

IMF cyber attack aimed to steal insider info-expert

Sun Jun 12, 2011 2:22pm BST

By [Jim Wolf](#) and [William Maclean](#)

WASHINGTON/LONDON, June 12 (Reuters) - A major cyber attack on the IMF aimed to steal sensitive insider information, a cyber security expert said on Sunday, as the race to lead the body which oversees global financial system heated up.

The U.S. Federal Bureau of Investigation is helping to investigate the attack on the International Monetary Fund, the latest in a rash of cyber break-ins that have targeted high-profile companies and institutions.

"The IMF attack was clearly designed to infiltrate the IMF with the intention of gaining sensitive 'insider privileged information'," cyber security specialist Mohan Koo, who is also Managing Director, Dtex Systems (UK), told Reuters in London.

A June 8 internal memo from Chief Information Officer Jonathan Palmer told staff the Fund had detected suspicious file transfers and that an investigation had shown a desktop computer "had been compromised and used to access some Fund systems".

"At this point, we have no reason to believe that any personal information was sought for fraud purposes," it said.

The New York Times cited computer experts as saying the IMF's board of directors was told of the attack on Wednesday, though the assault had lasted several months.

The IMF says it remains "fully functional" but has declined to comment on the extent of the attack or the nature of the intruders' goal.

News of the hack came at a sensitive time for the world lender of last resort, which is seeking to replace former managing director Dominique Strauss-Kahn, who quit last month after being charged with the attempted rape of a hotel maid.

French Finance Minister Christine Lagarde remains the frontrunner to replace him, although Stanley Fischer, the Bank of Israel Governor and a former IMF deputy chief, has emerged as a late candidate, and Mexico's central bank chief, Agustin Carstens, is another contender.

[ID:nL3E7HC039]

EMBOLDENED

Jeff Moss, a self-described computer hacker and member of the Department of Homeland Security Advisory Committee, said he believed the attack was conducted on behalf of a nation-state looking to either steal sensitive information about key IMF strategies or embarrass the organization to undermine its clout.

He said it could inspire attacks on other large institutions. "If they can't catch them, I'm afraid it might embolden others to try," said Moss, who is chief security officer for ICANN.

Tom Kellerman, a cybersecurity expert who has worked for both the IMF and the World Bank, said the intruders had aimed to install software that would give a nation state a "digital insider presence" on the IMF network.

That could yield a trove of non-public economic data used by the Fund to promote exchange rate stability, support balanced international trade and provide resources to remedy members' balance-of-payments crises.

"It was a targeted attack," said Kellerman, who serves on the board of a group known as the International Cyber Security Protection Alliance.

The code used in the IMF incident was developed specifically for the attack on the institution, said Kellerman, formerly responsible for cyber-intelligence within the World Bank's treasury team and now chief technology officer at AirPatrol, a cyber consultancy.

"LIFE-THREATENING"

Koo of Dtex Systems (UK) said the recent spate of attacks on large global organisations was worrying because they were targeted, well-organised and well-executed, not opportunistic.

"Perhaps most frightening of all is the fact that these type of attacks could quite easily be directed towards Critical National Infrastructure (CNI) organisations, for example Energy and Water, where the impact of such a breach would have severe, immediate and potentially life-threatening consequences for everyday citizens."

Cyber security experts said it might be difficult for investigators to prove which nation was behind the attack.

"Even developing nations are able to leverage the Internet in order to change their standing and ability to influence," said Jeffrey Carr, author of the book, "Inside Cyber Warfare".

"It's something they never could have done before without gold or without military might," Carr said.

CIA Director Leon Panetta told the U.S. Congress on June 9 that the United States faced the "real possibility" of a crippling cyber attack on power systems, the electricity grid, security, financial and governmental systems.

Lockheed Martin Corp, the Pentagon's No. 1 supplier by sales and the biggest information technology provider to the U.S. government, disclosed two weeks ago that it had thwarted a "significant" cyber attack. It said it had become a "frequent target of adversaries around the world".

Also hit recently have been Citigroup Inc, Sony Corp and Google Inc. (Reporting by [Lesley Wroughton](#), [Jim Finkle](#), Jim Wolf, Jim Vicini and William Maclean in London; Editing by [Jon Boyle](#))