

Presidential Hacks

Cyber Threat Condition



- 1 Low Risk—normal operations
- 2 Limited Risk—caution required
- 3 Moderate Risk—guarded operations
- 4 Increase Risk—increased vigilance
- 5 High Risk—take immediate action

INTEL: The FBI and U.S. Secret Service contacted both presidential campaigns to discuss hacking by foreign powers into their computer systems.

INTEL: Obama's team concluded on its own that the hackers were Russian or Chinese.

INTEL: Official sources say that there was no evidence either campaign had hacked the other.

INTEL: There is no doubt that foreign governments are actively targeting cyber space for sensitive U.S. information.

Also published on the DefenseTech.Org Cyber Warfare Blog.

The Technolytics Institute

4017 Washington Road
Mail Stop # 348
McMurray, PA 15317
P 888-650-0800
F 412-291-1193
I www.technolytics.com
E info@technolytics.com

Multiple sources are reporting that hackers have penetrated the email system of the White House. People described as "US government cyber experts" are said to suspect the cyber raids were sponsored by the Chinese regime. These sophisticated, targeted attacks repeatedly penetrated the unclassified network's defenses. The breaches seem to closely follow the "Grain of Sands" technique used by Chinese intelligence agencies. The "Grain of Sands" is a methodology used to derive intelligence from disparate pieces of data no matter how seemingly trivial, as each data point might just be the final little piece that completes the puzzle. It is important to note that inside sources tell us that the classified network and system was NOT compromised. This comes just days after Newsweek reported that both the Obama and McCain campaigns had their security breached by overseas hackers. Reportedly a significant amount of data had been exfiltrated. Intelligence Analysts at Spy-Ops believe that the hacks and data transfers were a concerted effort to track the candidates' policy positions which could aid in future negotiations with the United States. The FBI and U.S. Secret Service had notified both campaigns of the security breach in late August. At first, the campaign security thought it was just another "phishing" attack, using common methods. One source said the FBI told them "You have a problem way bigger than what you understand. You have been compromised, and a serious amount of files have been loaded off your system." Unofficial sources tell us that the attacks were traced back to Russia, China and an un-named third country.



This is at least cyber espionage or is it an act of cyber war? Are we at Cyber DefCom 1? A cyber warfare doctrine is needed to answer these questions.