Written by **C. Mitchell Shaw** on November 3, 2014

Russian Hacking Threatens U.S. National Security

The recent intrusion into a computer network at the White House, made public last week, appears to have been carried out by hackers working for the Russian government. While officials are saying that the affected network does not contain classified documents, it is still a major security breach. Hackers often test the vulnerability of less secure networks on a system to gain a better understanding of the types of security measures in place before moving on to the more secure networks in that system. With the information they gain — including usernames and passwords — they can begin attacking the more secure networks.

In the case of the White House, that would mean networks containing classified documents. According to the *Washington Post*, officials at the White House are claiming "there is no evidence the classified network was hacked." They also say they have taken action to "mitigate the activity." Though they would not comment on the duration of the attack, it appears it was for at least days, possibly longer.

One of the most disturbing elements in this case is that the hacking was not even discovered by the White House. The *Washington Post* reports that an "ally" made U.S. officials aware of it. There was no information on who the ally was or how it knew of the hacking. It is ironic that the U.S. government was oblivious to a hacker breaking into its computers considering how intent it is in breaking into the computers of others.

Senator Tom Coburn (R-Okla.), who is on the Senate Homeland Security Committee, is upset that Congress was not made aware of the cyber attack sooner. He says he has "yet to receive satisfactory answers" to his questions about "how the attack succeeded."

This is not an isolated incident. Over the past several years Russia has been responsible for multiple, sustained attacks on computer systems belonging to governments and security firms with government contracts, according to a report by FireEye Inc. From the *Wall Street Journal*, "The report is one of four recent assessments by cybersecurity companies, buttressed by reports from Google Inc. and U.S. intelligence agencies, pointing to Russian sponsorship of a skilled hacking campaign dating back to 2007. Targets included NATO, governments of Russia's neighbors, and U.S. defense contractors Science Applications International Corp. and Academi LLC, the U.S. security firm previously known as Blackwater." FireEye has dubbed the cyber-weapon used by the Russians "APT28."

FireEye's report came after the firm was called in to investigate a breach of a computer network at an unnamed company with U.S. government contracts. Those networks contained classified military documents. The investigators determined that the hack was of Russian origin, based on the Russian language found in the code and the fact that time stamps were during working hours in Moscow. The extreme sophistication of the tools used in the attack caused them to determine it was government sponsored.

How did the hackers get into these highly protected systems in the first place? It appears they used the same tactic on the White House that they have used in the past: an attack known as "Spear Phishing."

Phishing is a type of attack that uses e-mails and fake Internet addresses to gain information about an individual or group. An example would be an e-mail offering a service or product people may be interested in and including a link that purports to belong to a site selling the service or product. The link may contain a virus that invades the computer that accesses the link and harvests information from it, or it may ask for information to "confirm" your username, password, or credit card.

Spear Phishing goes beyond this, in that it is much more targeted in its approach. The hacker already has some information about the targeted person or group. This information is used to make the e-mail look like it's from a friend or colleague and is about something that's already been discussed. Whereas most people know better than to click a link in a spam e-mail, a Spear Phishing attack doesn't look like spam and has a much greater chance of getting past a person's defenses. White House officials said they have had employees change their passwords, indicating that this was a likely point of entry for the attack.

While a great deal of the recent media coverage of state-sponsored hacking has focused on China, Russia appears to be a much more serious threat. The digital weapons that have been developed are extremely sophisticated and difficult to detect. Once the hackers have penetrated a system, these tools are able to move around in the network (even to computers not connected to the Internet) and harvest data. That data is then encrypted and disguised as normal e-mail and sent back to the hackers. The software then cleans up behind itself and moves on to its next task.

The types of information Russia is targeting would give it a military advantage in the case of conflict. The FireEye report states, "since at least 2007, APT28 has been targeting insider information related to governments, militaries, and security organisations that would likely benefit the Russian government." It's much like the old strategy of football teams trying to get their hands on a rival's play-book. If Russia knows the strengths and weaknesses of other nations, it would be in a better position to act agressively.

Of course this is nothing new; governments have spied on each other for as long as there have been governments. What is new is the ability to do it remotely and with such precision and so little risk, bringing about a type of Digital Cold War. The United States has been the big player in cyber-spying for many years, using advanced programs such as PRISM and BOUNDLESSINFORMANT to scoop up data from all over the world, including that of foreign governments. Now that Russia is stepping up its ability to hack into U.S. government computers, it may eventually gain access to much of the data that the NSA and other agencies have collected. This is a good reason — among others — to put a stop to the NSA's surveillance of Americans.