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: **SUNDAY, JUNE 12, 2011 7:15 AM EDT**

TODAY'S EDITION

[redacted]

[redacted]

IMF Investigates Suspected Attack On Its Computers (WP)

By Howard Schneider, Ellen Nakashima
Washington Post, June 12, 2011

The International Monetary Fund's computer system was invaded by hackers recently, a potentially sensitive breach of a system that analyzes confidential information about the finances of most of the world's economies.

The scope and significance of the cyberattack are still being evaluated, but it marks the third recent raid on a major government financial institution.

The attacks come at a time when world economic officials are debating possible changes to currency rules, developing new regulations for banks and financial institutions, and crafting guidelines for the management of the world's top economies — issues that make inside information extremely valuable to an investor or an interested government.

IMF officials provided few details about the cyberattack, which occurred as the agency is wrestling with complex and contentious financial rescue programs in several European nations that have required painful cuts in social spending. The organization is also pressing nations such as China to reform their financial and currency policies.

There was "an incident of intrusion into our IT system," IMF spokesman David Hawley said Saturday. "We are investigating, and the fund is fully functional."

The hack was "recently detected," Hawley said, but he would not discuss when the intrusion occurred, how long it lasted, or the nature or amount of data that might have been compromised.

A U.S. Treasury Department spokeswoman said there was no reason to believe that sensitive information about the U.S. economy was jeopardized. The FBI will help investigate the incident, the Reuters news service reported late Saturday, citing a Defense Department spokeswoman.

IMF employees were told of the potentially serious "phishing" attack, first reported in the New York Times, in a memo on Wednesday. Staff members were given "the usual reminders" about computer security, Hawley said.

An intranet that links the IMF with the nearby World Bank was temporarily disconnected, according to a bank official who said the step was taken "out of an abundance of caution," and that the link included only "nonpublic, nonsensitive" information that allowed the two agencies to continue coordinating their work.

Depending on the type of information involved, the potential for disruptions to international markets is significant. Ongoing bailout talks in Greece, for example, hinge on whether private holders of Greek bonds will be forced to accept losses before the IMF and other European nations lend any more money to the deeply indebted nation.

Documents that shed light on the IMF's position — or provide confidential information on the finances of Greece or other nations — could be used by traders to profit.

The hacker group Anonymous recently called for an attack on the IMF's computers "in opposition to the corrupt Austerity Plans of the Greek Government leaders and the International Monetary Fund." IMF officials this month said they were taking steps to guard against such an attack.

Hawley said fund investigators do not think the group was involved in this incident.

Computer security experts say the brazen acts of economic espionage highlight the difficulty of protecting networks at sensitive organizations such as the IMF despite heightened efforts to defend against the theft of information.

A pattern of cyber-espionage against key economic policymaking institutions has emerged in recent years, and some experts believe China has been involved.

"Attacks are often associated with decision-making related to issues such as Chinese exchange-rate policies or trade practices," said John Mallery, a cyber expert at the Massachusetts Institute of Technology.

Two years ago, sensitive data were taken from the computers of senior U.S. Treasury Department officials before a U.S.-China economic dialogue, said an expert with knowledge of the intrusion.

The incident — using a tactic known as "spear phishing" that targets specific employees — involved carefully forged documents or very sophisticated malicious software, or malware, e-mailed to Treasury officials from the computers of unsuspecting government employees, the expert said. Federal investigators believe that attack originated in China, the source said.

Investigators have linked other attacks to computers in China — servers that may have been operated by

Chinese officials or residents, or may have been way stations for hackers operating from elsewhere. Canada's Treasury Board and Finance Ministry were targeted in January, and France's Finance Ministry was hacked in December by someone hunting for files related to a February meeting of officials from the Group of 20 top economic powers.

James Mulvenon of the Defense Group Inc.'s Center for Intelligence Research and Analysis said cyber-espionage "is mature enough that they could use it to get near real-time intelligence." It is not against international law, Mulvenon said, and "you're never going to be able to enshrine in a treaty anything that restricts a country's right to commit espionage."

IMF Computers Lose E-Mails In State-Based Attack (BLOOM)

By Michael Riley

Bloomberg News, June 12, 2011

The International Monetary Fund's computer system was attacked by hackers believed to be connected to a foreign government, resulting in the loss of e-mails and other documents, according to a person familiar with the incident.

Data was taken in the attack, according to the person, a security expert who couldn't be identified because he wasn't authorized to speak on the subject. He didn't say which government is thought to be behind the incident, which he said occurred before former Managing Director Dominique Strauss-Kahn was arrested for sexual assault on May 14.

The infiltration follows reported hacks at Google Inc. (GOOG), Sony Corp. (6758), Lockheed Martin Corp. (LMT) and Citigroup Inc. (C) in the past three months. The FBI has said it would increase efforts to combat cyber attacks by criminal gangs, industrial spies and foreign governments. Yesterday, Spanish police arrested three suspected members of the online hacking group Anonymous, which has said it carried out attacks on governments and websites belonging to Sony and MasterCard Inc. (MA)

"The Fund is fully functional," David Hawley, an IMF spokesman, said today in an e-mailed statement. "We are investigating an incident. I am not in a position to elaborate further on the extent of the cyber-security incident."

The attack was reported earlier by the New York Times.

The Federal Bureau of Investigation had no immediate comment, nor did Charles Miller, a U.S. Justice Department spokesman. Phone calls and e-mails to the Department of Homeland Security and Central Intelligence Agency weren't immediately returned. Strauss-Kahn has pleaded not guilty and is free on bail in New York awaiting trial. The Washington-based IMF, which is seeking a replacement for Strauss-Kahn, approved a record $91.7 billion in emergency loans last year and provides a third of bailout packages in Europe.

Internal IMF memos obtained by Bloomberg warned employees to be on their guard after a computer at the fund was "compromised."

"Last week we detected some suspicious file transfers, and the subsequent investigation established that a Fund desktop computer had been compromised and used to access some Fund systems," said a June 8 e-mail to employees from Chief Information Officer Jonathan Palmer. "At this point, we have no reason to believe that any personal information was sought for fraud purposes."

World Bank Quarantined

The memo, which included advice on how to detect and report hacking attempts, said the IMF's network connection to the World Bank was severed "as a precautionary measure." The intrusion wasn't connected to an attack by Anonymous, the memo said.

On June 1, the IMF's information technology department sent an e-mail to employees with the subject line "Important Notice: Virus Attacks." It warned of attempts to hack into the system.

"Staff are strongly requested NOT TO OPEN emails and video links without authenticating the source," the e-mail said. The capitalization is in the original message.

The fund told employees June 8 that it would replace their RSA SecurID tokens. EMC Corp.'s RSA security-systems unit offered to swap the tokens after a breach of its own network, disclosed in March, resulted in the theft of RSA data. A SecurID device is shaped like a key fob or a computer-memory stick and generates random-number passwords used to gain access to a computer network.

'Phishing' Expedition

"Nothing indicates that the SecurID tokens played a role in this intrusion," according to the IMF memo.

A June 9 e-mail from Palmer warned employees of "increased phishing activity." Phishing is the practice of obtaining information such as computer user names or passwords under false pretenses. Palmer's message included further instructions on how to detect and respond to cyber-attackers, warning employees not to divulge their passwords or open "unexpected documents."

"Exercise caution to protect yourself from cyber sharks!" Palmer wrote.

[redacted]