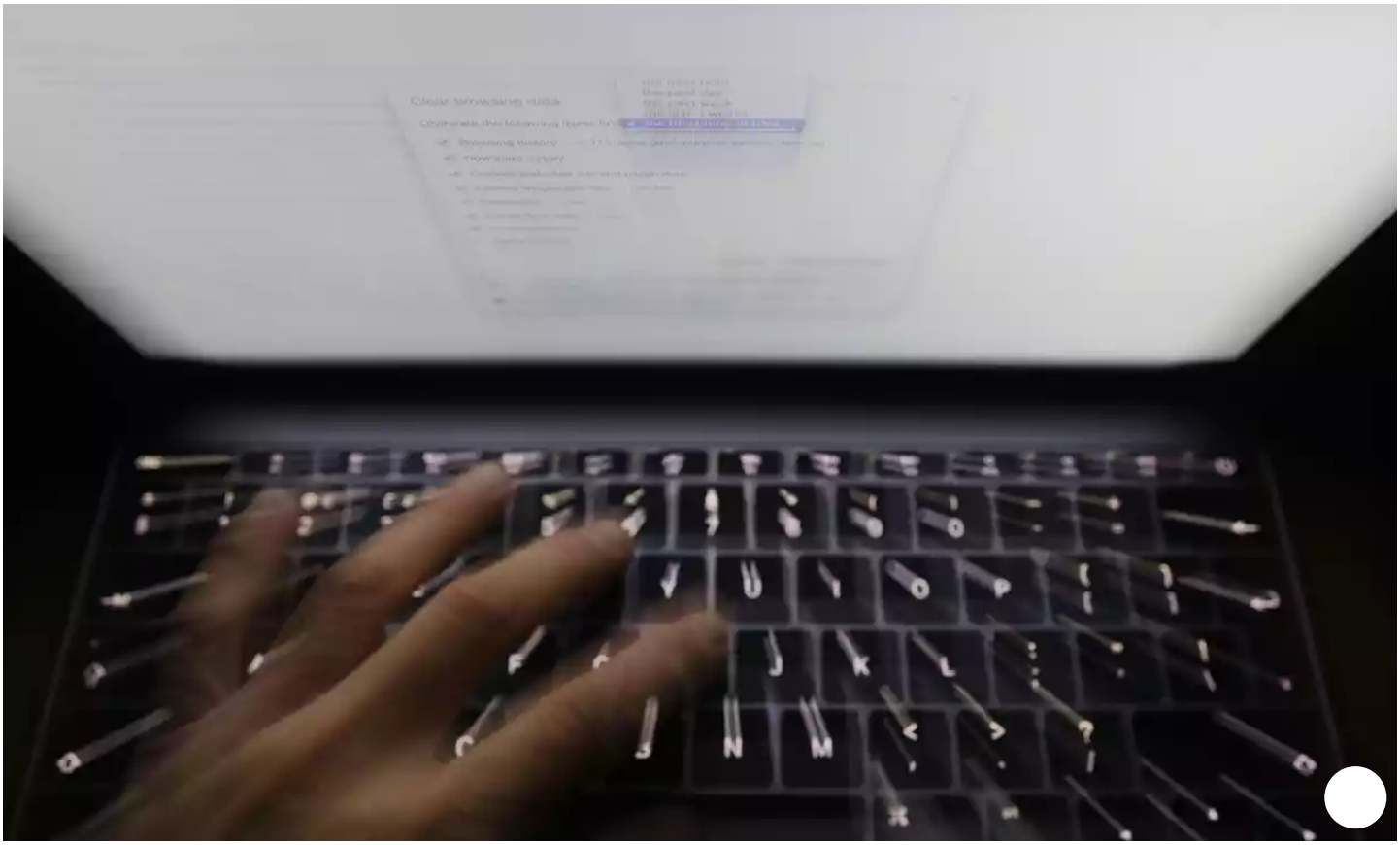
The Guardian



US and UK blame Russia for 'malicious' cyber-offensive

Security officials issue alert directly blaming Kremlin for attack as US warns Moscow it is 'pushing back hard'

Ewen MacAskill *Defence correspondent*

Mon 16 Apr 2018 19.23 BST

The cyberwar between the west and Russia has escalated after the UK and the US issued a joint alert accusing Moscow of mounting a "malicious" internet offensive that appeared to be aimed at espionage, stealing intellectual property and laying the foundation for an attack on infrastructure.

Senior security officials in the US and UK held a rare joint conference call to directly blame the Kremlin for targeting government institutions, private sector organisations and infrastructure, and internet providers supporting these sectors.

Rob Joyce, the White House cybersecurity coordinator, set out a range of actions the US could take such as fresh sanctions and indictments as well as retaliating with its own cyber-offensive capabilities. "We are pushing back and we are pushing back hard," he said.

Joyce stressed the offensive could not be linked to Friday's raid on Syria. It was not retaliation for the US, UK and French attack as the US and UK had been investigating the cyber-offensive for months. Nor, he said, should the decision to make public the cyber-attack be seen as a response to events in Syria.

Joyce was joined in the call by representatives from the FBI, the US Department of Homeland Security and the UK's National Cyber Security Centre (NCSC), which is part of the surveillance agency GCHQ.

The US and UK, in a joint statement, said the cyber-attack was aimed not just at the UK and US but globally. "Specifically, these cyber-exploits were directed at network infrastructure devices worldwide such as routers, switches, firewalls, network intrusion detection system," it said.

"Russian state-sponsored actors are using compromised routers to conduct spoofing 'man-in-the-middle' attacks to support espionage, extract intellectual property, maintain persistent access to victim networks and potentially lay a foundation for future offensive operations.

"The current state of US and UK network devices, coupled with a Russian government campaign to exploit these devices, threatens our respective safety, security, and economic wellbeing."

The US has given the cyber activity alleged to be from Russia the name GRiZZLY STEP.

The US and UK have previously blamed Russia for cyber-attacks such as crippling attacks last year that created disruption worldwide, including to the National Health Service, and for a cyber-intrusion into the US energy grid.

But they portrayed this as far more serious because of the potential to undermine infrastructure. Millions of machines had been targeted in a "sustained" campaign and the US and UK admitted they still did not know the full extent to which the system had been compromised.

Previously the two nations have spoken only of attacks "originating from Russia", with lines between Russian criminals and state activity being blurred, but they pinned blame on the Kremlin on this occasion.

The US and UK said they had "high confidence" that the Kremlin was behind the attack.

It is the first time they have issued joint advice to all sectors that might have been compromised, offering steps to to identify and neutralise potential problems relating to the attacks.

Ciaran Martin, the chief executive of the NCSC, which works closely with the surveillance agency GCHQ, said: "This is a very significant moment as we hold Russia to account."

Howard Marshall, who works in the FBI's cyber-division and who was on the conference call, said: "We will bring every tool to bear against them in every corner of cyberspace."

The decision of the US and UK governments to go public reflects a loss of patience with Moscow after a series of cyber-attacks and hacks allegedly originating from within Russia. It could also be born out of frustration over Russia's supposed interference in democratic elections in the US and Europe, its support for Syria's Bashar al-Assad and incidents such as the use of a nerve agent in Salisbury.

Both the US and UK, like Russia, have cyber-offensive capabilities. The head of GCHQ, Jeremy Fleming, in his first public speech last week, described how such a capability was used to degrade Islamic State's ability to disseminate propaganda from its Syrian headquarters in Raqqa. It was the first time that UK has admitted to having used its cyber-offensive capability.

Since you're here ...

... we have a small favour to ask. More people are reading the Guardian than ever but advertising revenues across the media are falling fast. And unlike many news organisations, we haven't put up a paywall - we want to keep our journalism as open as we can. So you can see why we need to ask for your help. The Guardian's independent, investigative journalism takes a lot of time, money and hard work to produce. But we do it because we believe our perspective matters - because it might well be your perspective, too.

I appreciate there not being a paywall: it is more democratic for the media to be available for all and not a commodity to be purchased by a few. I'm happy to make a contribution so others with less means still have access to information. *Thomasine, Sweden*

If everyone who reads our reporting, who likes it, helps fund it, our future would be much more secure. **For as little as £1, you can support the Guardian - and it only takes a minute. Thank you.**

Support The Guardian

Topics

- Cyberwar
- Russia
- Foreign policy
- GCHQ
- Hacking
- Espionage