Written by **C. Mitchell Shaw** on November 10, 2014

Russian "Trojan Horse" Discovered in Vital U.S. Computers

The Russian government-sponsored hacking of computer systems in the White House, reported last week, seems to be only the tip of the iceberg. *ABC News* has now reported that more computer systems have not only been hacked, but have been infected with a complex Trojan Horse malware program, dubbed "BlackEnergy." This is the same type of virus Russia used earlier this year to attack computer networks belonging to NATO. The infected systems here in the United States are government and industry networks that control vital parts of the nation's infrastructure, including "complex industrial operations like oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines and even some nuclear plants."

BlackEnergy would allow Russia to shut down or destroy these vital systems, creating chaos and causing untold damage to not only our infrastructure, but also our economy. There is the danger of a cyberattack that could threaten human life. The virus is able to be activated remotely, using a computer or mobile device, according to sources in the Department of Homeland Security. DHS ran a test of this type of software and succeeded in causing a power generator to self-destruct. If used to shut down or modify the operations of water systems used to cool nuclear reactors, BlackEnergy could cause such reactors to flood or overheat, possibly resulting in a meltdown of the reactors. Coupled with attacks on the power grid and oil and gas pipelines, the effect would be truly catastrophic.

It appears the same tactic of "Spear Phishing" that was used in previous attacks on U.S. computers, including those at the White House, was used to attack these systems. Spear Phishing is an attack using spam e-mail that is targeted and does not look like spam because it is disguised to look like it is from someone you know. Once the e-mail is opened, the virus installs itself and begins to infiltrate the network and any computer that accesses the network.

One of the most concerning parts of this infiltration of computer systems is that it has been in place since 2011, according to a bulletin issued by the DHS Industrial Control Systems Cyber Emergency Response Team. It was only discovered last week, presumably in conjunction with "an ally" alerting the United States to the hacking of White House computer systems. As the War on Terror continues to move more and more in the direction of mass surveillance of American citizens' everyday life, it appears that not enough is being done to protect our own computers.

So far, the virus has not been used to "damage, modify, or otherwise disrupt" any of the infected systems, instead sitting dormant and, until last week, undetected. Government officials do not know

when it could be activated, creating a situation similar to the "Mutually Assured Destruction" model of nuclear warfare — if you fire at us, we'll fire at you. The new Digital Cold War seems to be under way. Darien Kindlund, director of threat research at FireEye Inc, was quoted by *The Hill* as saying, "It's this slow warming of the water, where you don't know you're being boiled alive because it's so slow." FireEye is the cyberinvestigation firm that issued the report tying the Russian government to several high-level hacking incidents over the past several years. Kindlund said, "The main issue," is that it was "undetected for so long."