US warns retailers on data-stealing malware

July 31 2014

US government cybersecurity watchdogs warned retailers Thursday about malware being circulated that allows hackers to get into computer networks and steal customer data.

The Department of Homeland Security's Computer Emergency Readiness Team said retailers should step up defenses against the new malware dubbed "Backoff."

The government and security experts have found evidence of hackers using this tool starting on October 2013, and continuing to the present.

A security bulletin from DHS said the cyberattacks use the same kind of remote tools that allow people to access business networks from home or on the road.

These include Microsoft's Remote Desktop, Apple Remote Desktop, Chrome Remote Desktop and others.

"Once these applications are located, the suspects attempted to brute force the login feature of the remote desktop solution," the DHS bulletin said.

"After gaining access to what was often administrator or privileged access accounts, the suspects were then able to deploy the point-of-sale (PoS) malware and subsequently exfiltrate consumer payment data."

The posting said most anti-virus programs have been unable to identify

or block the malicious software introduced by the attackers. But with the release of technical details, security firms should be able to update their programs.

The malware can allow the hackers to "scrape" data from the infected computers and in some cases use a "keylogger" to gain access to passwords.

An infection "can affect both the businesses and consumer by exposing customer data such as names, mailing addresses, credit/debit card numbers, phone numbers, and e-mail addresses to criminal elements," DHS said.

"These breaches can impact a business brand and reputation, while consumers' information can be used to make fraudulent purchases or risk compromise of bank accounts."

DHS said it has been working with the security firm Trustwave Spiderlabs "to provide relevant and actionable technical indicators for network defense."

The warning comes months after news of a massive data breach that allows hackers to potentially access millions of credit cards from retail giant Target. Other retailers including eBay have said they were also affected by breaches.