



SALTED HASH- TOP SECURITY NEWS

By Steve Ragan

About |

Fundamental security insight to help you minimize risk and protect your organization

NEWS

Wendy's investigating possible POS breach

Fast-food chain has hired a forensics firm to help determine the problem



CSO | Jan 27, 2016 12:14 PM PT

Wendy's, one of the nation's largest fast-food chains, says they're investigating a possible breach of their POS systems after banking industry contacts alerted them to unusual activity on customer cards.

Bob Bertini, a spokesperson for Wendy's told investigative journalist Brian Krebs, the company had received reports from payment industry contacts concerning "unusual activity involving payment cards at some of our restaurant locations."

"Reports indicate that fraudulent charges may have occurred elsewhere after the cards were legitimately used at some of our restaurants. We've hired a cybersecurity firm and launched a comprehensive and active investigation that's underway to try to determine the facts."

Compare: HP ArcSight vs Splunk

Bertini said that the company began investigating the reports immediately, and that the time frame they're working with is late 2015. However, it's too soon to know the actual scope of the incident.

Until more information emerges, most experts agree the public should avoid hype and speculation. This could impact a few stores, or it could impact Wendy's as a whole.

"Keeping in mind that traditionally, big corporations and retailers use franchised-based models, in many cases their security in different branches is absolutely decentralized on practice. This allows bad actors to take advantage of such insecurities and successfully distribute malware on terminals in order to collect Track 2 data, and to perform intrusions into their targeted networks for data exfiltration," said the Andrew Komarov, Chief Intelligence Officer at InfoArmor.

In truth, many POS systems have not been upgraded for years. In anticipation of 'chip and sign' changes to credit cards, some vendors have held off even longer, waiting for the latest technology to upgrade, explained Simon Crosby, the CTO of Bromium.

"The bad guys today know the world is changing, and they're out to milk their current attacks for all they are worth before they have to change tack. A simple rule of thumb: If a vendor does not support chip and sign, pay cash," he added.

If confirmed, then Wendy's is in good company when it comes to retail and fast-food breaches. Looking back, Jimmy Johns, Landry's (Mortons, Rainforest Cafe), P.F. Chang's, Dairy Queen, and Chick-fil-a all had a common link between their security incidents, the attackers focused on individual stores and POS systems in order to capture card data.

"One of the most important things to note here is that it's often a merchant bank or individual cardholder working in collaboration with a reporter (Krebs) to disclose the issue publicly. This either indicates that the organizations are either withholding or, more likely, have limited or no knowledge of the breach. Given the distributed nature of these systems, and the lack of tooling, the breaches are difficult to detect prior to exfiltration of the information," said Jonathan Cran, the VP of Operations, Bugcrowd.

"Also worth noting, as the frequency of these breaches is increasing, there may be a rush from the underground to collect non-EV cards before all retailers mandate them. EV chips will help prevent actual card duplication, but they won't prevent online (card not present) theft."




Steve Ragan — *Senior Staff Writer*



Insider: 10 Tough Security Interview Questions, and How to Answer Them

 [View Comments](#)

You Might Like

Promoted Links by Taboola 

[Fatherhood's Changed Prince William](#)

Reuters TV

使用当地通讯卡让泰国旅行更加轻松



[Sign In](#) | [Register](#)



Carophile

If You Only Have Three Days in San Francisco

AFAR Media

5 traits of successful developers

Intel

So You Want to Sweat? 8 Life Hacks for Staying Fit with MS

Living Like You by Novartis

Homido turns just about any smartphone into a VR headset

A huge Navy destroyer looks like a small boat on radar

NSFW: T-Mobile hurls insults at competitors AT&T, Verizon and Sprint

Roberto Coin Centro

Robb Report