

## New Data Breach May Affect 330,000 Retail Locations Around the Globe

August 8, 2016 - It's an everyday occurrence for most of us. We walk into a retail store, check into a hotel or stop for a cup of coffee. To make payment for these items, we swipe our credit or debit card through a machine and simply walk away. Unless there is a problem - like identity theft - most of us will never think about the transactions we've made in the past again. But the news today about a malware attack at Oracle may make you think twice the next time swipe your card at payment terminal. There is a report out that Oracle's MICROS payment system - the third largest point of sale system on the globe - has been compromised by Russian hackers.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
po.src = 'https://apis.google.com/js/plusone.js';  
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

Krebs on Security is once again the first to report this hack. According to the report, more than 700 MICROS computer servers at Oracle were compromised by having malware installed on them. Although the MICROS payment system encrypts credit card data, making it difficult for hackers to access, the malware also allowed the hackers to access retailers' accounts through an online support portal. That portal reportedly provides direct access to point of sale terminals located in retail locations. Once hackers have that kind of access, they can actually read payment card data as it is input.

At present, there is no real evidence that the hackers have been using the installed malware in this way. But Krebs is reporting that infected servers at Oracle were communicating with a server located in Russia that is known to belong to a large Russian hacking group called Carbanak Gang. This group has been known to steal more than \$1 billion from other banks and retailers in the past. Given this, there is a very good chance that the group was using its access to MICROS to enrich itself.

It is not yet known when Oracle's computers were first infected and the company isn't saying too much publicly. They

have said that they have removed the malware from their systems and are telling their MICROS customers to change their passwords for their support site.

MICROS is a global payment system that is used by some of the biggest names in retail, restaurants and hotels. The breach may have affected as many as 330,000 point of sale locations.

Since this breach can't be attributed to any specific retailer, the only way for consumers to protect themselves from erroneous charges is to check their debit and credit card statements thoroughly and challenge charges for any items they don't recognize.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#).

Registration is easy and free.

Follow me on Twitter:

Follow ACCESS