360Cyber.co

POS
Malware
Case Study
By: James Moore Certified Cyber Security Analyst

PoS (point-of-sale) malware - Landry’s

- On January 2, 2020 Landry's announced a Malware attack (it’s 2nd)
- Landry's, Inc., is an American, privately owned, multi-brand dining, hospitality, entertainment and gaming corporation. Landry's, Inc. owns and operates more than 600 restaurants, hotels, casinos and entertainment destinations in the United States.
- The attackers collected Personally Identifiable Information (PII) including credit and debit card numbers, expiration dates, verification codes, and cardholder names.

PoS Malware Attacks

Point-of-sale malware is usually a type of malicious software that is used by cybercriminals to target point of sale and payment terminals with the intent to obtain credit card and debit card information.

Some Other Retailers affected by PoS Malware: Target, Apple Bees, Wendy’s, Daren Restaurants, Checkers and Rally's, Marriott Starwood Hotels, Panera Bread, Hyatt Hotels, Chipotle, Sonic, and Whole Foods.

PoS Malware has been on the decline from 2018 to 2020.

Although PoS Malware attacks are on the decline they still have the potential to come back if cyber criminals are able to circumvent chip-and-pin technologies.

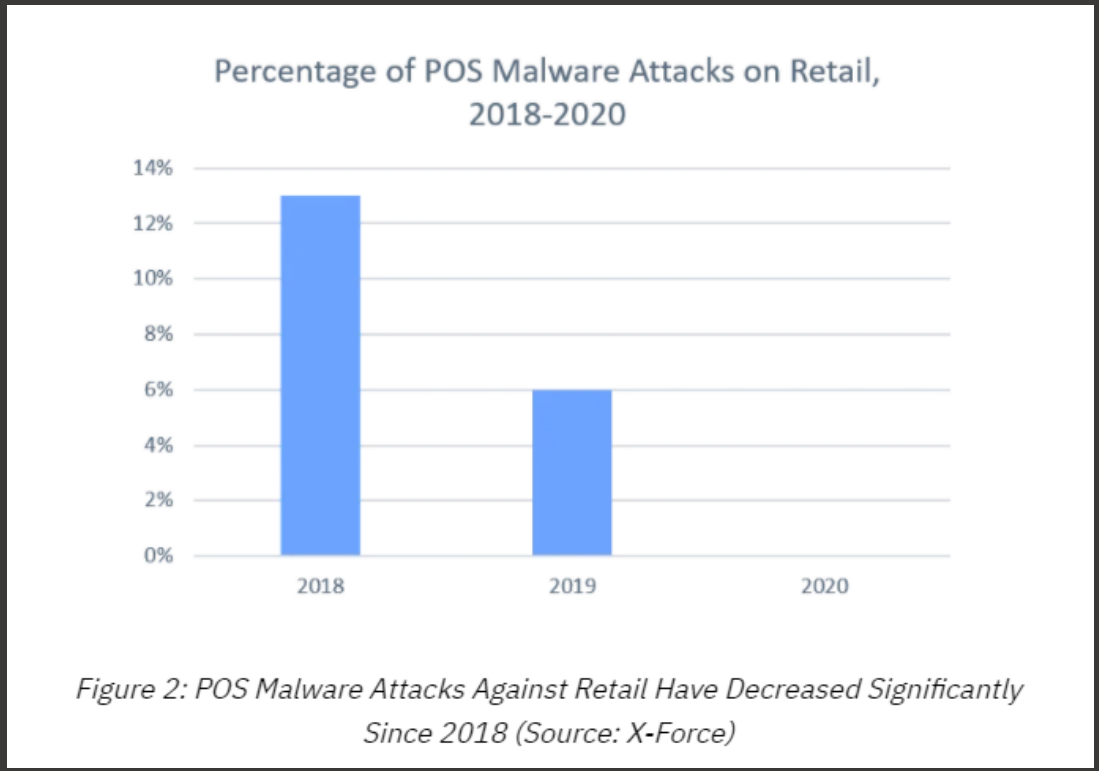

Figure 2: POS Malware Attacks Against Retail Have Decreased Significantly Since 2018 (Source: X-Force)

Landry’s

- Landry's, Inc., is an American, privately owned, multi-brand dining, hospitality, entertainment and gaming corporation. Landry's, Inc. owns and operates more than 600 restaurants, hotels, casinos and entertainment destinations in the United States.
- The malware affected cards mistakenly swiped on a Landry’s order-entry system (which did not have end point encryption), which is designed for use with a Landry’s reward card. Some customers cards were mistakenly swiped on the order-entry system where malware was installed.
- 63 of its 600 restaurants were affected by the breach.

Timeline

1. POS malware was active on the networks of bars and restaurants from as early as January 18, 2019, to October 17, 2019
2. December 31, 2019 Landry's notified customers
3. January 2, 2020 Landry's publicly announced a point-of-sale malware attack that targeted customers' payment card data
4. January 2, 2020 Landry's says all malware has been removed

Vulnerabilities

Unencrypted data

Although Landry's has previously suffered a data breach in 2016 (for lack of end-to-end encryption) they did not apply end to end encryption on their order entry systems. This allowed for a vulnerability for malware on their order entry system. After the 2016 breach they applied end to end encryption only on their PoS systems. Proper training of staff on proper use of PoS with the end-to-end encryption should have also taken place.

Costs

The cost for the data breach has not been publicly made available. However the incident from 2016 was around 20 million per the lawsuit filed by AIG.

Prevention

- End to end encryption needs to be implemented for all terminals.
- Training all employees on proper point of sale
- Using chip readers. Chipped cards produce a unique transaction code each time they are used, making it more difficult to replicate payment data.

References

Scott Ferguson (January 2, 2020) Restaurant Chain Landry's Investigates Malware Incident https://www.bankinfosecurity.com/restaurant-chain-landrys-finds-malware-in-payment-system-a-13571

Jeff Stone (November 27, 2019**)** AIG subsidiary tells court it's not responsible for Landry's legal costs in $20 million lawsuit filed after breach https://www.cyberscoop.com/aig-landrys-lawsuit-cyber-insurance/

Jeff Orr (January 3, 2020**)** Retail Point-Of-Sale Malware Hits Landry’s Restaurant Group https://www.cshub.com/attacks/articles/retail-point-of-sale-malware-hits-landrys-restaurant-group

Catlin Cimpanu (January 2, 2020) Landry's restaurant chain disclose POS malware incident https://www.zdnet.com/article/landrys-restaurant-chain-disclose-pos-malware-incident/

Camille Singleton (December 16, 2020) E-Commerce Skimming is the New POS Malware https://securityintelligence.com/posts/e-commerce-skimming-the-new-pos-malware/