Visa Security Alert

NOVEMBER 2019

ATTACKS TARGETING POINT-OF-SALE AT FUEL DISPENSER MERCHANTS

Summary:
In August and September 2019, Visa Payment Fraud Disruption (PFD) investigated two separate breaches at North American fuel dispenser merchants. The attacks involved the use of point-of-sale (POS) malware to harvest payment card data from fuel dispenser merchant POS systems. It is important to note that this attack vector differs significantly from skimming at fuel pumps, as the targeting of POS systems requires the threat actors to access the merchant's internal network. In one of the two cases investigated by PFD, the threat actors successfully compromised the merchant's network through a phishing email that contained a malicious attachment. Once the malware was deployed on the merchant's network, it scraped Track 1 and Track 2 payment card data from the random access memory (RAM) of the targeted POS system. **The threat actors were able to obtain this payment card data due to the lack of secure acceptance technology, (e.g. EMV® Chip, Point-to-Point Encryption, Tokenization, etc.) and non-compliance with PCI DSS.**

The targeting of fuel dispenser merchants is the result of the slower migration to chip technology on many terminals, which makes these merchants an attractive target for criminal threat actors attempting to compromise POS systems for magnetic stripe payment card data.

1. Implications for Fuel Dispenser Merchants

Card skimming at fuel pumps remains a pervasive and increasing threat for fuel dispenser merchants. However, these recent, more technically-advanced threat campaigns targeting fuel dispenser merchant POS systems marks a concerning trend that will likely continue. Many fuel dispenser merchants are currently updating their systems to accept and process more secure transactions, such as upgrading to devices that support chip. However, as long as the magnetic stripe readers are in place, fuel dispenser merchants are becoming an increasingly attractive target for advanced threat actors with an interest in compromising merchant networks to obtain this payment card data.

The recent attacks are attributed to two sophisticated criminal groups with a history of large-scale, successful compromises against merchants in various industries. The groups gain access to the targeted merchant's network, move laterally within the network using malware toolsets, and ultimately target the merchant's POS environment to scrape payment card data. The groups also have close ties with the cybercrime underground and are able to easily monetize the accounts obtained in these attacks by selling the accounts to the top tier cybercrime underground carding shops.

Fuel dispenser merchants should take note of this activity as the group's operations are significantly more advanced than fuel dispenser skimming, and these attacks have the potential to compromise a high volume of payment accounts. The deployment of devices that support chip will significantly lower the likelihood of these attacks.

Recommendations for Fuel Dispenser Merchants

Fuel dispenser merchants should deploy terminals that support chip wherever possible to deter attacks targeting POS environments, as well as the fraud that occurs at non-chip POS terminals. As a reminder, after the Visa October 2020 chip liability shift date, the responsibility for counterfeit fraud will shift to the fuel dispenser merchants who have not enabled chip acceptance.

Visa recommends fuel dispenser merchants take the following actions to mitigate against these threats:

- **Deploy and enable chip acceptance** on all point-of-sale devices.
- **Deploy Point-to-Pont Encryption (P2PE).**
- **Employ the IOCs contained in this report** to detect, remediate, and prevent attacks using the POS malware variant.
- **Educate employees about cyber threats and phishing.**
- **Provide each Admin user with their own user credentials.** User accounts should also only be provided with the permissions vital to job responsibilities.
- **Secure remote access with strong passwords, ensure only the necessary individuals have permission for remote access, disable remote access when not in use, and use two-factor authentication for remote sessions.**
- **Verify the implementation of required security patches:** PCI DSS requires that all system components and software are protected from known vulnerabilities by installing security patches. Visit the PCI SSC website for more information.
- **Monitor network traffic** for suspicious connections, and log system and network events.
- **Implement Network Segmentation,** where possible, to prevent the spread of malicious software and limit an attacker's foothold.
- **Maintain compliance with all security controls defined in the PCI DSS.**
- **In the event of a confirmed or suspected breach, refer to Visa's *What to do if Compromised (WTDIC),* published October 2019.**

For more information, please contact **paymentintelligence@visa.com**