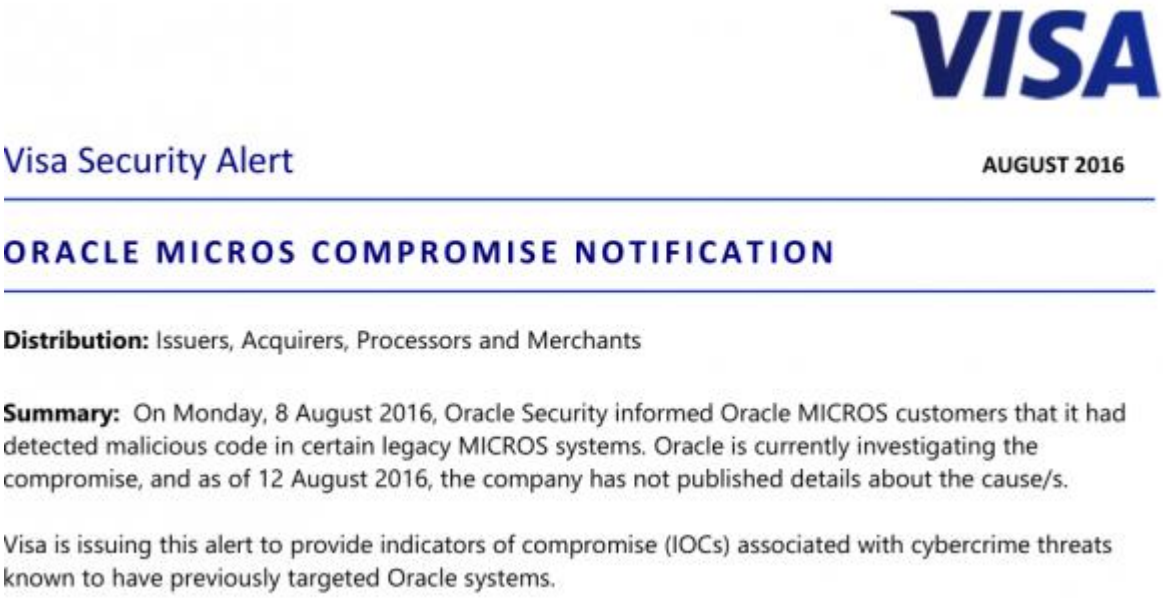
13
AUG 16

Visa Alert and Update on the Oracle Breach

Credit card industry giant **Visa** on Friday issued a security alert warning companies using point-of-sale devices made by **Oracle**'s **MICROS** retail unit to double-check the machines for malicious software or unusual network activity, and to change passwords on the devices. Visa also published a list of Internet addresses that may have been involved in the Oracle breach and are thought to be closely tied to an Eastern European organized cybercrime gang.



VISA

Visa Security Alert AUGUST 2016

ORACLE MICROS COMPROMISE NOTIFICATION

Distribution: Issuers, Acquirers, Processors and Merchants

Summary: On Monday, 8 August 2016, Oracle Security informed Oracle MICROS customers that it had detected malicious code in certain legacy MICROS systems. Oracle is currently investigating the compromise, and as of 12 August 2016, the company has not published details about the cause/s.

Visa is issuing this alert to provide indicators of compromise (IOCs) associated with cybercrime threats known to have previously targeted Oracle systems.

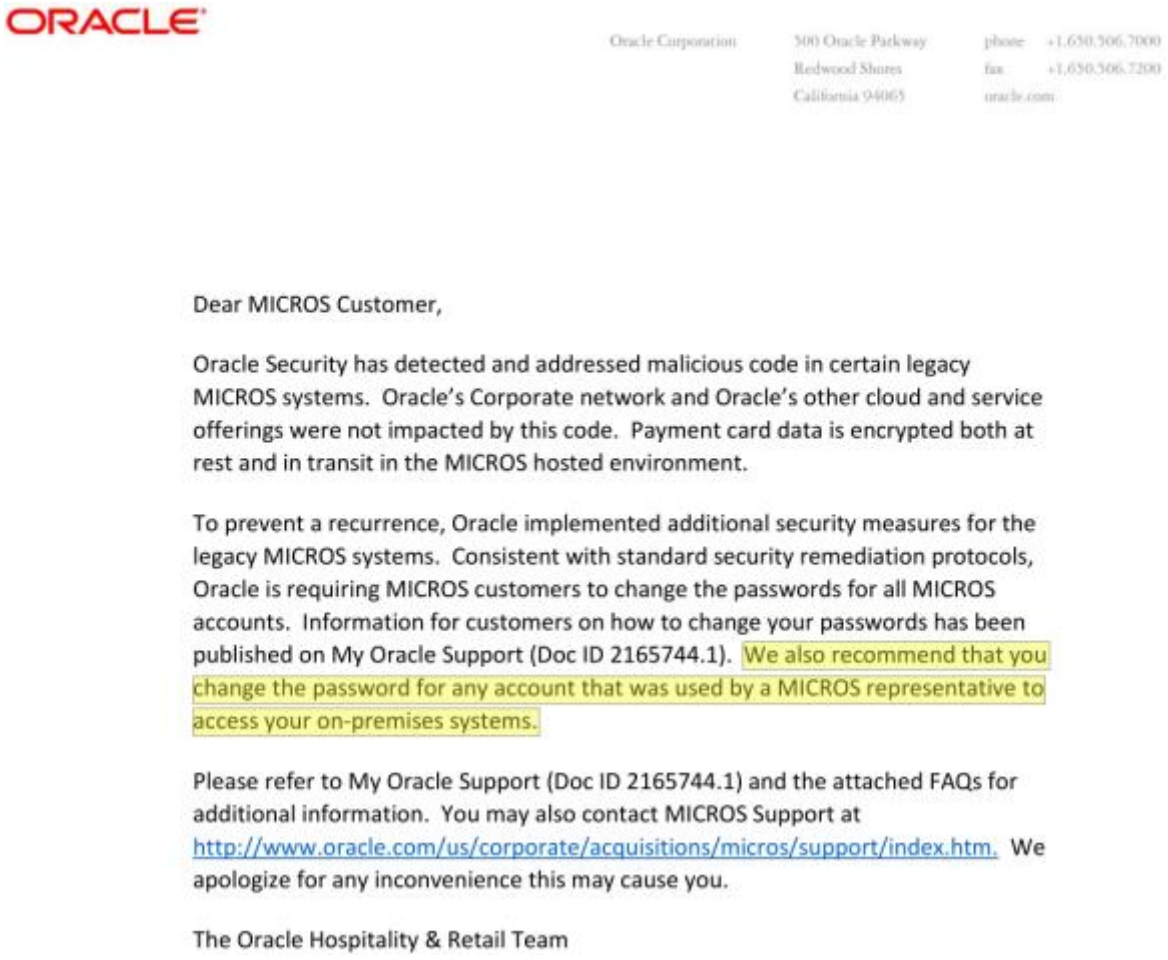
The Visa alert is the first substantive document that tries to help explain what malware and which malefactors might have hit Oracle — and by extension many of Oracle's customers — since KrebsOnSecurity broke news of the breach on Aug. 8. That story cited sources close to the investigation saying hackers had broken into hundreds of servers at Oracle's retail division, and had completely compromised Oracle's main online support portal for MICROS customers.

MICROS is among the top three point-of-sale vendors globally. Oracle's MICROS division sells point-of-sale systems used at more than 330,000 cash registers worldwide. When Oracle bought MICROS in 2014, the company said MICROS's systems were deployed at some 200,000+ food and beverage outlets, 100,000+ retail sites, and more than 30,000 hotels.

In short, tens of millions of credit cards are swiped at MICROS terminals monthly, and a breach involving the theft of credentials that might have granted remote access to even just a small percentage of those systems is potentially a big and costly problem for all involved.

So far, however, most MICROS customers are left scratching their heads for answers. A frequently asked questions bulletin (PDF) Oracle also released last Monday held little useful information. Oracle issued the same cryptic response to everyone who asked for particulars about how far the breach extended. "Oracle has detected and addressed malicious code in certain legacy MICROS systems."

Oracle also urged MICROS customers to change their passwords, and said "we also recommend that you change the password for any account that was used by a MICROS representative to access your on-premises systems."



ORACLE

Oracle Corporation 500 Oracle Parkway phone +1.650.506.7000
Redwood Shores fax +1.650.506.7200
California 94065 oracle.com

Dear MICROS Customer,

Oracle Security has detected and addressed malicious code in certain legacy MICROS systems. Oracle's Corporate network and Oracle's other cloud and service offerings were not impacted by this code. Payment card data is encrypted both at rest and in transit in the MICROS hosted environment.

To prevent a recurrence, Oracle implemented additional security measures for the legacy MICROS systems. Consistent with standard security remediation protocols, Oracle is requiring MICROS customers to change the passwords for all MICROS accounts. Information for customers on how to change your passwords has been published on My Oracle Support (Doc ID 2165744.1). We also recommend that you change the password for any account that was used by a MICROS representative to access your on-premises systems.

Please refer to My Oracle Support (Doc ID 2165744.1) and the attached FAQs for additional information. You may also contact MICROS Support at http://www.oracle.com/us/corporate/acquisitions/micros/support/index.htm. We apologize for any inconvenience this may cause you.

The Oracle Hospitality & Retail Team

One of two documents Oracle sent to MICROS customers and the sum total of information the company has released so far about the breach.

Some technology and fraud experts, including **Gartner** Analyst **Avivah Litan**, read that statement highlighted in yellow above as an acknowledgement by Oracle that hackers may have abused credentials gained in the MICROS portal breach to plant malicious code on the point-of-sale devices run by an unknown number of MICROS customers.
"This [incident] could explain a lot about the source of some of these retail and merchant point-of-sale hacks that nobody has been able to definitively tie to any one point-of-sale services provider," Litan told me last week. "I'd say there's a big chance that the hackers in this case found a way to get remote access" to MICROS customers' on-premises point-of-sale devices."

Clearly, Visa is concerned about this possibility as well.

INDICATORS OF COMPROMISE

In my original story about the breach, I wasn't able to reveal all the data I'd gathered about the apparent source of the attacks and attackers. A key source in that story asked that I temporarily delay publishing certain details of the investigation, specifically those known as indicators of compromise (IOCs). Basically, IOCs are list of suspect Internet addresses, domain names, filenames and other curious digital clues that are thought to connect the victim with its attacker.

I've been inundated all week with calls and emails from security experts asking for that very data, but sharing it wasn't my call. That is, until yesterday (8/12/16), when Visa published a "merchant communication alert" to some customers. In that alert (PDF), Visa published IOCs that may be connected with the intrusion. These IOCs could be extremely useful to MICROS customers because the presence of Internet traffic to and from these online destinations would strongly suggest the organization's point-of-sale systems may be similarly compromised.

Some of the addresses on this list from Visa are known to be associated with the **Carbanak Gang,** a group of Eastern European hackers that Russian security firm **Kaspersky Lab**estimates has stolen more than $1 billion from banks and retailers. Here's the IOCs list from the alert Visa pushed out Friday:

Scan networks for IOCs linked to Carbanak:

Carbanak Associated Indicators of Compromise

Confidence Level	Domain	Associated IP	Registered	Registrant Email	Registrar	DNS Service
High - High degree of correlation	clients1-google[.]com	85[.]10[.]229[.]196	10/21/15	Domainshield protected	OnlineNIC	SkyDNS
N/A	clients2-google[.]com	80[.]255[.]3[.]109	9/18/15	herman-k@rambler[.]ru	TLD	N/A
High - High degree of correlation	clients3-google[.]com	192[.]169[.]82[.]86	7/29/15	N/A	NameSilo	Qhoster
High - Corroborated	clients4-google[.]com	192[.]169[.]82[.]86	7/29/15	lobotamia29393@mail[.]ru	NameSilo	Qhoster
High - High degree of correlation	clients5-google[.]com	N/A	N/A	bornd-john@rambler[.]ru	NameSilo	Qhoster
High - High degree of correlation	clients6-google[.]com	N/A	12/2/15	Andrei.ryazanov.78@mail[.]ru	NameSilo	Qhoster
High - High degree of correlation	clients7-google[.]com	192[.]169[.]82[.]86	12/2/15	avraamlinkl@mail[.]com	NameSilo	Qhoster
High - High degree of correlation	clients8-google[.]com	164[.]132[.]221[.]147	12/2/15	Domainshield protected	OnlineNIC	SkyDNS
High - High degree of correlation	clients9-google[.]com	N/A	12/2/15	Domainshield protected	OnlineNIC	SkyDNS
High - Corroborated	clients12-google[.]com	107[.]181[.]246[.]211	12/3/15	g_mike@rambler[.]ru	N/A	CIShost[.]ru
High - Corroborated	clients14-google[.]com	185[.]86[.]149[.]115	12/3/15	g_mike@rambler[.]ru	PDR Ltd.	CIShost[.]ru

Visa warned merchants to check their systems for any communications to and from these Internet addresses and domain names associated with a Russian organized cybercrime gang called "Carbanak."

Thankfully, since at least one of the addresses listed above (192.169.82.86) matched what's on my source's list, the source agreed to let me publish the entire thing. Here it is. I checked my source's list and found at least five Internet addresses that were seen in both the Oracle attack and in a Sept. 2015 writeup about Carbanak by **ESET Security**, a Slovakian antivirus and security company. [NB: If you are unskilled at safely visiting malicious Web sites and/or handling malware, it's probably best not to visit the addresses in the above-linked list.]

Visa also mentioned a specific POS-malware threat in its alert called "**MalumPOS**." According to researchers at **Trend Micro,** MalumPOS *is malware designed to target point-of-sale systems in hotels and related industries. In fact, Trend found that MalumPOS is set up to collect data specifically from point-of-sale systems running on Oracle's MICROS platform.*

It should come as no surprise then that many of Oracle's biggest customers in the hospitality industry are starting to make noise, accusing Oracle of holding back key information that could help MICROS-based companies stop and clean up breaches involving malware and stolen customer credit card data.

> *"Oracle's silence has been deafening," said **Michael Blake**, chief executive officer at HTNG, a trade association for hotels and technology.*

"Oracle's silence has been deafening," said **Michael Blake**, chief executive officer at HTNG, a trade association for hotels and technology. "They are still grappling and trying to answer questions on the extent of the breach. Oracle has been invited to the last three [industry] calls this week and they are still going about trying to reach each customer individually and in the process of doing so they have done nothing but given the lame advice of changing passwords."

The hospitality industry has been particularly hard hit by point-of-sale compromises over the past two years. Last month, KrebsOnSecurity broke the news of a breach at Kimpton Hotels (Kimpton appears to run MICROS products, but the company declined to answer questions for this story).

Kimpton joins a long list of hotel brands that have acknowledged card breaches over the last year, including Trump Hotels (twice), Hilton, Mandarin Oriental, and White Lodging(twice), Starwood Hotels and Hyatt. In many of those incidents, thieves had planted malicious software on the point-of-sale devices at restaurants and bars inside of the hotel chains. And, no doubt, many of those cash registers were run on MICROS systems.

If Oracle doesn't exactly know which — if any — of its MICROS customers had malware on their point-of-sale systems as a result of the breach, it may be because the network intruders didn't have any reason to interact with Oracle's customers via the MICROS portal after stealing usernames and passwords that would allow them to remotely access customer on-premises systems. In theory, at that point the fraudsters could have bypassed Oracle altogether from then on.

BREACHED BY MULTIPLE ACTORS?

Another possibly interesting development in the Oracle breach story: There are indications that Oracle may have been breached by more than one cybercrime group. Or at least handed off from one to the other.

Late this week, **Thomas Fox-Brewster** at **Forbes** published a story noting that MICROS was just one of at least five point-of-sale companies that were recently hacked by a guy who — from an exhaustive review of his online chats — appears to have just sat himself down one day and decided to hack a bunch of point-of-sale companies.

Forbes quoted my old friend **Alex Holden** of Hold Security saying he had evidence that hackers had breached at least 10 payment companies, and the story focuses on getting confirmation from the various other providers apparently breached by the same cybercriminal actor.

Holden showed me multiple pages worth of chat logs between two individuals on a cybercrime forum [full disclosure: Holden's company lists me as an adviser, but I accept no compensation for that role, and he ignores most of my advice].

The discussion between the two hackers begins around July 15, 2016, and goes on for more than a week. In it, the two hackers have been introduced to one another through a mutual, trusted contact. For a while, all they discuss is whether the seller can be trusted to deliver the Oracle MICROS database and control over the Oracle MICROS customer ticketing portal.

In the end, the buyer is convinced by what he sees and agrees to pay the bitcoin equivalent of roughly USD $13,000 for access to Oracle's MICROS portal, as well as a handful of other point-of-sale Web sites. The buyer's bitcoin wallet and the associated transactions can be seen here.

A screen shot shared by one of the hackers involved in compromising Oracle's MICROS support portal. This screen shot was taken of a similar Web shell the hackers placed on the Web site of another POS provider (this is not the shell that was on Oracle).

According to the chat log, the hacker broke in by exploiting a file-upload function built into the MICROS customer support portal. From there the attackers were able to upload an attack tool known as a "WSO Web Shell." This is a crude but effective text-based control panel that helps the attacker install additional attack tools to harvest data from the compromised Web server (see screen shot above). The beauty of a Web shell is that the attacker can control the infected site using nothing more than a Web browser, using nothing more than a hidden login page and a password that only he knows.

The two hackers discussed and both viewed more than a half-dozen files that were apparently left behind on the MICROS portal by the WSO shell they uploaded in mid-July (most of the malicious files ended in the file extension "wso.aspx"). The chat logs show the pair of miscreants proceeding to target another 9 online payment providers or point-of-sale vendors. Some of those companies were quoted in the Forbes piece having acknowledged a breach similar to the Web shell attack at Oracle. But none of them have anywhere near the size of Oracle's MICROS customer base.

GOOD HOSPITALITY, OR SWEPT UNDER THE RUG?

Oracle maintains in its FAQ (PDF) about the MICROS attack that "Oracle's Corporate network and Oracle's other cloud and service offerings were not impacted." But a confidential source within Oracle's Hospitality Division told KrebsOnSecurity that the breach first started in one of Oracle's major point-of-sale data centers — specifically the company's large data center in Manassas, Va.

According to my source, that particular center helps large Oracle hospitality industry clients manage their fleets of MICROS point-of-sale devices.

"Initially, the customer's network and the internal Oracle network were on the same network," said my source, who spoke under condition of anonymity because he did not have permission

from his employer to speak on the record. “The networking team did a network segmentation of these two networks — ironically for security purposes. However, it seems as if what they have done actually allowed access from the Russian Cybercrime group.”

My source said that in mid-July 2016 Oracle sent out an email alert to employees of its hospitality division that they had to re-image their laptops without backing anything up.

“All of the files and software that were on an employee’s computer were deleted, which was crippling to business operations,” my source recalled. “Project management lost all their schedules, deployment teams lost all the software that they use to install on customer sites. Oracle did not tell the employees in this email that they got hacked but just to re-image everything with no backups. It seems as if Oracle did a pretty good job sweeping this incident under the rug. Most employees don’t know about the hack and it hasn’t been a huge deal to the customers. However, it is estimated that this cost them billions, so it is a really major breach.”

I sent Oracle a litany of questions based on the above, but a spokesperson for the company said Oracle would comment on none of it.

= Indicators =

104.156.240.212
104.232.35.136
104.250.153.57
107.181.246.211
107.181.250.221
108.61.57.43
128.177.144.59
144.168.45.128
151.80.8.10
162.212.105.78
172.28.202.31
184.22.81.68
185.29.9.28 (c)
185.86.149.115
185.86.149.60
186.106.120.113
190.82.81.132
194.146.180.58
195.154.43.52
198.23.210.156
207.182.98.21
208.167.254.234
209.51.131.190
216.155.131.74
216.170.116.120
220.130.157.99
23.227.196.99
23.249.164.109
31.131.17.128
45.63.23.135

45.63.96.216
5.45.179.185
5.45.192.117
51.254.95.100
51.254.95.99
59.55.142.171
60.228.38.213/login.aspx
66.232.124.175
71.63.154.49
72.233.55.10
74.125.39.18
80.83.118.240
80.83.118.245
82.163.78.188
83.183.76.156
85.186.125.217
86.55.7.54
87.236.210.109
87.236.210.116
87.98.153.34
91.207.60.68
94.140.120.133
95.215.44.136
95.215.45.228
95.215.45.64
95.215.45.69
95.215.45.90
95.215.45.98
95.215.46.2
95.215.46.32
95.215.46.76
95.85.12.179
98.129.249.174
clients14-google.com
mail.clients12-google.com
ns1.stats1-google.com
ns2.stats1-google.com
wambiri.net/login.aspx