# THE HOMELAND SECURITY *NEWS CLIPS*

PREPARED FOR THE DEPARTMENT OF HOMELAND SECURITY BY BULLETIN NEWS WWW.BULLETINNEWS.COM/DHS

**TO:** **THE SECRETARY AND SENIOR STAFF**

**DATE:** **TUESDAY, MARCH 1, 2011 7:15 AM EST**

## TODAY'S EDITION

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

## Morgan Stanley Hacked In China-Based Attacks That Hit Google (BLOOM)

By Michael Riley

Bloomberg News, March 1, 2011

Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers more than a year ago, according to leaked e-mails from a cyber-security company working for the bank.

The e-mails from the Sacramento, California-based computer security firm HBGary Inc., which identify the first financial institution targeted in the series of attacks, said the bank considered details of the intrusion a closely guarded secret.

"They were hit hard by the real Aurora attacks (not the crap in the news)," wrote Phil Wallisch, a senior security engineer at HBGary, who said he read an internal Morgan Stanley report detailing the so-called Operation Aurora attacks.

The nickname came from McAfee Inc., a Santa Clara, California-based cyber-security firm, which said the attacks occurred for about six months starting in June 2009 and marked "a watershed moment in cyber security." The number of companies known to be hit in the attacks was initially estimated at 20 to 30 and now exceeds 200, said Christopher Day, senior vice president for Terremark Worldwide Inc., which provides information-technology security services.

The HBGary e-mails don't indicate what information may have been stolen from Morgan Stanley's databanks or which of the world's largest merger adviser's multinational operations were targeted.

"They have given me access to a very sensitive report on their Aurora experience," Wallisch wrote in a May 10 e-mail to HBGary President Penny Leavy-Hoglund. "I will honor their wishes about not sharing the info with anyone, but the good news is that I have some great ideas for our final reports."

Sandra Hernandez, a spokeswoman for the New York-based bank, which unlike Google didn't disclose the attacks publicly, declined to comment on them specifically.

"Like any other company in our industry we deal with malware and attempted computer compromises as a matter of conducting business and work with law enforcement where appropriate," Hernandez said yesterday by phone.

FBI Deputy Assistant Director Steven Chabinsky said that hackers have increasingly targeted information related to mergers and acquisitions, data that can give companies involved an advantage in negotiations.

Google said in January 2010 after an attack lasting for months that it was one of 20 major U.S. companies breached by hackers using China-based servers, an event that McAfee Chief Technology Officer George Kurtz described as the "largest and most sophisticated cyberattack we have seen in years targeted at specific corporations."

U.S. diplomatic cables published by WikiLeaks and citing high-level Chinese sources later traced direction of the attack to the "Politburo Standing Committee level" of China's government.

Wang Baodong, a spokesman for the Chinese embassy in Washington, said cyber-hacking is an international issue and that many Chinese governmental websites have been attacked.

"China's stand on fighting hacking activities is clear and consistent, with relevant strict domestic laws and regulations in place, and is always ready to work with other countries to jointly strike down on hacking crimes," he said yesterday in an e-mail.

China's official news agency last year quoted an unidentified spokesman from the Ministry of Industry and Information Technology saying that accusations the government was behind the attacks were "groundless."

The attacks fueled escalating U.S.-China tensions and led to a call on China by Secretary of State Hillary Clinton to investigate Google's claims and make the results public.

The attacks also led Google to stop censoring search results generated by its Chinese search engine Google.cn. After months of negotiations with Chinese officials, Google began to shutter the site last March, redirecting users to the company's service in Hong Kong.

Google's share of revenue generated by the China search market fell to less than 20 percent in the fourth quarter of 2010 from 31 percent before the closure, according to Analysys International, a Beijing research firm. This month, China's official news agency launched its own Internet search site called Panguso that will conform to government-specified norms.

Dmitri Alperovitch, McAfee's vice president of threat research, said that the company believes the Aurora attacks were shut down by the hackers as Google began to uncover their activities near the end of 2009. The company announced on Jan. 12, 2010, that it had been a victim of an attack.

Kevin Mandia, chief executive officer of the cyber-security firm Mandiant, based in Alexandria, Virginia, said forensic investigations of the attacks showed that the hackers had penetrated various company networks over a period lasting more than a year and had hit some companies multiple times.

Day and Mandia, citing client confidentiality, didn't discuss the companies that were victims of the attack.

The HBGary e-mails were stolen from the firm's computer network by the group of hacker activists called Anonymous, which posted them on the Internet as a searchable database. HBGary confirmed the messages were stolen and declined last week to comment on their content.

Marc Zwillinger, an attorney for HBGary, didn't respond to a phone message seeking comment. Zwillinger has previously declined to comment on the HBGary e-mails' content, citing client confidentiality.

Morgan Stanley hired HBGary in 2010 to address suspected network breaches by hackers not linked to Operation Aurora who broke through the company's Internet security systems. The hackers successfully implanted software designed to steal confidential files and internal communications, according to dozens of HBGary e-mails that detail efforts to plug the holes.

One e-mail, dated June 19, said that the attackers may be the same ones who had hit a U.K.-based defense contractor and discusses hacking software called Monkif, which can be used by intruders to remotely orchestrate a sophisticated form of cyber attack known as an 'advanced persistent threat' or APT.

"This Monkif payload may represent APT or play a part in the APT's campaign," HBGary Chief Executive Officer Greg Hoglund wrote to Wallisch. "Phil, you might find this of value given that you are dealing with the same attack over at Morgan."