IS RUSSIA REALLY LAUNCHING CYBER ATTACKS ON THE US GRID?

The Trump administration has blamed the Russian government for a campaign of cyber attacks on its power grid stretching back at least two years.

It marks the first time the US has publicly accused Moscow of hacking into American energy infrastructure.

Beginning in March 2016, or possibly earlier, Russian government hackers attacked multiple critical infrastructure sectors, according to a US security alert.

These sectors included energy, nuclear, commercial facilities, water, aviation and manufacturing.

The Department of Homeland Security and the FBI said in the alert that a 'multi-stage intrusion campaign by Russian government cyber actors' had targeted the networks of small commercial facilities 'where they staged malware, conducted spear phishing, and gained remote access into energy sector networks.'

The alert did not name facilities or companies targeted.

The US Treasury Department has decided to impose sanctions on 19 Russian people and

five groups, including Moscow's intelligence services, for meddling in the 2016 US presidential election and other malicious cyber attacks.

Russia in the past has denied it has tried to hack into other countries' infrastructure, and vowed on Thursday to retaliate for the new sanctions.

The direct condemnation of Moscow represented an escalation in the Trump administration's attempts to deter Russia's aggression in cyberspace.

Senior US intelligence officials said in recent weeks the Kremlin believes it can launch hacking operations against the West with impunity.

US security officials have long warned that the United States may be vulnerable to debilitating cyber attacks from hostile adversaries.

It was not clear what impact the attacks had on the firms that were targeted.

But the alert provided a link to an analysis by the US cyber security firm Symantec last October that referred to a group it had dubbed Dragonfly.

The collective had targeted energy companies in the United States and Europe and in some cases broke into the core systems that control the companies' operations.

Russian threat to UK's National Grid

In the United Kingdom, National Cyber Security Centre officials have also issued advice to the likes of the Sellafield nuclear plant, Whitehall departments and NHS trusts over possible action from Vladimir Putin's government.

This after the Kremlin announced expulsions of British diplomats in response to Theresa May's decision expel 23 Russian embassy staff.

Ciaran Martin, head of the NCSC, warned in January of the risk of a 'category one' Russian cyber attack on the UK, which would involve "disruption of critical systems".

The NCSC's director of operations, Paul Chichester, told the Sunday Times: "It is absolutely right that we give advice to sectors on defending themselves from cyber-attacks.

"We are vigilant to cyber-threats wherever they come from and are ready to defend against them."

> *In the newspapers' recently, there has been a lot of focus on the Trump government's warning about possible attacks on utilities by Russia.*

To get more information on the cyber landscape, Metering & Smart Energy International spoke with Ilan Barda, CEO of Radiflow, a provider of cyber security solutions for critical infrastructure networks (i.e. SCADA), such as power utilities, oil and gas, water and others.

In the newspapers' recently, there has been a lot of focus on the Trump government's warning about possible attacks on utilities by Russia. How likely is an attack on utilities in either the US or Europe?

It is important that we differentiate between local initiatives with criminal or malicious intentions, such as hackers looking for financial gains or simply for the challenge or disgruntled employees and subcontractors, and government-sponsored attacks, which can also include terrorist organizations. Attacks from the first type are likely to increase and happen more frequently and, as a result, every utility should be prepared for such attacks.

Attacks from the second type are likely to be triggered only during situations of hostility between countries or political turmoil. However these types of attacks often involve earlier information and intelligence gathering as well as attempts to test new cyberattack tools. For both situations, it is important that a utility has industrial grade monitoring tools in place to detect such attacks at an early stage and improve its overall defence posture.

What form do you believe this kind of attack would take and to what extent could it disrupt business?

The local initiatives are likely to leverage IT attack methods in operational technology environments like the recent cryptojacking malware incident that we recently uncovered. Government-sponsored attacks as well as attacks coming from terrorist organizations are likely to be more sophisticated, including targeted use of new vulnerabilities on industrial devices, supply chain weaknesses and even a combination of physical and cyberattacks. Government-sponsored attacks are likely, for now, to be used for information and intelligence gathering and testing rather than actual damage, but still can cause damage, even if unintentionally.

Do you believe that a government is the likeliest candidate to attempt such an attack, or it is more likely to be an attack motivated by the desire to hold a utility to ransom ie: ransomware?

I believe that smaller municipal utilities and private energy suppliers are more susceptible to ransomware, cryptojacking and similar attacks. The larger utility providers are certainly more likely to be targeted by government-sponsored attacks and terrorist organizations.

What best practises do you suggest utilities undertake to ensure they are being as security aware as they can, without creating unwarranted panic?

The first step is to perform a security assessment to map the vulnerabilities and prioritise the identified risks. The second step is to build an implementation plan that will cover not just devices, but also manpower and procedures. Such a plan should be implemented in a gradual and realistic way in terms of budget, timeline and resources so it will not impact the ongoing operations and ensure an effective outcome.

We have already seen attacks on utilities using a variety of methods - ransomware, cryptojacking, trojans, phishing, supply chain and more. It must be assumed that the attackers have access to state-of-the-art technology and are using sophisticated methods. As such, utilities companies of all sizes need to be prepared in order to remain one step ahead of potential attackers.

In addition to utilities designing a strong cybersecurity infrastructure, information sharing is an important element that needs to be facilitated by governments and should involve both the utilities and the vendors. MI

For more information, please visit **www.radiflow.com** and follow the company on LinkedIn.