***Sony Films Are Pirated, and Hackers Leak Studio Salaries***

**By**[**BROOKS BARNES**](http://www.nytimes.com/by/brooks-barnes)**and**[**NICOLE PERLROTH**](http://www.nytimes.com/by/nicole-perlroth)DEC. 2, 2014



A scene from "The Interview," a comedy Sony plans to release for Christmas starring James Franco, left, and Seth Rogen as two American journalists recruited by the C.I.A. to kill North Korea's leader, Kim Jong-un.CreditEd Araquel/Columbia Pictures

LOS ANGELES — Just as Sony Pictures Entertainment appeared to be recovering from a crippling online attack last month, the studio found itself confronting new perils on Tuesday. The [Federal Bureau of Investigation](http://topics.nytimes.com/top/reference/timestopics/organizations/f/federal_bureau_of_investigation/index.html?inline=nyt-org)warned United States businesses of a similar threat, and additional Sony secrets were leaked online.

Sony, the studio behind “The Amazing Spider-Man” films and the “Breaking Bad” television series, restarted many of its computer systems on Monday after a Nov. 24 breach by a group calling itself #GOP, for Guardians of Peace. Executives at the entertainment company said they were also making progress in fighting the apparently related Internet pirating of five complete films, including the unreleased “Annie.”

But Sony was newly rattled by the leak of internal documents, one of which contained the pre-bonus annual salaries of senior executives, [showing 17](http://fusion.net/story/30789/hacked-documents-reveal-a-hollywood-studios-stunning-gender-and-race-gap/)who earn more than $1 million a year. The documents were published late Monday on Pastebin, the anonymous Internet posting site.

The breach exposed two things the secretive movie industry is extremely sensitive about — the piracy of films and details about [executive compensation](http://topics.nytimes.com/top/reference/timestopics/subjects/e/executive_pay/index.html?inline=nyt-classifier) — and sent a ripple of dread across Hollywood to Washington.

Although large attacks on companies are increasingly common, this one has played out like one of Sony’s own thrillers, with macabre images on computer screens of studio executives’ severed heads and theories that the attack could be retribution from North Korea for a coming Sony comedy about an assassination attempt on that country’s leader, Kim Jong-un.

Tom Kellermann, chief cybersecurity officer at Trend Micro, the private security firm, said that unlike stealth attacks from China and Russia, Sony’s hackers not only aimed to steal data, but also to send a clear message. “This was like a home invasion where after taking the family jewels the hackers set the house ablaze,” he said.

The attack at Sony comes as major American companies and government agencies are still reeling from online security threats. Breaches at major retailers like Target, Home Depot and Staples were only the beginning. Over the last year, the White House, the State Department, the nation’s largest bank, energy companies, even the Postal Service, were all breached by attackers who have yet to be identified or apprehended.

But the Sony attack, and new details about a spate of coordinated cyberattacks from Iran that emerged on Tuesday, have security experts and law enforcement authorities rattled, worried that Sony’s difficulties may be a harbinger of many more to come.

“In 2015 hackers will destroy systems not just for activism, but also for counter-incident response,” said Mr. Kellermann, suggesting that it would be more difficult for security firms and companies to investigate, respond and recover from cyberattacks.

The F.B.I. issued a private bulletin late Monday to a wide range of companies about a malicious software threat that wipes data from computers beyond the point of recovery.

The agency did not name the companies attacked, or say whether the bulletin was linked to the Sony attack, but the description mirrored the findings at Sony. The F.B.I. on Monday confirmed that it was working with the company to investigate the attack.

Joshua Campbell, an F.B.I. spokesman, said on Tuesday that the agency’s “flash” warning, first reported by Reuters, was a routine advisory intended to “help systems administrators guard against the actions of persistent cybercriminals.”

Two people with knowledge of the advisory’s contents said the bulletin warned companies of malware that could destroy data on their hard drives and prevent computers from rebooting. The malware overwrites data in such a way that it can be nearly impossible to recover using standard means.

Sony declined to comment on Tuesday beyond its previously released statements. “The company has restored a number of important services to ensure ongoing business continuity and is working closely with law enforcement officials to investigate the matter,” one statement read. Sony is notably dealing with the breach and its aftermath without a public relations chief, having dismissed its top corporate communications executive the week before the attack occurred.

To restore its computer systems, Sony’s movie and television divisions — a large music unit was not affected — hired the Mandiant division of FireEye, one of the larger online security firms.

With Mandiant’s help, business on Monday largely returned to normal at the studio, according to employees who spoke on the condition of anonymity. A previously scheduled town hall gathering to welcome a new movie marketing and distribution executive went forward as planned. The usual trade news trickled out — a casting announcement here, an international television deal there.

Inside Sony’s offices on Tuesday the mood was subdued but far from panicked, according to several employees, who said the attack had led to an unusually high degree of camaraderie. But they remained nervous about the breach of personal data and the possibility of [identity theft](http://topics.nytimes.com/your-money/credit/identity-theft/index.html?inline=nyt-classifier).



The unreleased Sony film “Annie” was pirated in a cyberattack in November, along with four other movies.CreditBarry Wetcher/Columbia Pictures

On Pastebin, hackers released on Monday evening what they said were “tens of terabytes” worth of internal Sony data. The post — titled “Gift of G.O.P.” — included links to various archives that appeared to contain Sony employees’ passwords, [Social Security](http://topics.nytimes.com/top/reference/timestopics/subjects/s/social_security_us/index.html?inline=nyt-classifier) numbers, salaries and performance reviews. (The password to open many of the files was “diespe123” (presumably an abridgment of “Die Sony Pictures Entertainment”). The studio has offered to enroll employees in a fraud protection program.

“The problem is that every time there is another leak, people clench up all over again,” said one executive in Sony’s home entertainment division.

On Nov. 24, just as Sony employees were settling into their work day, the hacking group took over many of the studio’s internal systems. Some screens included images of a menacing red skeleton with the warning, “If you don’t obey us, we’ll release data shown below to the world.”

What Sony was to obey was not specified and, aside from the pirated films, no corporate data was leaked — until the salary information showed up, along with [Social Security](http://topics.nytimes.com/top/reference/timestopics/subjects/s/social_security_us/index.html?inline=nyt-classifier) numbers, marketing plans, financial information and even the script to an in-house recruiting video, posted to Pastebin Monday evening. The information has since been pulled from the site.

The hackers also took over certain Twitter feeds for Sony films. For instance, an account for “Starship Troopers,” a science fiction series, was hacked to say, “You, the criminals including Michael Lynton will surely go to hell. Nobody can help you.” Mr. Lynton is chief executive of Sony Pictures.

The intrusion prompted Sony technicians to shut down the studio’s computer systems, leaving employees without email, the Internet or voice mail. Movie and television production continued, in part because the studio operates a separate, more secure system for processing video.

Why Sony? Although the studio is exploring multiple explanations, one theory involves North Korea. This Christmas, Sony plans to release “The Interview,” an R-rated comedy about two American journalists who are recruited by the Central Intelligence Agency [to kill Mr. Kim](http://www.nytimes.com/2014/11/30/business/media/intrusion-on-sony-unit-prompts-a-shutdown-of-messaging-systems.html). A spokesman for North Korea’s Foreign Ministry called the film — apparently after seeing a trailer — “the most undisguised terrorism and a war action.”

The spokesman added that the film would invite “a strong and merciless countermeasure.”

The destructive attack at Sony mirrors similar attacks last year on computers inside South Korea that paralyzed the computer networks at three major South Korean banks and two of the country’s largest broadcasters. Those attacks were traced back to computer addresses inside China, though many suspected that hackers inside China were working on behalf of North Korea, retaliating against South Korea for conducting military exercises with the United States, and for supporting recent American-led sanctions against the north.

Regardless, Sony is moving ahead with the release of the comedy. Seth Rogen, who stars in the movie, on Tuesday began a round of long-scheduled publicity interviews.

***Correction: December 2, 2014*** *An earlier version of a picture caption with this article misspelled the surname of an actor in “The Interview.” He is Seth Rogen, not Rogan.*