Gas stations have become a target for hacker groups, warns Visa

A recent security alert by Visa details how hacking groups are targeting gas stations to skim card data due to their vulnerabilities.

In summer 2019, Visa's Payment Fraud Disruption (PFD) identified three unique attacks targeting point-of-sale systems that were likely carried out by sophisticated cybercrime groups. Two of the attacks were carried out at U.S. gas stations.

Visa warns it has seen an increase of POS attacks against fuel dispenser merchants, and it is likely these retailers are an increasingly attractive target for cybercrime groups, according to the global payment provider.

The reason is the lack of secure acceptance technology such as EMV and tokenization, and non-compliance with PCI DSS.

Hacking groups such as FIN8 are actively exploiting vulnerabilities in gas station point-of-sale networks to skim card data without the need for modifications at the actual pumps.

In one of the incidents, Visa discovered how the hackers first sent a phishing email sent to an employee. The email contained a malicious link that, when clicked, installed a remote access Trojan on the network granting network access. Once the POS environment was successfully accessed, a Random Access Memory (RAM) scraper was deployed on the POS system to harvest payment card data.

Customers can avoid using their credit cards at the magnetic-stripe readers by paying cash or using a gas station payment app, according to consumer advocates.

Visa warns that "sophisticated threat groups have identified fuel dispenser merchants as an attractive target for obtaining track data."

Among the recommendations issued by Visa to retailers are: Employing the IOCs contained in the report, secure remote access with a strong password, enable EMV technologies, provide each admin user with their own user credentials, turn on behavioural analysis on anti-malware, monitor network traffic and maintain a patch management program.

In case of suffering a confirmed or suspected breach, refer to Visa's What to do if Compromised

(WTDIC), published October 2019.

Copyright © 2022. All rights reserved.