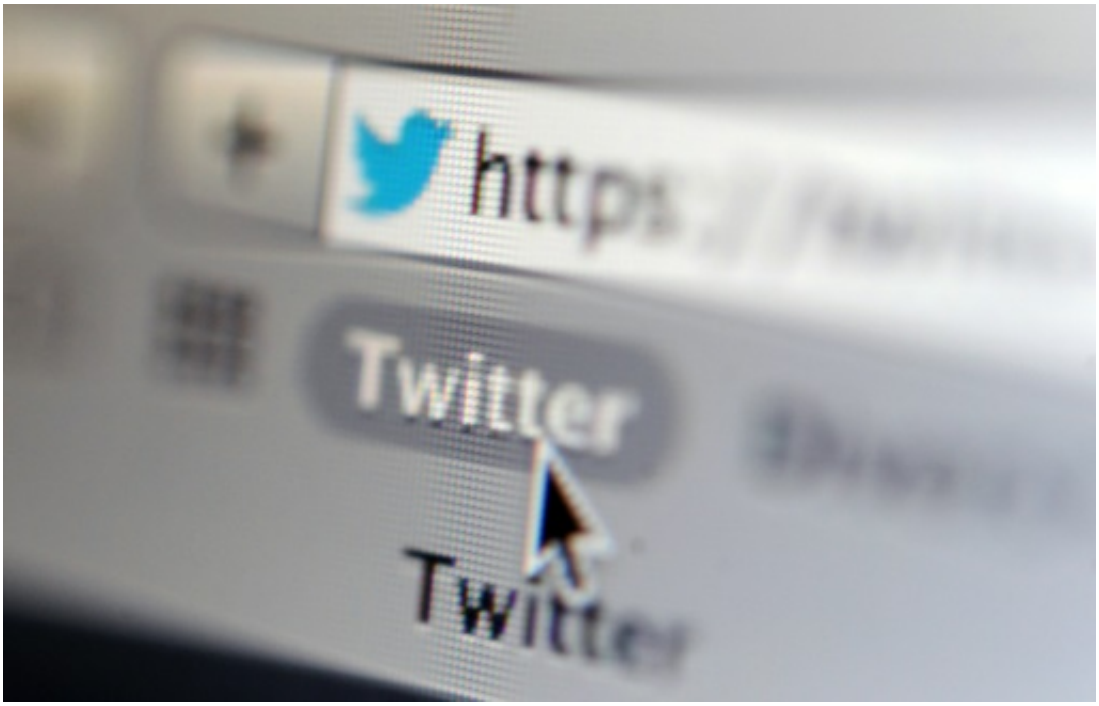
Hackers used Twitter to target US systems: researchers

July 30 2015



A report by the security firm FireEye says Russian-based hackers are using malicious software concealed in Twitter images to relay commands and steal data from US computer networks

Russian-based hackers are using malicious software concealed in Twitter images to relay commands and steal data from US computer networks, security researchers said this week.

A report by the security firm FireEye examined stealth techniques used

by hacker groups believed to be sponsored by the Russian government.

"Using a variety of techniques—from creating an algorithm that generates daily Twitter handles to embedding pictures with commands—the developers... have devised a particularly effective tool," FireEye said in the report released Wednesday.

Security researchers previously linked Russian-based hacker groups to efforts to penetrate computer networks at the White House and elsewhere.

FireEye said this group, dubbed APT29, is probably sponsored by the Russian government. It has been active since at least late 2014, according to the researchers.

The report said this particular attack tool, dubbed "Hammertoss," generates and looks for a different Twitter handle each day and seeks to blend in with normal traffic on the messaging platform.

Inside images generated in tweets, the hackers insert malicious code that enables them to steal data or gain access to computers that view the images.

"While the image appears normal, it actually contains steganographic data," or the practice of concealing a message, image or file within another message, according to FireEye.

The technique "undermines network defenders' ability to identify Twitter accounts used for (attacks), discern malicious network traffic from legitimate activity and locate the malicious payloads downloaded by the malware," the report said.

"This makes Hammertoss a powerful backdoor at the disposal of one of

the most capable threat groups we have observed."

More information: www2.fireeye.com/APT29-HAMMERT … SS-WEB-2015-RPT.html