commercial services.

Proponents say this would keep companies from using their search engines to produce biased results that promote their other businesses.

Opponents say the plan is unfairly

FATHER OF THE HOME VIDEO-GAME CONSOLE DIES

Ralph Baer, who invented the first console that let people play video games at home, died recently at his home in Manchester, New Hampshire, at the age of 92.

Baer, whose Jewish family escaped Nazi Germany right before World War II, began researching ways to play video games on a TV screen in 1966, while an engineer at defense contractor Sanders Associates.

He eventually designed hardware and software for the Brown Box—now on display at the Smithsonian Institution—which Sanders patented. The company licensed the technology to Magnavox, which used it in 1972 to develop the Odyssey, the first commercial home gaming console.

This helped transform gaming from an activity people undertook only on large machines to one people could play at home on TV, thereby kicking off what has become a multibillion industry.

The $100 battery-powered Odyssey used overlay sheets to simulate color graphics and had no sound capabilities. It sold about 100,000 units in 1972. This was five years before the Atari 2600 became the first million-unit-selling video game console. Atari had licensed Baer’s technology from Magnavox.

Baer, who was born in 1922, immigrated with his family to New York City from Germany in 1938. After working in a leather-goods factory, he saw an advertisement for a correspondence class in radio electronics and signed up.

Baer became a radio service technician until World War II, when he served in the US military intelligence service. He then obtained a bachelor’s degree in television engineering and got the job at Sanders, which he held until retiring in 1987 with 50 US and 100 international patents.

Baer also developed numerous toys and video games.

In 2006, US President George W. Bush awarded him the National Medal of Technology for his contribution to the video-game industry. The National Inventors Hall of Fame inducted him in 2010.
This marks the latest dispute between Google and European officials who, in the past, have investigated and fined the company for allegedly unfair business practices and privacy violations.

**Advanced Malware Spied on Victims for Six Years before Discovery**

Security vendor Symantec has discovered sophisticated malicious software that has been spying on individuals, governments, academic researchers, companies, and telecommunications infrastructures since 2008.

In a white paper, Symantec called the Regin malware “groundbreaking and almost peerless.”

Company researchers said it was used on targets primarily in Russia and Saudi Arabia, but also in countries such as Afghanistan, Austria, Belgium, India, Ireland, Mexico, and Pakistan. The malware reportedly was used to spy on numerous European Union companies.

Regin consists of various modules and divides its attacks into five stages. The malware ultimately collects passwords and screenshots from victims’ computers, monitors network traffic, gathers information from memory, retrieves deleted files, and takes over machines’ point-and-click capabilities.

According to Symantec, users could customize Regin and add new features and capabilities. For example, in one case, it was configured to analyze mail from Microsoft’s Exchange email databases.

Researchers said the attackers apparently used Regin to gather intelligence, not to steal intellectual property.

In one case aimed at specific individuals, the malware scoured airline and hotel computers to learn the dates when target victims were traveling and the hotels at which they were staying. It then searched various telecommunications systems to identify the people they spoke with.
Symantec says the malware infects victims in various ways, some still unidentified.

For example, the attackers have used social engineering to direct targets to fake versions of popular websites, which then uploaded Regin.

Researchers noted that the malware was so complicated that it probably took months or perhaps years to write and that the developers encrypted some of its modules and used other techniques to make it difficult to trace.

Security experts say the multistage approach and general complexity is like previous espionage tools—such as Flame and Stuxnet—believed to be developed by government hackers. However, they haven’t yet been able to identify who designed Regin.

They said they are aware of only 100 infections by the malware, first used to spy on individuals in 2008 before being withdrawn in 2011 and then updated and rereleased in 2013 to eavesdrop on bigger targets.

### Gaming Companies Worried that Using Virtual Reality Could Make Players Sick

Several new technological developments have caused excitement that game developers might finally incorporate virtual reality (VR) into their products.

For example, Oculus VR has unveiled several prototypes of its Oculus Rift virtual-reality head-mounted display and plans to release a commercial version next year, along with a software developer’s kit. The product could be used with games from various manufacturers.

Sony Computer Entertainment is developing Project Morpheus—a VR headset that would work with the Sony PlayStation 4 and PlayStation Vita game consoles—which could be available in 2015.

Players, console makers, and game developers have said VR could enhance the playing experience, which could ultimately increase device and game sales.

However, some major game publishers have not yet supported making the considerable investment necessary to introduce the technology into their products.

Two of the biggest publishers—Take-Two Interactive Software and Electronic Arts—say they are concerned that VR could give some players motion sickness.

According to Take-Two, not only does the technology currently cause nausea in some users but developers must also figure out how game controllers should work within a VR environment.

Electronic Arts—which has experimented with VR—says that the technology has potential but that prototype headsets have caused motion sickness in people, including those only slightly prone to such problems.

However, both companies say that the problem doesn’t seem
Some experts speculate they used denial-of-service attacks on Tor to force its traffic over connections that the authorities own and operate, thereby letting them see the senders’ IP addresses.

The ability of law-enforcement agencies to bypass Tor’s protection calls the anonymizing system’s effectiveness into question. However, some experts say the targeted websites’ owners may have made the errors that allowed investigators to locate them.

Tor lets users who download the necessary software surf the Web anonymously so that government agencies, companies, and others can’t easily uncover their IP address. The system accomplishes this by routing its Internet traffic through a worldwide volunteer network of about 5,000 nodes.

Typically, the service is used by people wanting anonymity such as government whistle-blowers and citizens of nations with repressive governments. However, criminals have also employed Tor.

“Today we have demonstrated that, together, we are able to efficiently remove vital criminal infrastructures that are supporting serious organized crime. And we are not just removing these services from the open Internet. This time we have also hit services on the darknet using Tor where, for a long time, criminals have considered themselves beyond reach. We can now show that they are neither invisible nor untouchable,” said European Cybercrime Center director Troels Oerting.

The countries involved in Operation Onymous were Bulgaria, the Czech Republic, Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Romania, Spain, Sweden, Switzerland, the UK, and the US.

Researchers: Many Children’s Apps Violate Users’ Privacy

A study by Carnegie Mellon University (CMU) computer scientists found that many Android applications for kids invade their privacy by gathering large amounts of personal information about them.

The researchers—led by associate professor Jason Hong, director of CMU’s Computer Human Interaction: Mobility Privacy Security group—analyzed about 1 million free apps. They awarded A, B, C, or D grades based on how the programs track visitors and whether users expect such tracking based on the nature of the app.

The results are posted on the project’s website (http://PrivacyGrade.org).

According to Hong, “These apps access information about a user that can be highly sensitive, such as location, contact lists, and call logs, yet it often is difficult for the average user to understand how that information is being used or whom it might be shared with.”

He continued, “Our privacy model measures the gap between people’s expectations of an app’s behavior and the app’s actual behavior. Most people expect apps such as Google Maps to be able to access their location, but most are surprised and troubled to learn that a game [also does].”

The majority of the most popular apps received higher grades. But 1,000 applications—including many for kids—received the lowest rating.

The problem, the researchers said, is that some developers want to make money from their free apps and thus add code that collects data they can sell to advertisers. In some cases, the study noted, developers aren’t trying to be malicious but don’t consider how intrusive these practices can be.

The CMU project—conducted in part with financial assistance from
Google, which developed and manages Android—has several limitations. For example, it grades only free apps. And, the researchers acknowledge, their privacy model and analytical tools may need some fine-tuning.

They used a program to scan Android apps to identify the programs’ privacy practices, as well as algorithms that compared those practices with user expectations.

Developers can comment on or disagree with grades their apps received from the researchers via a feedback form on the PrivacyGrade.org website.

Hong said he would like to conduct a similar study of iPhone apps but doesn’t yet have a contact at Apple to work with.

New Bluetooth Version Offers Online Connectivity, Could Advance Internet of Things
A standards group has adopted a new version of Bluetooth that would enable direct Internet connections for the first time. The technology could enable all types of devices to connect online.

Bluetooth 4.2 could thus prove important as the Internet of Things (IoT)—in which many types of everyday devices can connect to the Internet and to one another online—becomes widely adopted.

In addition to Internet connectivity, the new version of the short-range, low-power wireless technology—which the Bluetooth Special Interest Group (SIG) recently adopted—offers more speed and privacy than earlier versions.

It will let Bluetooth Smart sensors connect to the Internet via IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) technology. This approach lets even small objects—like those that could become part of the IoT—access the Internet via a gateway.

Bluetooth 4.2 will use packets 10 times the capacity of those used in earlier versions of the technology. This will enable connection speeds that are 2.5 times faster and reduce transmission errors. Also, larger packets’ greater efficiency will lower power consumption and increase devices’ battery life.

The new standard will also allow users to encrypt transmissions, which would be important for people who want to use their devices for secure activities such as unlocking their homes’ front doors.

To improve privacy, the specification will force beacons—Bluetooth-based technology that retail stores are increasingly using to send promotional messages to shoppers’ mobile devices—to obtain permission from users before tracking and contacting them.

Despite the improvements, industry observers say Bluetooth can still be difficult to pair with devices.

Scientists Build Molecular-Level Flash-Storage System
To improve the performance of computing and memory chips, engineers have made their circuitry and transistors smaller and smaller, allowing them to pack more on each unit.

Continuing this trend will be difficult, scientists say, because it would cause chips to experience problems such as increasing charge leakage and greater susceptibility to flaws. In addition, the manufacturing process would become more difficult and expensive.

Because of this, engineers are working on producing processor elements out of molecular-level elements, rather than traditional electronic components.

For example, researchers from the University of Glasgow and the University of Rovira i Virgili have developed a molecular system that could work as flash memory, which is nonvolatile, the researchers covered a wire with one layer of their caged molecules and applied a large negative charge. After the electricity was shut off, the charge remained along the wire throughout a 336-hour test. This indicated that a device using this technology could store and then provide data even after being turned off.

Users could read data from the device by applying a small charge and could delete stored information by applying a large positive charge.

Current problems with the new technology include high energy consumption and slow write and read speeds.

This scanning electron microscope image shows a 5-nanometer wire coated with cages of tungsten oxide molecules containing two selenium trioxide molecules. Researchers have demonstrated that this device might be able to function as high-performance flash memory.