US says North Korean malware lurking in computer networks

November 15 2017

US authorities said Tuesday malware developed in North Korea is still lurking in many computer networks, giving hackers backdoor access to government, financial, automotive and media organizations.

An alert issued by the Department of Homeland Security warned of surreptitious activity by the so-called "Hidden Cobra" hacker group, also known by the name "Lazarus."

US officials earlier this year blamed the group for a series of cyberattacks dating back to 2009, saying it was linked to the Pyongyang government.

In Tuesday's warning, the DHS Computer Emergency Response Team (CERT) said the hacker could still maintain a presence on victims' networks with the aim of "further network exploitation."

The report said some networks could be infected with the Volgmer "backdoor Trojan" or a remote administration tool known as Fallchill, which can give hackers complete control of a system.

It said FBI investigators suspect the Fallchill tool has been used since 2016 and Volgmer since 2013.

Private security analysts refer to Hidden Cobra as the "Lazarus" group of hackers linked to North Korea and likely behind a series of multimillion-dollar cyber thefts from banks around the world.

Some analysts say the Lazarus group may also have been behind the WannaCry ransomware outbreak earlier this year.

Hackers in the Hidden Cobra or Lazarus group have been active since 2009 and "have leveraged their capabilities to target and compromise a range of victims," according to a DHS report in June.

"Some intrusions have resulted in the exfiltration of data while others have been disruptive in nature."

DHS and FBI officials say the group "will continue to use cyber operations to advance their government's military and strategic objectives," according to the DHS report.

North Korea has denied orchestrating any cyber attacks, but the latest report comes amid rising tensions with the United States over the communist regime's nuclear testing program.