Infocyte®

Protecting Retail Customers From POS Attacks

Maintain the Health of POS Systems with Routine Assessments

RECENT POS BREACHES

Retailers:

- Forever 21
- Whole Foods
- Brooks Brothers
- Eddie Bauer

Hospitality Groups:

- Intercontinental Hotel Group
- Trump Hotels
- Hyatt Hotels

Restaurants:

- Avanti
- Wendy's
- Chipotle
- Arby’s
- Sonic
- Jason's Deli

POS Systems Under Attack

For the past several years, Point of Sale (POS) systems have been a prime target for cyberattacks. Last year, POS systems were besieged by hackers using malware such as LockPos/FlokiBot, MajikPOS, and JackPOS, to name a few. The reason is no mystery - POS systems are a key part of a retailer's transaction process. They provide an access point through which cybercriminals can access and steal customers' payment information, making them attractive targets for malicious hackers.

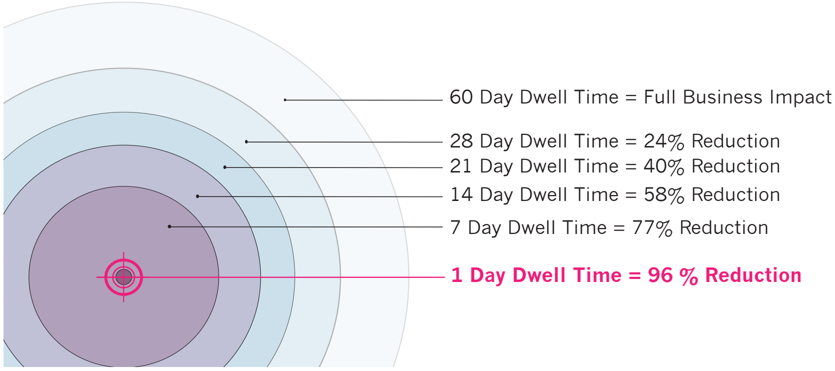
POS systems that support retail operations have been shown to be a weak spot in cybersecurity. A series of high profile hacks in 2017 exposed customers' personally identifiable information (PII) and payment card details. Recent POS malware created to hurt retailers include UDPoS and Poseidon, which has been identified by researchers as an evolved variant that was professionally designed to be quick and evasive with new capabilities such as communication with command-and-control servers, self-updating to execute new code and self-protection to guard against reverse engineering.

Business Impact of Controlling Dwell Time

One aspect that virtually defines the success of a hacker's attack is the length of time that the malware persists undetected on endpoints, otherwise known as dwell time. It is this period of time between infection and discovery that hackers use to steal data and siphon funds.

Retailers who rely on POS systems require the ability to control and limit dwell time if they are to begin properly and effectively protecting their customers' data and mitigate risk. The general business impact of dwell time has been studied and quantified. A recent research report[1] determined that simply limiting dwell time to 30 days results in a reduction of the impact on business by 23%. Further reductions in dwell time lead to a near eradication of the business impact, as seen in this diagram.

Controlling Dwell Time Protects Business



As this research shows, when retailers are able to successfully confine the dwell time of malware to one single day, they can effectively attain a 96% reduction in the impact to their business.

[1] Quantifying the Value of Time in Cyber-Threat Detection and Response, Aberdeen Group, February 2016

Defense Is Not Enough

Trust in defensive measures must be re-examined. Today's detection methods and technologies are predominantly focused on the real-time prevention and detection of attacks through 24/7 monitoring.

Whether EDR/EPP, firewalls, AV, or whitelisting, defensive solutions work to prevent malware from entering the network, however some malware does in fact bypass these defenses. When that occurs, these solutions are not designed to help find it post compromise.

What is missing from many enterprise security tool kits are solutions that work to detect the threats that have succeeded in compromising endpoints and are residing undetected.

Assessing the Health of POS Systems

Retailers would be advised to start taking proactive steps from to hunt down the malware that's residing undetected.

An excellent start is to use a scalable solution like Infocyte HUNT™ that can be used by your own security or IT teams to sweep endpoints including POS systems, looking for malware and APTs that are hiding on endpoints right now. Once found, these threats can be quickly neutralized.

Retailers using Infocyte HUNT are able to place controls around dwell time and reduce it, thereby limiting potential damage. The enterprise decides how often to scan endpoints, effectively placing a limit on the length of potential dwell time in the event of a breach.

Threat Hunting Simplified

Infocyte HUNT is an automated forensics-based tool built to detect hidden malware and persistent threats whether they are known or unknown, actively running or scheduled to run. Using a Forensic State Analysis methodology and memory un-mapping techniques, Infocyte combines and examines data from multiple sources including both volatile and non-volatile memory, along with non-memory based information required to identify persistence mechanisms.

Infocyte HUNT operates independent from the host OS and collects its own data, helping to ensure unbiased results. The reports generated are easy to read and action, providing a snapshot of the current state of each endpoint to help speed remediation.

Infocyte HUNT

- Definitively answers if your endpoints are compromised
- Advanced detection combines forensic automation and patent-pending memory analysis
- Infocyte's platform uses volatile memory analysis to determine the compromise state of an endpoint at a given point in time
- Infocyte HUNT is not reliant on a host OS, which may be itself compromised
- Fast — Infocyte HUNT can scan upwards of 50,000 endpoints per day
- Easy to use — Infocyte HUNT doesn't require experts or extensive training to use effectively
- Provides actionable intelligence within minutes

Don't wait to be told that you've been the victim of a cyberattack by angry customers or the authorities. Take control and proactively hunt for POS compromises with Infocyte HUNT.

Start Hunting.
Contact us to learn how.

Infocyte®

CORPORATE HEADQUARTERS
110 E. Houston St. Floor 6
San Antonio, TX 78205
+ 1.844.INFOCYTE (844.463.6298)
sales@infocyte.com

www.infocyte.com
@InfocyteInc