Researchers warn of 'hit and run' cyber attackers

September 26 2013

Security researchers said Wednesday they uncovered a "cyber mercenary" team which specializes in attacks on targets in Japan and South Korea, and warned of more operations of that nature.

Security researchers said Wednesday they uncovered a "cyber mercenary" team which specializes in attacks on targets in Japan and South Korea, and warned of more operations of that nature.

Kaspersky Labs identified the group as "Icefog," and said evidence

points to it being based in China.

Based on the targets, the attackers appear to have an interest in military, shipbuilding and maritime operations, computers and software, research companies, telecom operators, satellite operators, mass media and television.

Kaspersky said the operation was a "small yet energetic Advanced Persistent Threat (APT) group" which focuses on targets involved in the supply chain for Western companies.

The operation started in 2011 and has increased in size and scope over the last few years, according to the report presented at a Washington cybersecurity conference.

The attackers have been "hitting pretty much all types of victims and sectors. In most cases, attackers maintain a foothold in corporate and governmental networks for years, smuggling out terabytes of sensitive information," said Kaspersky researcher Costin Raiu.

"The 'hit and run' nature of the Icefog attacks demonstrate a new emerging trend: smaller hit-and-run gangs that go after information with surgical precision. The attack usually lasts for a few days or weeks and after obtaining what they were looking for, the attackers clean up and leave."

Raiu said these types of hackers-for-hire groups are growing, developing into a "kind of 'cyber mercenary' team for the modern world."

The researchers localized the attackers and "assume some of the players behind this threat operation are based in at least three countries: China, South Korea and Japan," with the largest number in China.

The report, presented at the Billington Cybersecurity Summit, said Icefog targeted attacks relied on spear-phishing e-mails that attempt to trick the victim into opening a malicious attachment or a website.

Some of these attachments include images of scantily clad women or "decoy" documents; when users click on the attachments, they unwittingly install malicious software which allows access to the attackers.

"The attackers are hijacking sensitive documents and company plans, e-mail account credentials, and passwords to access various resources inside and outside the victim's network," a Kaspersky statement said.

"In most cases, the Icefog operators appear to already know very well what they need from the victims. They look for specific file names, which are identified and transferred" to the attackers.