AUGUST 2016

blackfoot

BLACKFOOT NEWSFLASH

ADVICE FOR MERCHANTS USING RETAIL-J FOLLOWING ORACLE BREACH

A number of sources have published news that Oracle have suffered a breach at their MICROS POS division. We understand that Oracle have been in contact with customers to inform and update them about the breach.

The breach apparently involves more than 700 infected systems computers and servers at the company's retail division, but it is not clear which of Oracle's clients are affected at this stage. Of course by the time Oracle determine this, merchant breaches may have already occurred.

We understand that the Oracle breach affects their support infrastructure for legacy MICROS systems, including Retail-J.

As a result of the breach, compromised credentials for customer accounts at the Oracle MICROS support portal could be used to remotely administer, and more importantly, to upload card-stealing malware to, customer POS systems.

It is likely that any malware would look for networked machines running MICROS software, install itself, and then copy all data received from external ports (USB or serial), i.e. copying all data received from the PED or swipe device.

For merchants using MICROS PED encryption, the risk of a cardholder data breach from this malware is reduced.

Since Oracle cannot yet identify precisely which clients are affected by the breach, it is prudent for MICROS Retail-J merchants to proceed as though they have been breached, and take steps to minimise the potential damage.

Blackfoot recommend the following actions as a minimum:

Reset passwords for the Oracle MICROS online support portal.

Reset any system passwords that have been used by or shared with MICROS support representatives (including but not restricted to admin accounts, local user accounts, Back Office, Estate Manager, tills, ftp, remote access, etc.).

Perform an Anti-virus scan on all components of the Micros system, making sure that the AV tool can detect and remove the MalumPOS malware.

Pay special attention to perimeter controls, IPS/IDS/Logs/Firewalls/etc., in order to detect any deviations from normal network traffic.

Check for any network traffic to or from the indicators of compromise (IOCs) IP addresses associated with the suspected criminals, the Carbanak Gang. On Krebs on Security here and from Visa (published in relation to the Oracle MICROS breach) here.

Pay special attention to anti-virus/malware logs on POS systems and back-end servers accessible by Oracle support, in order to detect the occurrence of malware/unusual executables.

Ensure that in-bound firewall rules for access to POS systems restrict access to Oracle support IP address ranges.

If you are an Oracle MICROS Retail-J customers and are concerned about these issues, please call Blackfoot on 0845 805 2409

blackfoot

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >
ASSESS >
ASSURE >

This material is for information purposes only and does not take into consideration the particular circumstances or objectives of your business. Whilst every reasonable effort has been made to ensure the accuracy of the information in this document, Blackfoot UK Limited shall not be held liable for any errors or omissions.