Joint US – UK statement on malicious cyber activity carried out by Russian government

The NCSC, FBI and DHS have issued a joint Technical Alert about malicious cyber activity carried out by the Russian Government.

Today, the U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the UK's National Cyber Security Centre (NCSC) released a joint Technical Alert about malicious cyber activity carried out by the Russian Government.

The targets of this malicious cyber activity are primarily government and private-sector organisations, critical infrastructure providers, and the internet service providers (ISPs) supporting these sectors.

Specifically, these cyber exploits are directed at network infrastructure devices worldwide such as routers, switches, firewalls, and the Network Intrusion Detection System (NIDS).

Network device vendors, ISPs, public sector organisations, private sector corporations and small-office/home-office customers should read the alert (TA18-106A) and act on the recommended mitigation strategies. The alert contains indicators of compromise, technical details on the tactics, techniques and procedures (TTPs), and contextual information regarding observed behaviors on the networks of compromised victims.

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. Multiple sources, including private and public-sector cyber security research organisations and allies, have reported this activity to the U.S. and UK governments.

Jeanette Manfra, National Protection and Programs Directorate (NPPD) Assistant Secretary for Cybersecurity and Communications said:

> "Russian government activities continue to threaten our respective safety, security, and the very integrity of our cyber ecosystem. We condemn this

latest activity in the strongest possible terms and we will not accept nor tolerate any malign foreign cyber operations, intrusions, or compromises — to include influence operations. We call on all responsible nations to use their resources—including diplomatic, law enforcement, technical, and other means—to address the Russian cyber threat.

"Through information sharing programs like Automated Indicator Sharing (AIS), we are building the capacity for collective defense to minimize threats between U.S. and UK network devices. While DHS cannot protect every network at all times, we can ensure that we are all collectively empowered to secure our networks through government and industry working together.

"Cyber security is a shared responsibility, and we understand that identifying a threat in one organisation's network can prevent an attack in another. Today's joint Technical Alert is an example of how we are working with allies and partners to prevent cyber actors from impacting critical infrastructure to the fullest extent possible. Although this is the first time the NCSC is included as an author in a DHS and FBI joint product, our collaborative work has proved useful and effective in response to previous cyber related events. I look forward to continuing this important partnership as we work against these threats."

Howard Marshall, FBI Deputy Assistant Director said:

"The activity highlighted today is part of a repeated pattern of disruptive and harmful malicious cyber action carried out by the Russian government.

"As long as this type of activity continues, the FBI will be there to investigate, identify and unmask the perpetrators, in this case, the Russian government. The joint Technical Alert released today underscores our commitment to working with our partners, both at home and abroad, to combat malicious cyber activity and hold those responsible accountable. We do not make this attribution lightly and will hold steadfast with our partners."

Ciaran Martin, CEO of the National Cyber Security Centre said:

"Russia is our most capable hostile adversary in cyberspace so tackling them is a major priority for the National Cyber Security Centre and our U.S. allies. This is the first time that in attributing a cyber attack to Russia the U.S.

> and the UK have, at the same time, issued joint advice to industry about how to manage the risks from the attack. It marks an important step in our fight back against state-sponsored aggression in cyberspace.
>
> "For over twenty years, GCHQ has been tracking the key Russian cyber attack groups and today's joint UK-U.S. alert shows that the threat has not gone away. The UK government will continue to work with the U.S., other international allies and industry partners to expose Russia's unacceptable cyber behaviour, so they are held accountable for their actions.
>
> "Many of the techniques used by Russia exploit basic weaknesses in network systems. The NCSC is leading the way globally to automate defences at scale to take away some of those basic attacks, thereby allowing us to focus on the most potent threats."

Anyone who finds signs of the malicious activity described in TA18-106A is encouraged to report them to DHS's National Cybersecurity and Communications Integration Center (NCCIC), FBI, NCSC or law enforcement immediately.

PUBLISHED

15 April 2018

WRITTEN FOR

Small & medium sized organisations

Self employed & sole traders

Public sector

Large organisations

Cyber security professionals

NEWS TYPE

General news