US gives detailed look at Russia's alleged election hacking

December 30 2016, by Tami Abdollah

The U.S. has released its most detailed report yet on accusations that Russia interfered in the U.S. presidential election by hacking American political sites and email accounts.

The 13-page joint analysis by the Department of Homeland Security and the FBI is the first such report ever to attribute malicious cyber activity to a particular country or actors.

It was also the first time the U.S. has officially and specifically tied intrusions into the Democratic National Committee to hackers with the Russian civilian and military intelligence services, the FSB and GRU, expanding on an Oct. 7 accusation by the Obama administration.

The report said the intelligence services were involved in "an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens." It added, "In some cases, (the Russian intelligence services') actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack."

Over the summer stolen emails from Democrats were posted by an online persona known as Guccifer 2.0, believed by U.S. officials to be linked to Russia. Outrage over documents that appeared to show favoritism for Hillary Clinton forced the DNC's chair, Debbie Wasserman Schultz, to resign.

The U.S. released the technical report Thursday as President Barack Obama sanctioned the GRU and the FSB, the GRU's leadership and companies which the U.S. said support the GRU.

The sanctions were the administration's first use of a 2015 executive order for combatting cyberattacks against critical infrastructure and commercial espionage. Because election systems aren't considered critical infrastructure, Obama amended the order Thursday to allow for sanctions on entities "interfering with or undermining election processes or institutions."

The retaliation against Russia, just weeks before President-elect Donald Trump takes office, culminated months of political handwringing about how and whether to respond to Moscow's alleged meddling. U.S. intelligence agencies concluded that Russia's goal was to help Trump win—an assessment Trump has dismissed as ridiculous. Trump said Thursday the U.S. should move on, but that he would meet with the intelligence community's leaders next week for an update on the situation.

The report did not go far beyond confirming details already disclosed by cybersecurity firm CrowdStrike, which was hired to investigate the DNC hacks.

It described the intelligence services' use of "spearphishing"—fake emails intended to trick victims into typing in their user names and passwords. At least one person opened attachments with malicious software. The report noted that actors "likely associated" with Russian intelligence services are continuing to engage in spearphishing campaigns, including one launched just days after the U.S. election.

The DNC was infiltrated by the FSB in summer 2015 and again by the GRU in spring 2016 using spearphishing emails that often appeared to

come from legitimate or official organizations, the report said.

Russian officials have denied any involvement in hacking U.S. political sites and emails.

The report provided clues, or pieces of code left behind by hackers, cybersecurity workers in the private sector could look for to identify compromised systems and prevent more intrusions. The Department of Homeland Security said it has already included this information within its own cyber threat information-sharing program, which automatically flags threats in real time for participating companies and agencies.

Releasing such a report was a political twist on the administration's strategy of "name and shame," in place since 2012 and used to bring indictments against Chinese military hackers for economic espionage and Iranian hackers for an attack on banks and a small dam in New York. It was also a far more detailed and sophisticated telling of Russia's hacking, with technical indicators of compromise, compared to the spare technical details released after the Obama administration publicly blamed North Korea for a cyberattack against Sony Pictures Entertainment.

U.S. officials also provided antivirus vendors with two malicious software samples used by Russian intelligence services.

© 2016 The Associated Press. All rights reserved.

Citation: US gives detailed look at Russia's alleged election hacking (2016, December 30) retrieved 22 April 2024 from https://phys.org/news/2016-12-russia-alleged-election-hacking.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.