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.

About Oracle MICROS

Oracle MICROS offers a range of software, hardware and related services, including point-of-sale systems (POS) along cloud solutions to manage hotels, food and beverage facilities, and retailers. According to Oracle Micros, MICROS' technologies are in use across 330,000 customer sites in 180 countries.

Oracle Customer Notification

According to media sources, Oracle Security provided a notification to Oracle MICROS customers on 8 August 2016, informing them of the following:

- Oracle Security has detected and addressed malicious code in certain legacy MICROS systems
- Oracle has confirmed that it's investigating a breach of its Micros division.
- Oracle's own systems, corporate network, and other cloud and service offers were not impacted.
- Oracle MICROS users will have to change their account passwords immediately
- The company reportedly stated that payment data was not at risk, as that information is encrypted both at rest and in transit in the MICROS environment.

Although Oracle has not provided additional details on the exact date or extent of the breach of Oracle MICROS, some media reports suggest that the support portal for MICROS clients was also compromised.

1. Cybercrime threats to Oracle MICROS

Visa is aware of two cybercrime threats, “Carbanak” and “MalumPOS”, which have previously targeted Oracle systems. Indicators of compromise (IOCs) associated with both Carbanak and MalumPOS are provided in section two [2] of this report.

Carbanak

On 8 August 2016, a media source reported that the “Oracle’s MICROS customer support portal was seen communicating with a server known to be used by the “Carbanak.”

According to Kaspersky Lab, in February 2015, the Carbanak group used techniques commonly seen in Advanced Persistent Threat (APT) incidents to successfully target one financial institution’s (a bank) money processing services, Automated Teller Machines (ATM) and financial accounts. In some cases, Oracle databases were manipulated to open payment or debit card accounts at the same bank or to transfer money between accounts using the online banking system. The ATM network was also used to dispense cash from certain ATMs at certain times where money mules were ready to collect it as part of this operation.

In March 2015, Visa provided an industry-wide public alert and mitigation guidance concerning Carbanak. Visa recommends that all financial institutions and retailers scan their networks for the presence of Carbanak. If detected, please contact law enforcement immediately and activate security incident procedures.

MalumPOS

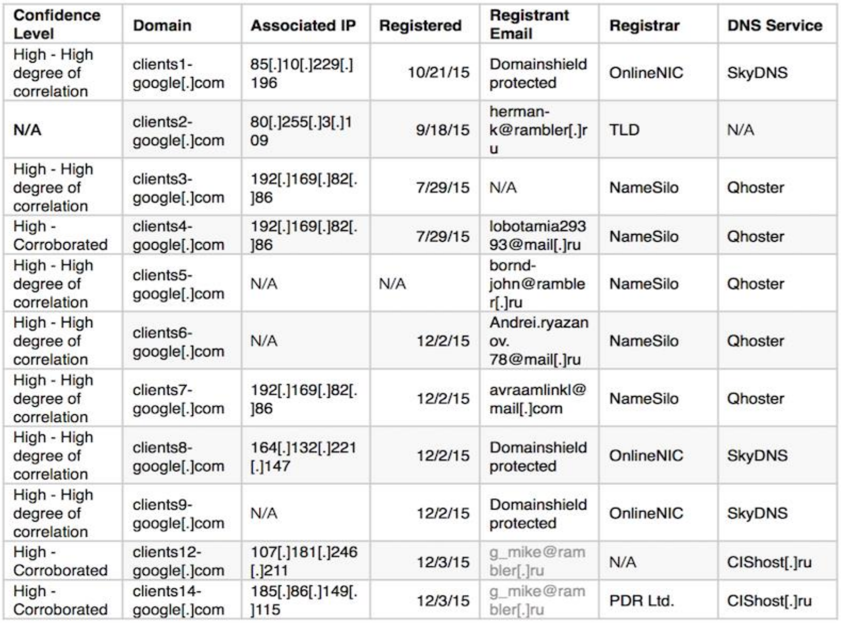
Discovered by TrendMicro in 2015, MalumPOS is known to specifically target Oracle MICROS point-of-sale devices. MalumPOS is described as simple and non-obfuscated malware, written in the Delphi programming language. Visa is aware that MalumPOS is still actively used by cyber criminals.

2. Mitigation action recommended for Oracle Micros Customers

- Change passwords for any account used by a MICROS representative to access the customer's on-premises systems.
- Scan network for the following:
  - Psexec file
  - Files with .bin extension (located in \All users\%AppData%\Mozilla\ or c:\ProgramData\Mozilla\)
  - Svchost.exe file (located in Windows\System32\com\catalogue\)
  - Svchost.exefile (located in C:\ProgramData\Mozilla\svchost.exe)
    - This file provided remote access functions, such as the ability to execute arbitrary commands, upload/download files.
  - Operating system (Windows) running services ending in "sys"

- 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	ClShost[.]ru
High - Corroborated	clients14-google[.]com	185[.]86[.]149[.]115	12/3/15	g_mike@rambler[.]ru	PDR Ltd.	ClShost[.]ru

- Scan networks for IOCs linked to MalumPOS:

File Name	File Name	Description
Mnv.exe	757ae5eed0c5e229ad9bae586f1281b5de053767	Oracle Forms process, MICROS 9700 VISAD Driver
Nvsvc.exe	2cf2f41d2454b59641a84f8180fd7e32135a0dbc	MICROS 9700 SSL GW
Nvsvc.exe	f728bf7d6dbfc4c7bea21d6a3fd0b88f4fe52a4a	Oracle Forms process, Web-based PoS systems
Nvsvc.exe	798bc2d91293c18af7e99ba7c9a4fd3010051741	Accessed through MicrosoftTM, Windows Internet Explorer, Shift4 Corporation Universal
Nvsvc.exe	90e85b471b64667dbcde3aee3fa504c0d4b0ad35	Transaction Gateway, PAR Springer-Miller Systems
Rdp.exe	fe713f9bb90b999250c3b6a3bba965d603de32a3	Looks like a test
Winini.exe	d0b3562d868694fd1147e15483f88f3a78ebedfb	Client stub

- Additionally, Visa recommends the following best practices to reduce the risk of exposure:
  - Educate employees how to avoid phishing scams and opening emails with attachments
  - Maintain updates for all software and patches (address zero day vulnerabilities)
  - Turn on heuristics (behavioral analysis) on anti-malware to search for suspicious behavior

Visa will continue to report any mitigation guidance, technical indicators of compromise associated with this compromise, or additional details on the overall extent of the compromise as details are made available.

For questions and information please contact, **paymentintelligence@visa.com**

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- U.S. and Canada: USFraudControl@visa.com