KPMG Cárdenas Dosal, S.C.
Manuel Ávila Camacho 176 P1,
Reforma Social, Miguel Hidalgo,
C.P. 11650, Ciudad de México.
Teléfono: +01 (55) 5246 8300
kpmg.com.mx

February 22, 2019

INTERIM INCIDENT REPORT

The following is KPMG Cárdenas Dosal S. C.'s (KPMG Mexico) interim report regarding the information security incident (Incident). Our investigation is ongoing, and a final Incident Report will be provided as soon as possible.

Incident Summary

KPMG Mexico, the Mexican member firm of KPMG International (KPMGI) was engaged to provide certain tax services to a number of clients in Mexico (Tax Services). In connection with the Tax Services, KPMG Mexico received credentials to access the website of the Servicio de Administración Tributaria (Mexican Tax Authority) and downloaded information (Information) required to perform the Tax Services. The Tax Services and the associated deliverables are not impacted by the Incident.

Over a period from November, 2018 to January, 2019, a small group of KPMG Mexico personnel working in the firm's tax technology group on the development of tax tools (Small Group) violated the firm's strict information protection and security policies by downloading and placing the Information in a database on a virtual machine in an Azure cloud environment with default settings. The database, virtual machine, and Azure cloud environment they were in, were all unauthorized under KPMG's policies and are collectively referred to as the Unauthorized Environment. ***The Unauthorized Environment was <u>not</u> part of KPMG Mexico's authorized Azure environment and was <u>not</u> connected in any way to any KPMG Mexico or any other KPMG member firm technology infrastructure.***

On January 30, 2019, KPMG Mexico Information Security and its Office of General Counsel learned of the existence of the Unauthorized Environment and the fact that it had been entered by at least one intruder. It is important to re-emphasize that the database that was hosted and compromised in the Unauthorized Environment was installed with default settings, which resulted in it being accessible without a password to anyone on the Internet. Thus, we believe it was likely easily detected through scanning software commonly used by many. For the same reason, we believe that any intruders were not targeting KPMG Mexico and that the intrusion was simply opportunistic.

KPMG Cárdenas Dosal, S.C.
Manuel Ávila Camacho 176 P1,
Reforma Social, Miguel Hidalgo,
C.P. 11650, Ciudad de México.
Teléfono: +01 (55) 5246 8300
kpmg.com.mx

On January 29, 2019, upon being contacted by another KPMG client who had been contacted by a blogger about the Incident, the Small Group then deleted the Unauthorized Environment – again, without authorization. Thus, it is unfortunately not possible, through recovery processes, to determine precisely what information was in the Unauthorized Environment or which information is potentially in the possession of any unauthorized third party. It is also not possible to determine precisely what Information, if any, was taken.

Through interviews with the Small Group, KPMG Mexico learned that Azure Blob storage was used as a staging area for data loaded into the MogonDB in the Unauthorized Environment. Since the contents of the compromised MongoDB database were deleted, but the Azure Blob storage was not deleted, KPMG Mexico has made the assumption that any data found in the Azure Blob could have been potentially loaded into the MongoDB and thus is the potential data set that might have been exposed. KPMG has therefore offered all potentially affected employees of clients whose information could have been in the Unauthorized Environment the monitoring services provided by Experian Information Solutions, Inc.

An investigation of this Incident was immediately launched, and comprehensive remedial measures are underway. KPMG Mexico and all of the KPMG network are deeply committed to the protection of client information, which is a fundamental and critically important professional obligation. We profoundly regret that the Incident occurred and are committed to working with you to mitigate any of the consequences of it.

More specific information about the Incident follows.

Timeline of Events

November 2018 – January 2019	Small Group downloaded Information in XML format from Mexico Tax Authority and initially stored the XML files in Azure Blob Storage.
December 1, 2018	As determined by the logs received from Microsoft, MX developers began the build of the Unauthorized Environment using a trial subscription that comes with Visual Studio. The Unauthorized Environment was not part of KPMG Mexico (or any other KPMG Firm) technology infrastructure / network. In that environment, they installed the Unauthorized Environment database. The Unauthorized Environment was not installed securely. A default installation was used.
December 18, 2018 – December 22, 2018	The Small Group initially stored the XML files in an unauthorized Azure Blob Storage and then uploaded them to the Unauthorized Environment.

KPMG Cárdenas Dosal, S.C.
Manuel Ávila Camacho 176 P1,
Reforma Social, Miguel Hidalgo,
C.P. 11650, Ciudad de México.
Teléfono: +01 (55) 5246 8300
kpmg.com.mx

January 21 , 2019	The KPMG Mexico security team began security testing of the application named Plataforma Fiscal, developed by the Small Group. Testing included only the application associated to the database and not the database itself, as the security team was not aware of the existence of the MongoDB.
January 22, 2019	An external 'security researcher' named Bob Diachenko claimed to have discovered the insecure MongoDB in the Unauthorized Environment using Shodan.io (a vulnerability search engine). He emailed one of the affected KPMG clients (Please see Ex. 1.)
January 23, 2019	A ransom note was placed in the Unauthorized Environment, stating that the information was taken. (Please see Ex. 2.) The note demanded 0.5 Bitcoin (cryptocurrency) in exchange for the return of the information.
January 23, 2019	The 'security researcher' posted a tweet, this time reporting that cyber criminals wiped the data from the MongoDB database in the Unauthorized Environment and that the database included Comprobante Fiscal Digital por Internet / Digital Tax Receipt by Internet) and PII information.
January 28, 2019	The 'security researcher' posted another tweet, this time listing 41 companies which had payroll invoices in the Unauthorized Environment.
January 29, 2019	The 'security researcher' copied INAI (Mexican Privacy Authority - @INAIMexico) on the tweet with the 41 exposed entities. (Please see Ex.3) Note: as of February 20, there has been no contact from INAI
	The 'security researcher' posted log entries as evidence of the data having been deleted from the database.
	KPMG Mexico client emailed an individual in the Small Group, asking questions about the tweet of the security researcher.
	Without authorization, the Small Group deleted the Unauthorized Environment.
January 30, 2019	Development team director (Frankys Baez) and partner in charge of the development team (David Ricardez) notified Alejandra Flores (MX NITSO) regarding the Incident.
January 30, 2019	The 'security researcher' posted that someone other than him has identified the owner of the Unauthorized Environment and that the information will be released by him in a report. Note: As of February 22, 2019, no such report has materialized.

KPMG Cárdenas Dosal, S.C.
Manuel Ávila Camacho 176 P1,
Reforma Social, Miguel Hidalgo,
C.P. 11650, Ciudad de México.
Teléfono: +01 (55) 5246 8300
kpmg.com.mx

February 1, 2019	KPMG Mexico lodged a criminal complaint to the Ministerio Público regarding the Incident.
	Through interviews with the database administrators / developers, the investigation team learned that there was never a backup of the MongoDB until January 29, 2019. They attempted to recover the database from a backup the developers had created. Once the backup was restored, it contained only information inserted in the database after the deletion.
February 5, 2019	KPMG also asked Microsoft for restoration of the Unauthorized Environments, backed-up logs or any available artifacts. KPMG US engaged Microsoft to see if they could provide help to recover what was deleted and/or provide logs to help with forensic analysis. Microsoft was unable to do so and did not have any security logs.
	The 'security researcher' reiterates that he will release a report but contradicts an earlier posting by writing in this posting that the owner of the database is still unknown.
February 15, 2019	Microsoft provided Azure Resource Manager (ARM) logs which were not helpful with the identification of the threat actor. However, since they are operational logs, they did show the actions associated with the environment being deleted.

Investigation Findings

The investigation is ongoing. Preliminarily, it has been determined that without the knowledge of KPMG Mexico Information Security, the Small Group proceeded with using Azure trial subscriptions, despite Information Security having previously denied authorization to do so.

The Small Group used the certificates and passwords to download client data from the Tax Authority site into the Unauthorized Environment as described above. On some occasions, the Small Group obtained the certificates and passwords directly from the clients. The data should have been downloaded through KPMG's secure network access onto a secure KPMG approved server. Instead, the Small Group downloaded to the Unauthorized Environment without the knowledge of KPMG Information Security and in direct contravention of Information Security's prior direction. All of these actions were very serious policy violations.

Remedial Measures taken and Preventive Steps Going Forward

Two of the members of the Small Group have been separated from the Firm. The rest of the members of the Small Group have been suspended from their functions and are awaiting further disciplinary action pending the results of the investigation.

KPMG Cárdenas Dosal, S.C.
Manuel Ávila Camacho 176 P1,
Reforma Social, Miguel Hidalgo,
C.P. 11650, Ciudad de México.
Teléfono: +01 (55) 5246 8300
kpmg.com.mx

KPMG Mexico is embarking on an enhanced training and communication program to remind all firm personnel regarding the firm's information protection and security policies, procedures and protocols and the penalties for non-compliance.

KPMGI issued a communication for distribution through the network of member firms, reiterating the importance of effectively managing the risks of using cloud environments and following approved processes and procedures to do so in a secure manner.

KPMG has begun efforts to identify potentially unauthorized instances of Azure usage by reviewing employee corporate credit card transactions. KPMG has also engaged with Microsoft to gather an inventory of existing Azure environments attributed to KPMG. This will be provided to member firms to support local cloud usage monitoring efforts.

KPMG Mexico will work with KPMGI's Information Protection Group (IPG) to conduct an after-action exercise and produce a report to review current practices and develop recommended actions for improvement within the next 90 days.

Conclusion

In conclusion, we reiterate our profound disappointment in the Small Group's actions, which were again, completely contrary to KPMG's information protection and security policies and practices, and our deep regret that it affected you and your employees. We are committed to continuing to work with you so that all of your concerns are addressed fully and promptly.

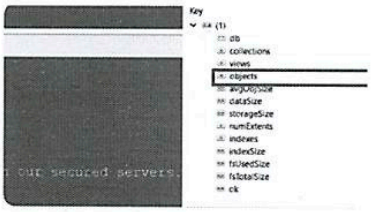
KPMG Cárdenas Dosal S. C. (KPMG Mexico)

Appendix - Exhibits

KPMG Cárdenas Dosal, S.C.
Manuel Ávila Camacho 176 P1,
Reforma Social, Miguel Hidalgo,
C.P. 11650, Ciudad de México.
Teléfono: +01 (55) 5246 8300
kpmg.com.mx

So, it took cyber criminals only 2 days to find and wipe out an unprotected MongoDB with almost 5 Million records of Mexican electronic invoices (CFDI), with a lot of PII involved. Data seemed to be managed by yet-unknown provider, with some big companies on board...

Traducir Tweet



23/01/19 8:23

Exhibit 1. Bob Diachenko tweet

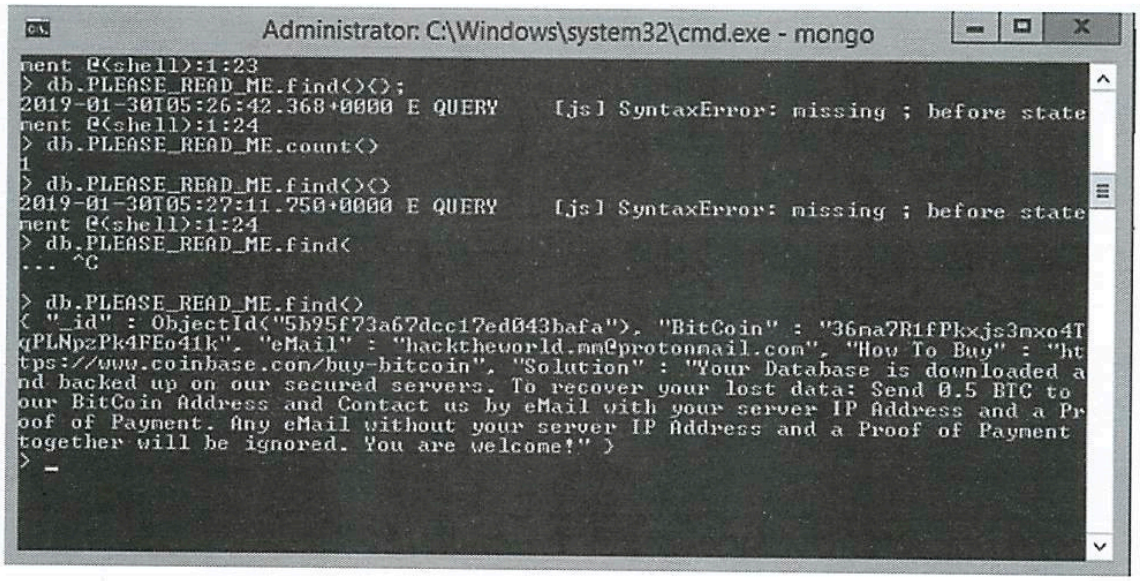


Exhibit 2. Ransom message

https://twitter.com/MayhemDayOne/status/1089931008173060097

KPMG Cárdenas Dosal, S.C.
Manuel Ávila Camacho 176 P1,
Reforma Social, Miguel Hidalgo,
C.P. 11650, Ciudad de México.
Teléfono: +01 (55) 5246 8300
kpmg.com.mx

Exhibit 3. Tweet to INAI by Bob Diachenko