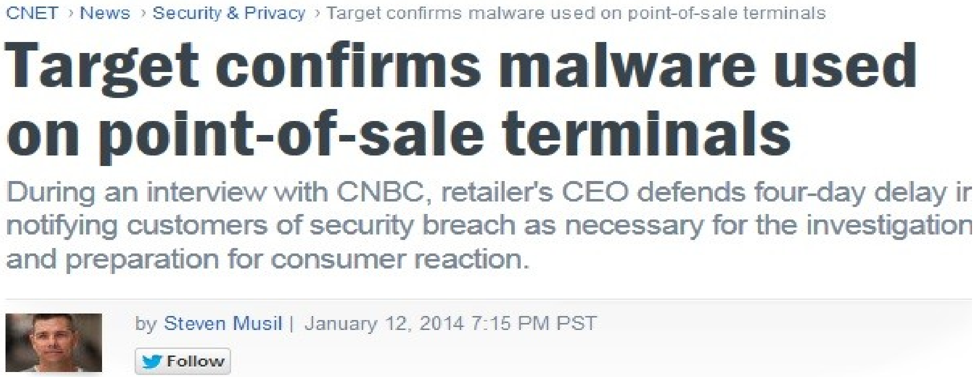
IBM Systems Lab Services & Training - Power Systems

Services for AIX, i5OS, and Linux on Power– PowerCare Eligible

http://www.ibm.com/systems/services/labservices/platforms/labservices_power.html

AIX Malware Prevention Workshop

with AIX Trusted Execution



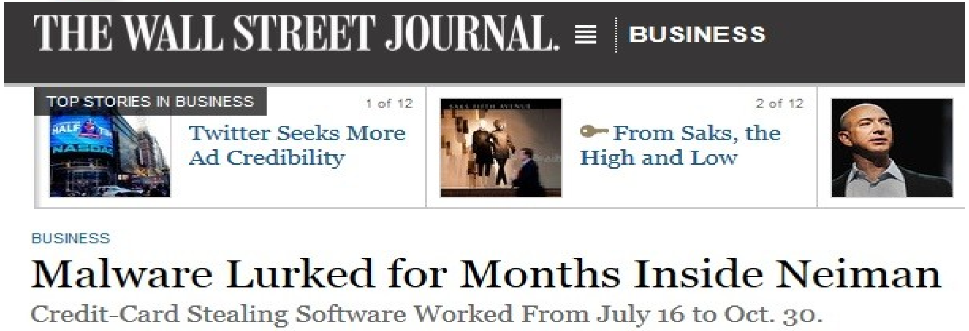
CNET › News › Security & Privacy › Target confirms malware used on point-of-sale terminals

Target confirms malware used on point-of-sale terminals

During an interview with CNBC, retailer's CEO defends four-day delay ir notifying customers of security breach as necessary for the investigation and preparation for consumer reaction.

by Steven Musil | January 12, 2014 7:15 PM PST

Follow



THE WALL STREET JOURNAL. ≡ | BUSINESS

TOP STORIES IN BUSINESS

1 of 12

Twitter Seeks More Ad Credibility

2 of 12

From Saks, the High and Low

BUSINESS

Malware Lurked for Months Inside Neiman

Credit-Card Stealing Software Worked From July 16 to Oct. 30.

Overview:

Companies frequently and unknowingly fail to deploy proper security countermeasures for malware, which exposes these companies to high risk of a security breach leading to numerous harmful effects, such as damage to a company's brand, huge financial losses, identity theft, costly litigation, etc.

Fortunately, IBM has provided a powerful solution, AIX Trusted Execution (TE), to drastically reduce the risk posed by malware, and IBM Lab Services has provided a service to help you quickly deploy this indispensable tool for preventing malware on AIX networks.

Workshop Description:

In this workshop, we will look at the nuts and bolts of Trusted Execution (TE) deployment and work through several TE lab exercises in order to gain experience in addressing the most critical elements of TE deployment

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate scope, agenda, schedule and required materials.

- Customer provides overview of their current malware prevention tooling, (if possible)
- IBM team prepares the service agenda, schedule, etc.

Phase 2 – AIX Malware Prevention Workshop (on-site):

Example Tasks

- Learn how to prevent and detect the various types of malware, such as: viruses, rootkits, trojan horses, etc using TE
- Learn how to generate TE logging reports
- Learn how TE can be used to satisfy regulatory standards, such as PCI, HIPAA, NERC-CIP,DoD STIG, SOX-COBIT
- Learn how to install and configure TE
- Learn how to enable 3rd party scripts and applications for TE monitoring
- Learn how to prevent scripts and applications from being infected or altered by malware

Deliverables – Step-by-step configuration documents & all slides

TE Demo (Optional – Time permitting)

Duration:

2 days on-site

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Stephen Dominguez – *WW LBS AIX Security Lead* - sdoming@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182