China, Russia linked to cyberspying, researchers say

October 28 2014, by Rob Lever

The Russian and Chinese governments are likely behind widespread cyberespionage that has hit targets in the US and elsewhere, two separate security reports said Tuesday.

One team of researchers led by the security firm Novetta Solutions said it identified a hacker group believed to act "on behalf of a Chinese government intelligence apparatus."

A separate report by the security frim FireEye said a long-running effort to hack into US defense contractors, Eastern European governments and European security organizations is "likely sponsored by the Russian government."

The Chinese group, which was dubbed Axiom, "is a well resourced, disciplined and sophisticated cyberespionage group operating out of mainland China," said Novetta chief executive Peter LaMontagne in a statement released with the study.

"Novetta has moderate to high confidence that the organization tasking Axiom is a part of Chinese Intelligence apparatus," the company said.

"This belief has been partially confirmed by a recent FBI flash released to Infragard (a partnership with the FBI and private sector) stating the actors are affiliated with the Chinese government."

Axiom has hacked pro-democracy non-governmental organizations and

other groups and individuals "perceived as a potential threat to the stability of the Chinese state," Novetta said.

"Axiom uses a varied tool-set ranging from generic malware to very tailored, custom malware designed for long-term persistence that at times can be measured in years."

The report was the result of research from a variety of security organizations including Cisco, FireEye, F-Secure, iSight Partners, Microsoft, Tenable and others.

Coordinated 'disruption'

The report said the firms went beyond simply collecting information and cooperated on a "coordinated, effective remediation and disruption" of the Chinese networks.

"Novetta feels that the unified approach... provides the highest level of visibility and establishes the foundation necessary to effectively counter a threat of this nature," the report said.

"It is Novetta's hope that others within industry will embrace and adopt a similar approach in the future."

In the other report, FireEye researchers said they uncovered evidence that links the Russian government to the cyberespionage efforts that have been known to originate from that part of the world.

FireEye said the hacker group dubbed APT28 "does not appear to conduct widespread intellectual property theft for economic gain, but instead is focused on collecting intelligence that would be most useful to a government."

It has targeted insider information related to governments, militaries, and security organizations since 2007, the report noted.

"Despite rumors of the Russian government's alleged involvement in high-profile government and military cyber-attacks, there has been little hard evidence of any link to cyberespionage," said Dan McWhorter, FireEye vice president of threat intelligence.

"FireEye's latest advance persistent threat report sheds light on cyberespionage operations that we assess to be most likely sponsored by the Russian government, long believed to be a leader among major nations in performing sophisticated network attacks."