

Sony PlayStation Taken Down for Weeks by Hackers

May 2011

This may be the biggest hacking story in history – at least so far. In mid-April, 2011, hackers gained access to Sony's online gaming servers and stole sensitive personal information for over 100 million accounts. It is estimated that this breach could cost Sony and credit/debit card issuers up to \$2 billion U.S. in recovery expenses, not to mention the cost of pending lawsuits.

As soon as Sony discovered the breach, it closed down its online gaming services until it could restructure its security defenses. This happened on Wednesday, April 20th. At the time, Sony indicated that its services might be down for a few days. As of this writing, gaming services have been down for three weeks and counting. Sony has stopped predicting when its online games will resume.

Though Sony is teaming with the FBI (the U.S. Federal Bureau of Investigation) and private investigators, the perpetrators have yet to be identified. However, there is evidence that points to a hacking group that wanted to get revenge for Sony's "unfair legal actions" against a well-known hacker who had managed to find and publish the secret keys to Sony's online games.

Sony's Online Gaming Services

Several Sony entities were involved in this incident. Sony Online Entertainment (SOE) is Sony's game development and publishing division. Its games are MMORPG games – massive multiplayer online role-playing games – in which millions of subscribers compete with each other for mastery.

PlayStation 3 is the latest version of Sony's very popular home video game console. It is used to play both offline and online games and competes with Microsoft's Xbox and Nintendo's Wii.

The PlayStation Network (PSN) is Sony's online network for supporting multiplayer games using the PlayStation 3.

Qriocity (pronounced curiosity) is Sony's on-demand streaming services for videos, music, games, and ebooks.



Sony PlayStation 3 console (Christian Science Monitor)

Sony Online Entertainment, PlayStation Network, and Qriocity are all subscription-based services with monthly subscription fees. Sony maintains the account information for all subscribers on its servers. There are about 77 million subscribers for PSN and another 25 million for SOE.

The Intrusion

From April 16 through April 18, 2011, unbeknownst to Sony, hackers gained access to Sony's gaming servers for the PlayStation Network, Qriocity, and SOE. Sony personnel did not detect the intrusion into the PSN and Qriocity servers until the following day, April 19th. On April 20th, they shut down the PSN and Qriocity services, explaining that the servers were down for maintenance. All online gaming using the PlayStation 3 console was dead, though offline games could still be played. All Qriocity streaming services were terminated.

It was not until April 23rd that Sony publicly disclosed the breach of PSN and Qriocity. It acknowledged that 77 million accounts were vulnerable but said that it did not think any critical personal data had been compromised. Later, Sony revealed that names, addresses, email addresses, birthdates, and login information might have been compromised. However, it had no indication that credit- or debit-card numbers had been stolen, though this could not be ruled out.

On April 25th, Sony announced that the enhancements it needed to beef up its security protection services would be time-consuming. On May 1st, it predicted that some services would be back online during the first week in May.

Then on May 1st, the magnitude of the disaster was discovered to be worse than originally thought. The investigating team found that the mid-April attacks had also similarly compromised the 25 million subscriber accounts for SOE. The company shut down the Sony Online Entertainment services the next day and ceased making predictions as to when services would be restored. As of this writing, May 8th, no further word has been forthcoming as to when online gaming services will be restored.

Even Congress Gets Involved

Shortly after Sony announced that credit- and debit-card information may have been stolen, the U.S. House of Representatives' Subcommittee on Commerce, Manufacturing, and Trade sent Sony a letter demanding answers to several questions. On its May 4th PlayStation blog, Sony summarized its responses to the Congressional inquiry:

"In summary, we told the subcommittee that in dealing with this cyber attack we followed four key principles:

1. Act with care and caution.
2. Provide relevant information to the public when it has been verified.
3. Take responsibility for our obligations to our customers.
4. Work with law enforcement authorities.

"We also informed the subcommittee of the following:

- Sony has been the victim of a very carefully planned, very professional, highly sophisticated criminal cyber attack.
- We discovered that the intruders had planted a file on one of our Sony Online Entertainment servers named "Anonymous" with the words "We are Legion."
- By April 25, forensic teams were able to confirm the scope of the personal data they believed had been taken, and could not rule out whether credit card information had been accessed. On April 26, we notified customers of those facts.
- As of today, the major credit card companies have not reported any fraudulent transactions that they believe are the direct result of this cyber attack.
- Protecting individuals' personal data is the highest priority and ensuring that the Internet can be made secure for commerce is also essential. Worldwide, countries and

businesses will have to come together to ensure the safety of commerce over the Internet and find ways to combat cybercrime and cyber terrorism.

"We are taking a number of steps to prevent future breaches, including enhanced levels of data protection and encryption; enhanced ability to detect software intrusions, unauthorized access and unusual activity patterns; additional firewalls; establishment of a new data center in an undisclosed location with increased security; and the naming of a new Chief Information Security Officer."

Sony's Customer Care Response

On May 5th, Harold Stringer, CEO of Sony, reiterated that credit-card numbers did not appear to have been compromised:

" To date, there is no confirmed evidence any credit card or personal information has been misused; and we continue to monitor the situation closely. We are also moving ahead with plans to help protect our customers from identity theft around the world. A program for U.S. PlayStation Network and Qriocity customers that includes a \$1 million identity theft insurance policy per user was launched earlier today, and announcements for other regions will be coming soon."

The identity-theft insurance that Mr. Stringer referred to is AllClear ID Plus from Debix. It provides monitoring of credit-card usage, notification of suspicious activity, and the assignment of an investigator to help resolve credit issues. It provides \$1 million of identity-theft insurance for covered expenses. Sony will provide the service free to all U.S. customers for the first year. It is looking into providing similar protection to its other international customers.

In addition, Sony is offering thirty days of free service plus one additional day for every day that the gaming services are down.

The Potential Cost to Sony

Not even considering litigation or regulatory costs, Sony can face some extraordinary costs. Simply replacing a credit- or a debit-card costs the issuing bank an estimated \$25. With the potential of replacing millions of cards, this is a big expense for the issuing banks, one that Sony may have to pick up.

In addition, there is the cost of the identify-theft insurance for 100 million subscribers. This is bound to cost millions of dollars. It has been estimated that Sony's costs for the intrusion could range in the order of \$1 to \$2 billion dollars U.S..

Who Dunit?

The big open question is who were the perpetrators? Sony is working with the FBI and several select private investigation firms to try to track them down. Though there has been no definitive word on the culprits, there is a strong suspicion. It has to do with an earlier hacking of Sony's PlayStation.

George Hotz, known on the web as Geohot, is a renowned and very successful 22-year old American hacker. He is known for unlocking Apple's iPhone, allowing it to be used with other wireless carriers contrary to AT&T's and Apple's intent.

Late in 2009, Hotz announced his intention to hack Sony's PlayStation; and in January, 2010, he posted details of how he had gained control for read/write access of the PlayStation operating system.

On January 2, 2011, Hotz took a dramatic step when he posted the root keys for the PlayStation 3 on his web site. The keys are used by PlayStation 3 to validate that a piece of software is legitimate. Knowing the root keys, hackers can create custom software for the PlayStation and can use pirated games.

Sony was faced with a dilemma. The root keys can only be changed via a hardware modification. Once made, current games would be rendered inoperable. In response to this threat, Sony obtained a restraining order against Hotz on January 11th and initiated legal action. The root keys were immediately taken off of his web site.



George Hotz (Wikipedia)

Then suddenly, on April 2nd, a distributed denial of service (DDoS) attack was made on the PSN servers, taking down PlayStation games for several hours. The attack was launched by an online distributed, decentralized activist group calling themselves "Anonymous." Anonymous stated that the attack was in defense of free speech – presumably Hotz's right to post any information that he wanted to.

On April 11, 2011, Sony and Hotz announced that the lawsuit had been settled on the condition that Hotz would never again hack Sony products. Anonymous declared that it would intensify its attacks on Sony and called for a day of protest on April 16th. The intrusion to Sony's servers and theft of user information occurred from April 16th to April 18th.

Interestingly, during the investigation of the break-in, the investigators found a calling card of sorts stored on a server. It was a file named "Anonymous" and contained the message, "We are Legion." This led to the suspicion that Anonymous was the culprit. However, Anonymous denied involvement, saying that "We are trying to fight criminal activities by corporations and governments, not steal credit cards." George Hotz also condemned the attack, noting that stealing databases was much different than hacking to gain play access.

The jury is still out.

Lessons Learned

Beware of hackers. They can do serious damage if they want to. And they are probably smarter than you are. Even worse, this incident shows that they are a loosely knit group that can be fiercely loyal to each other.

Sony has learned a great deal from this incident, unfortunately at great cost. As Sony summarized its reply to the U.S. Congress in its blog:

"We are taking a number of steps to prevent future breaches, including enhanced levels of data protection and encryption; enhanced ability to detect software intrusions, unauthorized access and unusual activity patterns; additional firewalls; establishment of a new data center in an undisclosed location with increased security; and the naming of a new Chief Information Security Officer."

They are all good defenses to consider.

Acknowledgements

Thanks to our subscriber, Mike Kelley, for pointing us to this event and for providing much of the research that went into this article. Additional information came from the following sources:

George Hotz Releases Playstation 3 Root Keys, *The Tech Journal*; January 4, 2011.
Sony and PlayStation 3 jailbreaker George Hotz settle out of court, *Joystiq*; April 11, 2011.
Congress Has Questions for Sony About Attack, *New York Times*; April 29, 2011.
Cyber Crime, *Lanka Business Online*; May 3, 2011.
Sony data breach could be most expensive ever, *Christian Science Monitor*; May 3, 2011.
Sony Hired Investigators To Catch Hackers Behind Security Breach, *News Blaze*; May 4, 2011.
PlayStation breach compromises millions of users' online data, *Indiana Daily Student*; May 5, 2011.
PlayStation hack: timeline of huge security breach, *The Telegraph*; May 5, 2011.
Sony CEO Stringer apologizes for PlayStation, *CNET News*; May 5, 2011.
PlayStation Network Down Indefinitely - - Again, *PC World*; May 8, 2011.
PlayStation Network, *Wikipedia*.
Sony Online Entertainment, *Wikipedia*.
Qriocity, *Wikipedia*.
PlayStation Network Outage, *Wikipedia*.
George Hotz, *Wikipedia*.