OVERVIEW

Why does Malware Target Banks…

Strictly speaking, malware is a means to an end. Ransomware, for example, is just a form of malware with a goal of extorting the recipient. But many forms of malware are designed to go undetected for as long as possible, stealing data such as credit card numbers, social security numbers, proprietary data, even espionage-like activities such as recording in-person conversations.

Credit card data breaches are far and away the most common form of malware data breaches. Criminals typically implant malware on Point of Sale (POS) terminals or servers which siphons credit card data to their servers, which they sell in batches on underground markets. In late 2019, the East Coast gas station chain Wawa disclosed that it suffered this exact flavor of breach, and by January 2020 they were listed for sale, with the seller claiming over 30 million cards were available as a result of the breach. The malware went undetected for approximately 9 months.

Although specific details have been scant on which malware affected Wawa, Visa has continually referred to two advisories it issued around the time of the Wawa breach: a general advisory, and a more specific advisory which included Indicators of Compromise. Their recommendations are consistent with ours.

BEST PRACTICE

Malware Resulting in Data Breach

Resilience's Cyber Meteorology Framework models cyber risk trends and helps companies stay up-to-date with current best practices and mitigation guidance. Resilience's model for a data breach caused by a malware infection recommend that organizations do the following to prevent and mitigate these attacks:

1. Use Attack Surface Monitoring software to periodically (and ideally, continuously) monitor your organization's internet footprint to detect common vulnerabilities on your internet-facing infrastructure
2. Implement Network Segmentation to deter an actor from moving from one server to another. In this case, it's especially concerning if an actor moves to POS terminals.
3. Employ endpoint detection and response (EDR) products
4. Ensure users and administrators use strong, unique passwords and are provisioned their own accounts. Use a password manager to generate and rotate these.

INSURANCE

Breach of Privacy

A malware-caused data breach is every CISO's nightmare. Insurance should cover the costs associated with responding to Payment Card Industry Data Security Standard investigations, and the potential assessments that the payment card brands may levy after an event. Ask your broker for more information.

Example Claim

National fast food chain suffered a malware data breach at its point-of-sale machines. POS terminals at 1,250 locations were hacked, and more than 12 million credit cards were stolen - some later suffering fraudulent charges. PCI investigation launched, multi-million dollar assessment issued, and class action lawsuit filed.