Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SSC Bulletin on Malware Related to Recent Breach Incidents

27 August 2014

URGENT Immediate Action required:

In a statement released on 22 August by the United States Secret Service and Department of Homeland Security, a warning was issued that a Point of Sale (POS) malware dubbed “Backoff” may have infected systems in over 1,000 organizations and represents a very real threat to the security of cardholder data in all organizations. This malware released in 2013 infects electronic cash registers (ECRs) and similar POS systems, and was not recognized by antivirus software solutions until this August. It infects POS systems and has already resulted in large amounts of cardholder data being compromised and transmitted to criminal organizations.

In support of this statement, the PCI Council strongly encourages organizations as a matter of urgency to consider the following recommendations:

1. Contact your provider of antivirus solutions and ensure you have the most recent and up to date version of antivirus software that will detect “Backoff” and other similar malware.
2. Run this solution immediately.
3. Review all system logs for any strange or unexplained activity, especially large data files being sent to unknown locations.
4. Require all default and staff passwords on systems and applications to be updated. Provide good guidance on choosing a secure password (see PCI Data Security Standard Requirements 2,8).

The PCI Council additionally recommends that merchants consider implementing PCI-approved point-of-interaction (POI) devices that support the secure reading and exchange (SRED) of data which encrypts data at the point of capture and would prevent exposure of clear-text data within the ECR or similar POS systems. Merchants should also consider implementing a PCI-approved point-to-point encryption (P2PE) solution which includes SRED devices and protects the data until received by the secure decryption facility.

Should systems be found to be infected or unusual activity suspected, organizations should contact their acquiring bank immediately.

As the National Cybersecurity and Communications Integration Center (NCCIC), United States Secret Service (Secret Service), and third-party partners further detailed in a “Backoff” advisory on 31 July, is imperative to have good system and network data security in place. The PCI Standards outline the security controls necessary to effectively help prevent hackers from penetrating a payment environment and installing malicious software that would jeopardize the protection of card data as it is being processed. These include techniques for maintaining POS security and a secure terminal environment, and monitoring and managing access to systems.

Regarding malware specifically, organizations should review the following security risk mitigating control areas outlined in PCI Data Security Standard (PCI DSS) 3.0:

- Proper firewall configuration – Requirement 1
- Changing vendor defaults and passwords on devices and systems – Requirement 2
- Regularly updating anti-virus protections – Requirement 5
- Patching systems – Requirement 6
- Limiting access and privileges to systems – Requirements 7,9
- Requiring 2-factor authentication and complex passwords – Requirement 8
- Inspection of POS devices – Requirement 9
- Monitoring systems to allow for quick detection – Requirements 10, 11
- Implementing sound security policies for preventing intrusions that may allow malware to be injected – Requirement 12
- Managing third party access to devices and systems, and specifically remote access from outside a merchant’s network — Requirements 8, 12

Attacks of this kind underscore the critical importance of a multi-layered approach to payment card security that addresses people, process and technology. PCI Standards provide layers of defense to ensure businesses can prevent, defend and detect attacks on their systems. A daily coordinated focus on maintaining these controls – making payment card security a business as usual practice - provides a strong defense against data compromise.

Managing third party provider access remains a challenge for organizations. The Council also encourages organizations to reference recently released guidance developed by a Special Interest Group on managing risk and securing data when working with third parties to support PCI DSS ensure payment data and systems entrusted to third parties are maintained in a secure and compliant manner. For more information on the PCI Standards and supporting resources for payment security, please visit: www.pcisecuritystandards.org