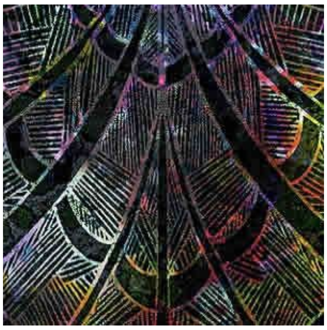
HealthManagement
Promoting Management and Leadership

Fighting 'Dark Web' Hackers



The "dark web" is something hidden from most users of the internet. This is because the dark web lies within what is known as the deep web – a part of the internet not indexed by search engines and without registered websites and domains.

Special software is required to access the dark web, which is especially designed not to allow one to find identities, locations, users, web sites or domains. As such, the dark web has become the source of numerous problems for healthcare CIOs and CISOs.

"The dark web hosts a variety of data posted for sale in forums, discussion groups and catalogue-style sites," explains Michelangelo Sidagni, chief technology officer at NopSec, a vendor of cybersecurity technology. "These include zero-day exploits with proof-of-concepts that never were disclosed and are for sale for hefty prices in bitcoins; one-day exploits for vulnerabilities that currently have patches but have no public exploits disclosed yet; custom malware, bot-as-a-service, DDoS-as-a-service, all for sale; and personally identifiable information such as credit cards, Social Security numbers, and login information that can be used in phishing attacks."

All of these vulnerabilities, exploits and custom malware can be used to compromise healthcare organizations. For instance, cybercriminals can hit healthcare organisations with unpatched vulnerabilities for which, for a very low price, they can buy an exploit for an existing vulnerability with a patch and then install some form of custom undetectable malware into a network.

Thus, security professionals need to look at security in a holistic way across the enterprise and applies best practices in risk management to build a more complete defence against the dark web, according to Bryan Hurd, senior executive, security strategy, at Versive, an artificial intelligence-based cybersecurity technology vendor.

Another way to protect against dark web-fuelled cyberattacks is to have security managers monitor and fix those vulnerabilities present in their networks that currently have one-day exploits on sale in the dark web, Sidagni said. CIOs and CISOs also need to monitor current dark web forums and black hat hacker sites indicating that a particular healthcare organisation has been compromised through monitoring of log-ins, credit cards, Social Security numbers and other PII for sale in the dark web, he added.

Hurd also highlights the importance of "collective action" in fighting attackers using the nefarious web.

"Instead of individual hospitals and healthcare companies trying individually to monitor the dark web for vulnerabilities or indicators of their medical information up for sale, they should consider collective action and threat information sharing via the National Health Information Sharing and Analysis Center (NH-ISAC) and other trusted communities," he said.

This model is a best practice used by the financial and critical infrastructure communities, Hurd added.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Mon, 24 Jul 2017