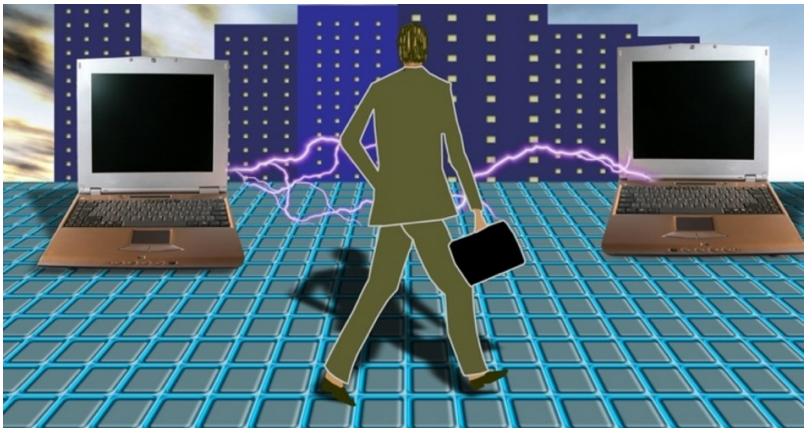
Written by **Bob Adelmann** on July 2, 2014

Russian Malware Infecting U.S. Energy Grid



An alert from software giant Symantec on Monday announced an "ongoing campaign" by Russia-based cyber-terrorists who have changed their focus from espionage to sabotage. Their primary targets are energy companies using oil and natural gas to provide electrical power to the national grid.

The infections are so powerful that not only can they disrupt internal messaging and controls but they can also disrupt the operations of the physical power plants and pipelines, according to Symantec:

> An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims.
>
> The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and … could have caused damage or disruption to energy supplies in [the] affected countries.

The attacks emanating from Russia target not only the United States but Spain, France, Italy, Germany, Turkey, and Poland, but they are focused primarily on the United States and Spain.

Symantec said that Dragonfly is no small group of weekend hackers, either: "The Dragonfly group is technically adept and able to think strategically … the group found a "soft underbelly" … invariably smaller, less protected companies."

According to Symantec, this is a government-sponsored operation: "The Dragonfly group is well-resourced with a range of malware tools at its disposal and is capable of launching attacks through a number of different [malware protocols]."

Eric Chien, the chief researcher for Symantec, is frightened over the implications of its discoveries: "When they do have that type of access, that motivation wouldn't be [just] for espionage. When we look at where they're at, we're very concerned about sabotage."

Dragonfly has already had success in infecting "industrial control systems" (ICS) equipment providers by using "software with a remote access type Trojan." Once installed, the software handed off control of physical plant operations to the saboteurs in Russia:

> [The Trojan] caused companies to install the malware when downloading software updates [to their] computers running ICS equipment.
>
> These infections not only gave the attackers a beachhead in the targeted organizations' networks but also gave them the means to mount sabotage operations.

In trying to decipher the attacks for laymen reading their chilling report, it compared the Trojan malware to Stuxnet, the computer worm that targeted Iran's nuclear power plant's fast-spinning centrifuges. It resulted in nearly one-fifth of Iran's nuclear centrifuges spinning out of control, destroying themselves as a result. The big difference is that Stuxnet was focused on a very narrow

target, while the latest expansion now targets entire power grids across the country and around the world.

Explained Symantec: "Dragonfly appears to have a much broader focus, with espionage … as its current objective with sabotage as an optional capability."

Dragonfly is Symantec's name for the operating group behind the attacks, while other observers call it the "Energetic Bear." Its existence has been known and tracked since at least 2011, said Symantec, and its initial targets were defense and aviation companies in the United States and Canada. But it shifted its focus to the more vulnerable energy sector in the United States in early 2013.

While using arcane language in its customer alert such as "back doors" and "watering holes" — terms familiar only to computer techies and their managers — Symantec identified seven different companies targeted by the group, one of whom downloaded the infected software to 250 of its unsuspecting customers.

> Symantec is not the first to discover the group masterminding the attacks, nor the first to pin the blame on government-sponsored groups in Russia. Stuart Poole-Robb, a former MI6 (British Secret Intelligence Service) agent and founder of a security consulting firm, said:
>
> To target a whole sector like this at the level they are doing … speaks of some form of government sanction.

These are people working with FAPSI [Russia's Spetssvyaz intelligence service], working to support mother Russia.

CrowdStrike, a California company engaged in exposing Internet adversaries, has been tracking Dragonfly for years, and in its January update, it noted that "Energetic Bear [synonymous with Dragonfly] is an adversary group with a nexus to the Russian Federation that conducts intelligence collection operations against a variety of global [targets] with a primary focus on the energy sector."

Symantec offers Internet security software and consulting services to help companies protect themselves from such attacks but the U.S. government has also been very busy as well. Recognizing the potential disaster inherent in such potential attacks, which could destroy the energy infrastructure of the country, the United States Cyber Command was established as a part of the United States Strategic Command in 2009 in Fort Meade, Maryland. Its mission is: "To conduct full spectrum military cyberspace operations in order to … ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."

This is being matched by similar cyber warfare units in South Korea and Great Britain.

Neither Symantec nor Crowdstrike offered any scenarios of the possible impact such attacks might have on the United States, but fiction writers such as James Wesley Rawles (author of *Survivors*) and William Forstchen (author of *One Second After*) have carefully crafted believable scenarios following successful attacks on America's power grid. In *One Second After*, after an electromagnetic pulse shuts down the electric grid, no electronic appliances work, and citizens are largely forced to live an 18th-century life — hunger and die offs of people begin quickly when food storage is compromised.

What is clear from Symantec's warning to its customers, however, is that Russia is no friend of the United States. It fully intends to extend its present advantage through its "well-resourced" efforts to gain control of America's electric power grid, while the U.S. government and private companies such as Symantec are playing catchup ball to keep that from happening.

A graduate of Cornell University and a former investment advisor, Bob is a regular contributor to The New American *magazine and blogs frequently at www.LightFromTheRight.com, primarily on economics and politics. He can be reached at badelmann@thenewamerican.com.*