السيد // مدير مكتب النائب العام

بعد التحية,,,

بالإشارة إلى البلاغ المقدم من السيد مدير عام مصرف الصحارى والمقيد بسجل الوارد العام (7097-2024م) والذي كان مفاده تعرض الموقع الإلكتروني الخاص بالمصرف لواقعة إختراق من قبل أحد عناوين (بروتوكلات الإنترنت IP) التابعة لمكاتب شركة الجيل (أحد مزودي خدمة الإنترنت في البلاد) وطلب فدية مالية قدرها (100.000$ مائة ألف دولار) نظير عدم نشر بيانات زبائن المصرف وكما أوضح بأن المنظومة المصرفية وحسابات الزبائن لم يتم المساس بها بأي شكل من الأشكال .

عليـــــــه

وبعـــــد مباشرة أعمال الإستدلال الفني والعمل على تضييق دائرة الإشتباه لمعرفة مستخدم العنوان الإلكتروني IP ساعة حدوث الواقعة وكذلك حصر الأضرار التي أحدثتها واقعة الإختراق ومسبباتها .. إستخلصنا الآتي:-

- بعد التواصل مع السيد نائب رئيس مجلس إدارة شركة العنكبوت الليبي (الشركة المضيفة لموقع المصرف محل الواقعة) أتضح أنه من خلال تسجيلات الدخول على هذا الموقع الإلكتروني تبين وجود رقم بروتوكول الإنترنت IP (165.16.16.60) الخاص بمقر شركة الجيل الجديد بمدينة بنغازي شارع دبي .
- رقم الـIP (165.16.16.60) هو أحد أرقام بروتوكولات الإنترنت الخاصة بشركة الجيل الجديد مكتب بنغازي والذي يستخدمه جُل من يلج إلى خدمة الإنترنت بالمبنى , وبالتواصل مع السيد البراء خليفة ابديري مدير عام الشركة سالفة الذكر أفاد بعدم إمكانية تحديد الجهاز المستخدم في الواقعة إلا أنه أمدنا بسجل الحضور والإنصراف داخل مكتب بنغازي لليوم الذي يُشتبه فيه حدوثها .

العنوان : المقر الرئيسي / مجمع المحاكم، طرابلس - ليبيا
ص.ب : 82064 www.attorneygeneral.gov.ly - E-mail: info@lago.ly - P.O.Box: 82064

- ولمعرفة الأضرار التي نجمت عن واقعة الإختراق والأمر الذي سهل حدوثها تبين حصول مرتكب الواقعة على بيانات شخصية لعدد (30990 ثلاثون ألف وتسعمائة وتسعون) من زبائن المصرف وهذه البيانات متمثلة في (الإسم - الرقم الوطني - أرقام الهواتف - رقم جواز السفر - رقم بطاقة الأغراض وتاريخ إنتهاء الصلاحية) .
- من أهم أسباب حدوث هذه الواقعة هو إنشاء صفحة داخل موقع المصرف بإستخدام برمجيات غير آمنة متمثلة في (WordPress) , والذي أفاد السيد صلاح أبو حمرة مدير إدارة أمن المعلومات بالمصرف أنها أنشئت بغير علمه و لا بالرجوع إلى إدارته , حيث أنشئت من قبل فريق مكتب التواصل بالمصرف , وقام المذكور سلفاً بمدنا بنسخة من تقريره الفني حول الواقعة .

نـــرى بمخاطبة السيد مدير نيابة مكافحة جرائم الفساد بنغازي لوجود محضر إستدلال بالواقعة تم إحالته من قبل إدارة مكافحة الجرائم الاقتصادية وغسل الأموال .

والســـلام

نائـــب النيابـــة//
عمـــر محمد اسكيليـــح
«رئيس قسم ضبط شؤون المعلوماتية والاتصالات»

صورة منه الى
السيد /المستشار النائـــب العـــام/للعلم
الملـــف الدوري العـــــام/ للحفظ
..04_____2024/07/28م

العنوان : المقر الرئيسي / مجمع المحاكم، طرابلس - ليبيا
ص.ب : 82064 www.attorneygeneral.gov.ly - E-mail: info@lago.ly - P.O.Box: 82064

مصرف الصحارى

Website: WWW.SAHARABANK.LY

تقرير حادثة اختراق الموقع الالكتروني

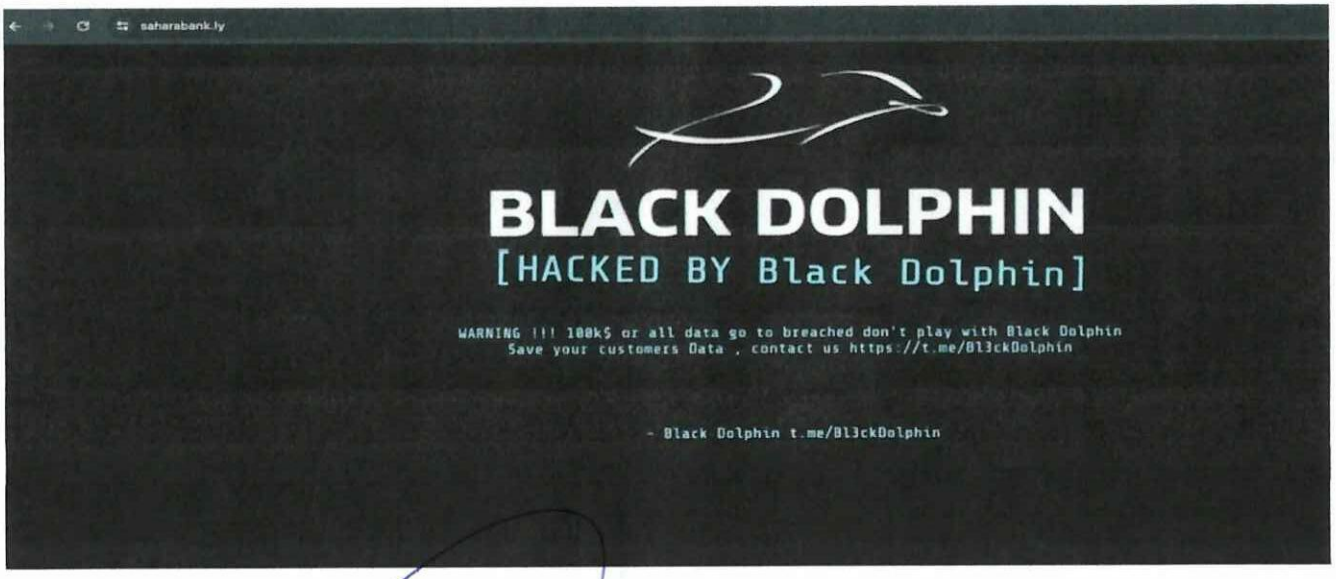
مصرف الصحارى
SAHARA BANK

صلاح ابوحمرة
مدير إدارة امن المعلومات
EMAIL: SALAH.ABUHAMRA@SAHARABANK.LY

المحتويات

نظرة عامة على الحادثة

يمتلك مصرف الصحارى موقعاً الكترونيا مستضاف من قبل شركة العنكبوت الليبي، يستخدم هذا الموقع من اجل نشر الأخبار و معرفة شكاوى الزبائن و مؤخرًا تم استعمال الموقع كقاعدة بيانات مستقلة عن المنظومة المصرفية من اجل تسريع عملية مطابقة بيانات الأغراض الشخصية 4000$ وبدون علم من إدارة امن المعلومات، وفي يوم الثلاثاء وعند حوالي الساعة 12:00 صباحا الموافق 7-5-2024 اعلن أحد المخترقين قيامه بالدخول الى موقع المصرف و السيطرة عليه وعلى إثرِ هذه الادعاءات قام فريق امن المعلومات بالدخول الى الموقع حيث وجدنا الصورة ادناه :



الخطوات المتبعة على الحادثة ومستوى الضرر

- توجه الفريق الى مدينة بنغازي وعلى معطيات التقرير تم توجيه بلاغ رسمي من قبل السيد مساعد مدير ادارة الفروع للمنطقة الشرقية الي إدارة مكافحة الجرائم الاقتصادية وغسيل الأموال (الجهة الأمنية المعنية بالبلاغ) وكذلك أخذ الاقوال من قبل الفريق المكلف من ادارة امن المعلومات بشأن التبليغ عن الواقعة.
- تم إضافة الأدلة الجنائية الرقمية للمحضر الجنائي الخاص بالواقعة وارفاق تقرير مفصل يوضح عنوان المهاجم وكذلك وقت وتاريخ الهجوم.
- تم متابعة اجراء التحقيقات اللازمة بالخصوص من قبل الجهات الامنية المعنية.

وحسب ما تم افادتنا به شفويا من قبل السيد مدير ادارة مكافحة الجرائم الاقتصادية وغسيل الأموال بمدينة بنغازي انه قد تم زيارة مقر شركة الجيل الجديد بمدينة بنغازي ومن خلال تقريرهم بعد جمع الادلة تبين أن الشبكة الخاصة بشركة الجيل الجديد بها ثغرات امنية عديدة كما يوجد اجهزة حاسوب داخل الشبكة تم تنزيل برامج خبيثة ليتم استغلالها في عملية الهجوم والوصول الي اجهزة وخوادم عديدة وانه لا يوجد جدار حماية للشبكة الخاصه بشركة الجيل الجديد مما يؤكد عملية الهجوم من قبل الشركة على الخوادم الخاصة بموقع المصرف والمستضافة لدي شركة العنكبوت.

الخطوات المتبعة على الحادثة ومستوى الضرر

قام الفريق أولا بعد التأكد من الواجهة الموجودة في الشكل أعلاه بالخطوات التالية: -

1- تمت إعادة السيطرة على الموقع الالكتروني للمصرف في حوالي 3 دقائق منذ اكتشاف واقعة الهجوم

2- تم قطع النشر الخاص بالموقع حتى يتم التأكد من الملفات الموجودة على الموقع.

3- تم نسخ سجلات الدخول و سجلات التعديلات على الموقع ليتم تحليلها لاحقا.

4- توجه الفريق في اليوم التالي الى شركة العنكبوت الليبي وتم طلب سجلات الأحداث منهم وقد تم افادتنا بعدم توفر السجلات المطلوبة من قبلهم لعدم قدرتهم على التحليل الجنائي (**Forensic Analysis Event**) للأحداث.

تبين من خلال متابعة الملفات ان عملية الاختراق قد تمت فعلا على الموقع ولكن بدون معرفة موقع الدخول او المستوى الذي وصل إليه المخترق، لاحظ الفريق وجود قاعدة بيانات ليس لإدارة امن المعلومات علم بها وتحتوي على 30990 بيانات زبون والمتضمنة داخلها (اسم، رقم وطني، ارقام هواتف، رقم جواز، رقم بطاقة الأغراض ، و تاريخ انتهاء الصلاحية) .

5- قاعدة البيانات التي تم اضافتها الي الموقع لم يكن عليها أي آثار تشفير او تلف.

وعلى اثر هذه المعلومة قامت إدارة امن المعلومات بطلب تحليل رقمي جنائي من شركة سايبرتيك (**Cybertech**) الشركة المسؤولة عن مشروع تقييم الثغرات الأمنية بالمصرف .

ومن خلال التحليل الجنائي الرقمي تبين أن المخترق قام بالدخول عن طريق صفحة يملكها المصرف على **WordPress** مرتبطة بعنوان فرعي **Lb.saharabank.ly** ومنها تمكن من اختراق الخادم الخاص بالاستضافة لدي شركة العنكبوت الليبي ورفع فيروسات على النظام مكنته من الحصول على وصول غير مشروط للنظام وتغيير الاكواد الخاصة به .

أكد الفريق على ان المخترق تمكن من الحصول على كافة المعلومات الموجودة لعدم وجود تشفير على قاعدة البيانات داخل الموقع.

ومن خلال التحليل تبين ان العنوان الشبكي المسؤول عن الهجوم (165.16.16.60) وهذا العنوان مخصص لطرف شركة الجيل الجديد بمكتب بنغازي وبناء على ذلك قام الفريق بالآتي:

الأسباب الرئيسية لعملية الإختراق: -

1- وجود صفحة قام فريق من مكتب التواصل اعدادها على الWordPress بدون علم إدارة امن المعلومات و اخذ الموافقات اللازمة (يعتبر ال **WordPress** من اكتر البيئات المملؤة بالثغرات).

2- تستخدم شركة العنكبوت الليبي المستضيفة للموقع جدار ناري مشترك مع مستخدميها بدائي ومفتوح المصدر وغير قادر على مواكبة تطورات الفيروسات.

3- لا يحتوي الخادم المقدم من شركة العنكبوت على نظام حماية من الفيروسات اطلاقا مما سهل على المهاجم رفع الملفات دون اكتشافها.

4- عدم تحديث البيانات من قبل فروع المصرف وعدم وجود البيانات الكافية في المنظومة المصرفية لزبائن المصرف والتي تسهل في عملية مطابقة البيانات لمنظومة الأغراض الشخصية بمصرف ليبيا المركزي

5- مماطلة بعض الإدارات والاشخاص في عملية الربط لمنظومة مصرف ليبيا المركزي والذي يعد سبب كافي لإيجاد حلول بديلة والغير آمنة من قبل إدارة المصرف وذلك لتسهيل إجراءات المطابقة لزبائن المصرف

6- تأخر تنفيذ المشروع المقترح والمقدم من إدارة أمن المعلومات (مشروع منع تسرب البيانات (**DLP**) بالرغم من تقديمها منذ حوالي سنة للجنة المشتريات والمماطلة في طرح العطاء او شراء هذا النظام من قبل لجنة المشتريات

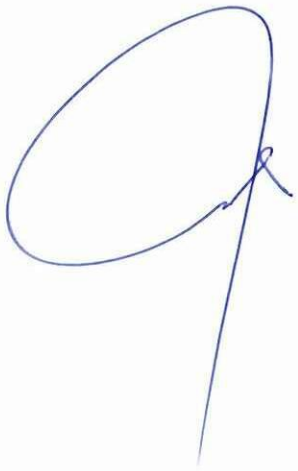
كيف كان التعافي من الحادثه :-

1- تم ترقية النظام الخاص بالخادم المقدم من قبل شركة العنكبوت الليبي.

2- إعادة تصميم الموقع.

3- إيقاف عمل البطاقات الخاصة بالمصرف عن العمل في عمليات الشراء عن طريق الإنترنت بتعليمات مباشرة من إدارة امن المعلومات.

4- تنصيب مضاد فيروسات على الخادم لضمان عدم وجود أي ملفات ضارة.



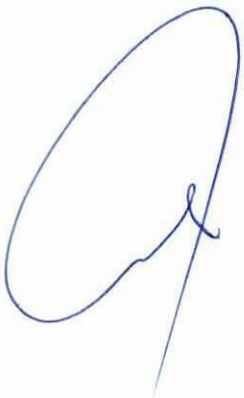
ملخص

إن الاحداث الخاصة بالاختراق كانت نتيجة انشاء صفحة داخل موقع لا يخلو من الثغرات وعرضة للهجمات (WordPress)

وتمت إضافتها دون علم وموافقة من إدارة امن المعلومات او الاطلاع الدائم، وأن قاعدة البيانات التي قد تم رفعها الى الموقع عن

طريق مكتب التواصل حسب تعليمات من لجنة مطابقة بيانات منظومة الأغراض الشخصية المكونة من قبل المدير العام لم تكن

مشفرة , ولم تطلع إدارة امن المعلومات على طريقة استخراج قاعدة البيانات والأشخاص المخولين بها



التوصيات

من خلال واقعة الهجوم الالكتروني وللأحداث التي كانت سببا في الهجوم وأدت الي تسرب البيانات الخاصة بزبائن المصرف مما كان لها الأثر الكبير على سمعه المصرف وللحد من هذه الهجمات الإلكترونية فإننا نوصي بالآتي: -

1. نقل خوادم استضافة الموقع لدي شركة العنكبوت الليبي الي المصرف وتجهيز البيئة الملائمة لذلك مع أخد الاحتياطات الأمنية اللازمة أثناء التنفيذ.
2. نقل تبعية إدارة الموقع الالكتروني (تصميم، تنفيد، إشراف) الي إدارة امن المعلومات
3. نظرا لكثرة استهداف المواقع والخدمات الالكترونية ولتطور البرامج الخبيثة التي تؤدي الي تشفير البيانات وطلب فدية من قبل المخترقين نوصي بتنفيذ **(DELL Power Protect and Cyber Recovery)**على بيانات المنظومة المصرفية والتأكد من سلامة كافة البيانات الخاصة بالنسخ الاحتياطية .
4. الإسراع في تنفيذ جميع المشاريع المقترحة والمقدمة من إدارة أمن المعلومات والتي تم احالتها الي لجنة المشتريات وبالأخص مشروع منع تسرب البيانات**DLP** وغيرها من المشاريع الأمنية.
5. إلزام جميع إدارات المصرف بعدم إضافة او تعديل داخل البيئة الخاصة بالمصرف الابعد الرجوع الي إدارة امن المعلومات.
6. التقيد والالتزام بجميع المناشير والتعليمات الصادرة من إدارة امن المعلومات.

اعتماد

إدارة امن المعلومات

مصرف الصحاري SAHARA BANK إدارة أمن المعلومات

حضور وانصراف العاملين بمنطقة الاتصالات الشرقية يوم 17/04/2024

الرقم الشخصي	الاسم الأول	المنصب	القسم	التاريخ	ايام الاسبوع	استثناء	وقت تسجيل الدخول	وقت تسجيل الخروج
000000146	عمر عبدالوهاب أحمد	مهندس شبكة نقل البيانات	فريق نقل البيانات	2024-04-17	الأربعاء		08:01	14:30
000000200	بكار الصالحين بكار	رئيس قسم التشغيل و الصيانة - المنطقة الشرقية	رؤساء الأقسام - المنطقة الشرقية	2024-04-17	الأربعاء		07:43	13:01
000000201	توفيق عمر عوض عثمان	رئيس وحدة عمليات الشبكة	رؤساء الوحدات - قسم التشغيل والصيانة	2024-04-17	الأربعاء		08:08	13:00
000000209	خالد عبدالله محمد	رئيس وحدة توزيع الخدمات	رؤساء الوحدات - قسم التشغيل والصيانة	2024-04-17	الأربعاء		08:03	13:15
000000372	صالح محمد امقاوي	سائق	وحدة الخدمات	2024-04-17	الأربعاء		08:24	13:21
000000441	زهير أحمد محمد	رئيس وحدة تقنية المعلومات	رؤساء الوحدات - قسم التشغيل والصيانة	2024-04-17	الأربعاء		08:58	14:03
000000446	أنيس مصطفى إدريس	مهندس شبكة تراسل	فريق شبكة التراسل	2024-04-17	الأربعاء	تبرير تأخير	10:03	13:00
000000448	أحمد عبد الناصر ناصر	مهندس شبكة النفاذ التجميعي	وحدة توزيع الخدمات	2024-04-17	الأربعاء		08:46	13:00
000000450	أسامة مفتاح العربي	رئيس فريق شبكة التراسل	وحدة شبكات النقل	2024-04-17	الأربعاء	تبرير تأخير	09:32	13:05
000000451	سراج صلاح الدين محمد	رئيس وحدة تنفيذ المشاريع	منطقة الإتصالات الشرقية	2024-04-17	الأربعاء		09:00	13:03
000000452	عبد الغفار علي مفتاح	مهندس قوى	فريق القوى والتكييف	2024-04-17	الأربعاء		08:45	13:01
000000461	فرج مفتاح فرج	رئيس قسم الموارد البشرية و المالية	رؤساء الأقسام - المنطقة الشرقية	2024-04-17	الأربعاء		08:53	13:03
000000464	وليد علي محمد	ملاحظ أمن وسلامة	وحدة الخدمات	2024-04-17	الأربعاء		08:01	08:56
000000523	حمزة علي عبدالقادر	رئيس القسم التجاري	منطقة الإتصالات الشرقية	2024-04-17	الأربعاء		08:51	13:01
000000534	عبد المجيد محمد	رئيس وحدة شبكات النقل	رؤساء الوحدات - قسم التشغيل والصيانة	2024-04-17	الأربعاء		08:57	13:01
000000553	فرج مساعد جبريل	أمين سر	منطقة الإتصالات الشرقية	2024-04-17	الأربعاء		08:57	16:14
000000558	عثمان سالم عثمان	فني تركيبات وأعمال مدنية	فريق الكوابل والتركيبات	2024-04-17	الأربعاء		08:18	13:01
000000559	مفتاح خليفة امحمد	رئيس فريق الكوابل والتركيبات	وحدة عمليات الشبكة	2024-04-17	الأربعاء	تبرير تأخير	09:06	13:05
000000569	المهدي عبد اللطيف أدم	رئيس قسم الموارد البشرية و المالية	رؤساء الأقسام - المنطقة الشرقية	2024-04-17	الأربعاء	تبرير تأخير	09:09	13:17
000000577	محمد سلامة محمد فرج	مهندس قوى	فريق القوى والتكييف	2024-04-17	الأربعاء		08:47	13:23
000000599	عبد المالك عثمان فرج	مهندس شبكة نقل البيانات	فريق نقل البيانات	2024-04-17	الأربعاء	تبرير تأخير	09:07	13:09
000000617	مجد الدين أحمد	مهندس شبكة تراسل	فريق شبكة التراسل	2024-04-17	الأربعاء	تبرير تأخير	10:01	13:28
000000618	محمد ميلاد امراجع	مهندس شبكة النفاذ التجميعي	وحدة توزيع الخدمات	2024-04-17	الأربعاء		08:54	13:02
000000619	محمد يوسف امريض	مهندس شبكة تراسل	فريق شبكة التراسل	2024-04-17	الأربعاء	تبرير تأخير	09:08	13:31
000000623	حسن موسي محمد	موظف خدمات	وحدة الخدمات	2024-04-17	الأربعاء	تبرير تأخير	09:04	13:11
000000637	محمد امهيدي امراجع	رئيس فريق القوي و التكييف	وحدة عمليات الشبكة	2024-04-17	الأربعاء		08:16	13:00
000000639	فرج صلاح حمد	محاسب	وحدة الحسابات والمالية	2024-04-17	الأربعاء		08:56	13:00
000000682	علي احمد السنوسي	فني تركيبات وأعمال مدنية	فريق الكوابل والتركيبات	2024-04-17	الأربعاء	تبرير تأخير	10:03	13:04
000000683	فائز مختار عبد الرزاق	موظف خدمات	وحدة الخدمات	2024-04-17	الأربعاء		08:46	13:00
000000703	محمد ادريس فرج	محاسب	وحدة الحسابات والمالية	2024-04-17	الأربعاء		08:51	13:40
000000705	جبريل شعبان عبد الله	فني تركيبات وأعمال مدنية	فريق الكوابل والتركيبات	2024-04-17	الأربعاء		08:53	13:01
000000706	محمد علي سالم	مهندس قوى	فريق القوى والتكييف	2024-04-17	الأربعاء		08:48	13:00
000000707	رمضان راجي محمد	موظف خدمات	وحدة الخدمات	2024-04-17	الأربعاء		08:57	13:22
000000708	احمد فرج علي	سائق	وحدة الخدمات	2024-04-17	الأربعاء		08:55	13:03
000000751	أيمن مصطفى	أمين سر	قسم التشغيل والصيانة - المنطقة الشرقية	2024-04-17	الأربعاء		08:05	13:08

الرقم الشخصي	الاسم الأول	المنصب	القسم	التاريخ	ايام الاسبوع	استثناء	وقت تسجيل الدخول	وقت تسجيل الخروج
000000753	طه احمد صالح	مهندس تركيبات وأعمال مدنية	فريق الكوابل والتركيبات	2024-04-17	الأربعاء	تبرير تأخير	09:27	13:01
000000754	محمد حمد فرج	مهندس قوى	فريق القوى والتكييف	2024-04-17	الأربعاء		08:59	15:13
000000755	محمد حمد عبد الرحمن	مهندس قوى	فريق القوى والتكييف	2024-04-17	الأربعاء		08:50	15:13
000000758	احمد ونيس حمد فرج	مهندس دعم فني خدمات تقنية	وحدة تقنية المعلومات	2024-04-17	الأربعاء		08:56	13:00
000000767	عقيلة رفعت عقيلة	مدير تشغيل شبكة النفاذ المباشر و اللاسلكي	وحدة توزيع الخدمات	2024-04-17	الأربعاء	تبرير تأخير	09:18	13:00
000000796	احمد مراجع معتوق	أمين مخزن	وحدة المشتريات	2024-04-17	الأربعاء		08:16	13:03
000000817	عبدالرحمن المبروك	سائق	وحدة الخدمات	2024-04-17	الأربعاء		08:46	13:20
000000818	محمد عمران فرج	مهندس دعم فني خدمات تقنية	وحدة تقنية المعلومات	2024-04-17	الأربعاء		08:38	13:00
000000826	محمد علي محمود	مهندس دعم فني خدمات تقنية	وحدة تقنية المعلومات	2024-04-17	الأربعاء	تبرير تأخير	09:27	13:10
000000833	فرج يونس عبدالونيس	سائق	وحدة الخدمات	2024-04-17	الأربعاء		08:37	13:00
000000853	عبدالله محمد صالح	مهندس شبكة النفاذ النحاسي	وحدة توزيع الخدمات	2024-04-17	الأربعاء		08:45	13:00
000000855	حسن عثمان حسن	مهندس شبكة تراسل	فريق شبكة التراسل	2024-04-17	الأربعاء		08:21	13:00
000000863	قيس خالد عقيلة	مهندس شبكة النفاذ النحاسي	وحدة توزيع الخدمات	2024-04-17	الأربعاء		08:27	13:00
000000873	يحيى علي محمد	مهندس تركيبات وأعمال مدنية	فريق الكوابل والتركيبات	2024-04-17	الأربعاء		08:34	13:56
000000877	عبدالمالك يوسف محمد	مهندس شبكة النفاذ النحاسي	وحدة توزيع الخدمات	2024-04-17	الأربعاء		08:32	13:00
000000897	ابراهيم مصطفى حسن	مهندس تركيبات وأعمال مدنية	وحدة متابعة تنفيذ المشاريع	2024-04-17	الأربعاء		08:40	13:01
000000898	علي سليم محمد	فني تركيبات وأعمال مدنية	وحدة متابعة تنفيذ المشاريع	2024-04-17	الأربعاء		08:51	13:01

مصرف الصحارى
SAHARA BANK

الصادر : م. ص. إ.ع 364/ 05/ 2024م
التاريـــخ : 04/ ذو القـــعدة/1445 هـ
المـــوافـــق : 13/ مايـــــو /2024م

مكتب النائب العام
قسم المعلومات والتوثيق
15. 05. 2024
الوارد العام
تم التوثيق

السيد المستشار / النائب العام .

تحية طيبة وبعد،،،

في الوقت الذي نُثمّن فيه جهودكم خدمةً للصالح العام و ذوداً عن حقوق المواطنين ، فإننا نود أن نتقدم لحضرتكم بالإبلاغ عن واقعة محاولة إختراق الموقع الإلكتروني للمصرف من قبل أحد العناوين الإلكترونية التابعة لمكاتب شركة الجيل " مزود إنترنت في الدولة " مقرها مدينة بنغازي والتهديد بنشر بيانات الزبائن وما يكتنفها من "سرية مصرفية" مع المطالبة بمبالغ مالية قيمتها ($100,000.00) مائة ألف دولار ، وذلك في مقابل عدم النشر ، وهذا من واقع التقرير الفني المعد من إدارة أمن المعلومات بالمصرف مرفق نسخة منه .
كما نود التوضيح بأن المنظومة المصرفية وحسابات الزبائن لم يتم المساس بها بأي شكل من الأشكال .

وعطفاً على ما سبق بيانه ،،،

نأمل من سيادتكم التكرم مشكورين بإتخاذ ما يلزم من إجراءات حماية لحقوق المصرف وزبائنه وسمعته التجارية من عمليات القرصنة الإلكترونية ، لاسيما وأن بعض مواقع التواصل الإجتماعي استغلت هذه الواقعة كوسيلة للظهور والشهرة مما أدى لحدوث حالة من الفزع والفوضى من جانب بعض الزبائن خوفاً من إحتمال إختراق حساباتهم .

أدام الله عدلكم
والسلام عليكم ورحمة الله وبركاته

مصرف الصحارى
SAHARA BANK
طرابلس - ليبيا
الإدارة العامة

أحمد حامد الحضيري
المدير العام لمصرف الصحارى

مكتب النائب العام
وحدة الوارد العام
2024 -05- 14
رقم التسجيل 7097

صورة إلى :
السيد/ رئيس مجلس الإدارة
السيد/ مدير إدارة الشؤون القانونية
ملف الصادر + ملف الموضوع
أمين

تم ضبط شؤون المعلوماتية والإتصالات
رقم الوارد/ 432
التاريخ/ 2024-5-21

بتاريخ 7-5-2024

انـــــه في يوم الثلاثاء الموافق 7.5.2024 تعرض الموقع الالكتروني الي محاولة هجوم سيبراني عند الساعة 12:00 صباحا وتم صد محاولة الهجوم وإيقاف الموقع الالكتروني عن العمل من قبل إدارة امن المعلومات و رئيس وحدة الموقع الإلكتروني بمكتب التواصل مباشرة بالتدخل السريع بإعطاء التعليمات اللازمة وتنفيذ الإجراءات المضادة.

تم تغيير واجهة الموقع الالكتروني بصورة تحمل رابط وعنوان حساب التلغرام الخاص بشخص يدعي انه المخترق ويطالب بمبلغ مالي .

قمنا بإيقاف الموقع لحوالي 3 دقائق كإجراء لصد الهجمة و تم من خلالها استرجاع الموقع الالكتروني.

قمنا بفحص الموقع من العناوين التي حاولت الدخول الي الموقع وتبين ان جميع العناوين هي من داخل ليبيا وجاري فحصها والتأكد منها.

قمنا بالتأكد من عدم وجود ضرر بقاعدة البيانات او حذفها وأن البيانات لايوجد بها أي ضرر من قبل منفذي محاولة الهجوم .

وعند حوالي 3:30 صباحا تم ادعاء نشر بيانات تخص زبائن المصرف على Dark web و تمت اضافتها من قبل زبائن المصرف عند إتمام عملية المطابقة الخاصة بمنظومة الأغراض الشخصية لمصرف ليبيا كما موضح بالمرفق

كما تم تطبيق الإجراءات الاتية

- تم تغيير كلمة المرور مباشرة واعداد كلمة مرور جديدة للموقع الالكتروني
- تم التأكيد على عمل Web application firewall داخل الموقع الخاص بالمصرف و نظام تقييم الثغرات الأمنية tenable was يعمل بشكل المطلوب كما موضح في المرفق بعدم وجود أي ثغرات.
- تم اختبار اختراق الموقع من قبل شركة Cybertech بعمل هجوم سيبراني على الموقع وتم صد الهجوم من قبل الWAF.
- تم التواصل مع شركة TrendMicro للقيام بتحليل الموقع الالكتروني للمصرف وكذلك لتقديم الدعم اللازم من اجل صد أي محاولة هجمات الكترونية.
- تم البحث بإستخدام SocRadar في Darkweb ولم يتم الإعلان او الإفصاح عن أي معلومات تخص المصرف داخل Darkweb

وبهذا فإننا ننفي وصول الهجوم الي خوادم وبيانات المنظومة المصرفية أو شبكة المصرف وان محاولة الاختراق قد تمت لموقع المصرف الالكتروني المستضاف من قبل Libyan spider و نؤكد بأن المنظومة المصرفية وشبكة المصرف تعمل بالشكل الطبيعي بأقصى درجات الأمان ولم يتم تهديدها بأي نوع من التهديدات أو إختراقها .

وبافتراض انه قد تم فعليا نشر البيانات المزمع الحصول عليها من قبل الموقع الالكتروني فإنه في كل عملية الكترونية شـــــائعه كـــ (عملية حجز العملة الأجنبية، مطابقة البيانات) تظهر العديد من الروابط المزيفةfaked والتي من شأنها ان توهم الزبون بأنها مصادر موثوقة لتقديم الطلب عن طريق تعبئة البيانات المطلوبة ويعتبر احد السيناريو للحصول على البيانات المنشرة .

يتم تسريب البيانات بطريقة أخرى عن طريق أحد الموظفين المتحصلين على البيانات ولديهم امتيازات الوصول الي البيانات المزمع نشرها

ملاحظة:

توجه فريق إدارة امن المعلومات ورئيس وحدة المواقع الالكترونية مباشرة من الساعة 8 صباحا الى مقر شركة العنكبوت الليبي وقاموا باستخراج سجل العناوين كافة التي سجلت الدخول الى الموقع

المرفقات :

تقرير من نظام الثغرات الأمنية

تم إغلاق لوحة الحضور Cpanel الخاصة بالموقع إحترازيا
و كذلك إيقاف جميع خدمات إضافة البيانات على الموقع أو تعديلها

و السلام عليكم

إدارة امن المعلومات
رئيس وحدة المواقع الالكترونية بمكتب التواصل

←رد
- إعادة توجيه

تم إغلاق لوحة الحضور

tenable Vulnerability Management

Vulnerability Management Overview (Explore)

Vulnerability Age: Managing SLAs

	90+ Days	61-90 Days	31-60 Days	15-30 Days	8-14 Days	0-7 Days
Critical	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Low	0	0	0	0	0	0

SLA Progress: Vulnerability Age

	Not Meeting SLAs	Meeting SLAs
Critical	0	0
High	0	0
Medium	0	0
Low	0	0

Vulnerability Priority Rating (VPR)

Rating 9.0-10

0

0

0

0

Severity Statistics by Source

Discovered by Nessus

Severity

0 Critical

0

Discovered by Nessus Agent

Severity

0 Critical

0

Discovered By Agentless

Severity

0 Critical

0

Scan Health

Tenable Research Advisory

Missing Patches

Applied Patches

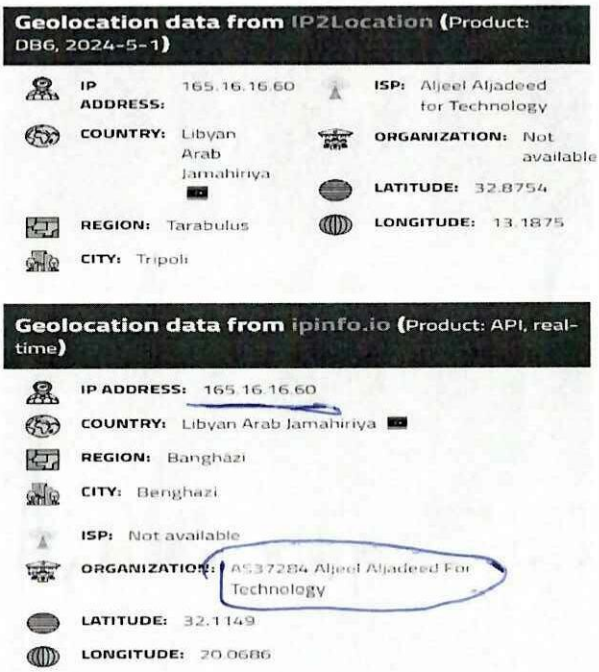
Critical and High Exploitable Vulnerabilities

Future Threats: Not Yet Exploitable Vulnerabilities

	Published 0-30 Days Ago	Published 31-90 Days Ago	Published 91-180 Days Ago	Published 180+ Days Ago
Proof of Concept	0	0	0	0
Unproven Exploit	0	0	0	0

السيد مدير ادارة امن المعلومات
بعد التحية ،،،
بناء على التكليف الصادر من طرفكم بخصوص متابعة التحقيق الجنائي الرقمى بشأن واقعه الاختراق الامنى لموقع المصرف الإلكتروني وعلى ماتم انجازه بالخصوص
نفيذكم بأنه قد تم الاتي:

- بعد عملية جمع الاستدلالات والأدلة الكافية لمحاولِ الاختراق وحيث ان العنوان الشبكى المسؤول عن عملية الاختراق كان من طرف شركة الجيل الجديد كما موضح اذناه



- تم توجيه بلاغ رسمى من قبل السيد مساعد مدير ادارة الفروع للمنطقة الشرقية الى الجهات الامنية وكذلك أخد الاقوال من قبل الفريق المكلف من ادارة امن المعلومات بشأن التبليغ عن الواقعة.
- تم اضافة الادلة للمحضر الجنائي للواقعة بتقرير مفصل يوضح عنوان المهاجم وكذلك الوقت والتاريخ للهجوم.
- تم اجراء التحقيقات اللازمة بالخصوص من قبل الجهات الامنية المعنية.

وحسب ما تم افادتنا به شفويا من قبل السيد مدير ادارة مكافحة الجرائم الاقتصادية وغسيل الاموال انه قد تم زيارة مقر شركة الجيل الجديد بمدّينة بنغازي ومن خلال تقريرهم بجمع الادلة بأن الشبكة الخاصة بشركة الجيل الجديد يوجد بها ثغرات امنية كما يوجد اجهزة حاسوب تم تنزيل برامج خبيثة عليها يتم من خلالها استغلال عمليه الهجوم والوصول الى اجهزة وخوادم عدة وعدم وجود جدار حماية للشبكة الخاصة بشركة الجيل الجديد مما يؤكد عملية الهجوم من قبل الشركة على الخوادم الخاصة بموقع المصرف والمستضافة لدي شركة العنكبوت

وعليه فقد تم ارسال محضر الاستدلالات الى نيابة مكافحة الفساد ببنغازي
كما تم إفادتنا برسالة من قبل ادارة مكافحة الجرائم الاقتصادية وغسيل الاموال بخصوص احالة المحضر الى النيابة العامة لأتخاد الاجراءات اللازمة

ملخص استدلالات لنتائج التحقيق من طرف المصرف:

- تم إضافة صفحة من اجل تعبئة بيانات الزبائن لإجراء عمليات المطابقة في منظومة الأغراض الشخصية بمصرف ليبيا المركزي
- تم إضافة الصفحة ببرنامج WordPress من قبل رئيس وحدة الموقع الالكتروني بمكتب التواصل وبدون علم إدارة امن المعلومات واخد الموافقات اللازمة
- تم إضافة قاعدة بيانات من قبل المنشئ على الصفحة التي تم اضافتها ولم يتم تشفير البيانات بكلمة مرور
- تم استغلال هذه الثغرة من قبل المخترق وتم إضافة برنامج خبيث بتاريخ 17-04-2024 على خادم الويب من عنوان شبكي 165.16.16.60 مكنه من الدخول الي لوحة التحكم الخاصة بالموقع الالكتروني
- تمت عملية الهجوم على الموقع بتاريخ 2024/5/7 وتغيير الواجهة الخاصة بالموقع الالكتروني
- قام المهاجم بمسح جزء كبير من الملفات الخاصة بسجلات الدخول
- بعد عملية تحليل مفصلة وجدنا ملف في تطبيقات الويب alfa.shtml ومن خلال استغلال هذه الثغرة تمكن المهاجم من تنفيذ الأوامر دون مصادقة او تسجيل الدخول الي النظام

وبهذه الجهود المبذولة من قبل فريق ادارة امن المعلومات نشكر السيد مساعد مدير ادارة الفروع للمنطقة الشرقية لتعاونه الكامل ومساعدته في تسهيل الاجراءات المتعلقة بالخصوص

معدي التقرير

فريق إدارة امن المعلومات

مصرف الصحارى
SAHARA BANK

الأربعاء 29 /م-(05)/ايار/2024م
اشارتي: 2024 / 05 / 547

السيد/ لـواء. دكـتور
المهـــدي محمـــد حمـــد بيانكـــو
مدير الإدارة العامة لمباحث الأموال العامة،،،

بعد التحية،،،

بدايةً أود أن اتقدم لكم بالأصالة عن نفسي وبالنيابة عن كافة موظفي مصرف الصحارى بخالص شكرنا وتقديرنا لوقوفكم بجانبنا كإدارة منطقة شرقية لمصرف الصحارى في الاعتداء الذي تعرضنا له من هجوم إلكتروني على موقع مصرف الصحارى واتخاذكم الإجراءات اللازمة لإيجاد المسؤولين عن هذا الهجوم وضمان حقوق مصرفنا.

وعليه، فإننا نأمل منكم التفضل مشكورين بتزويدنا بإفادة من طرفكم بشأن واقعة الهجوم الإلكتروني على موقع مصرف الصحارى وعلى ما تم اتخاذه من طرفكم من إجراءات بالخصوص ليتسنى لنا اتخاذ الإجراءات القانونية اللازمة من طرف المصرف للحفاظ على سرية بيانات عملائنا وحماية حقوقنا.

شاكرين لكم حسن تعاونكم الدائم معنا ،،،
والســـلام عليكـــــم ،،،

د. خالد أحمد الشريف
مساعد مدير إدارة الفروع للمنطقة الشرقية

مصرف الصحارى
SAHARA Bank
ادارة الفروع
الشرقية

صـ:
السيد/ مدير عام المصرف المكلف.
السيد/ م.م.ع. للأعمال المصرفيـــة.
السيد/ مدير إدارة الفـــــــروع.
السيد/ مدير إدارة الشؤون القانونية.
السيد/ مدير إدارة أمن المعلومـات.
الصـــــــــــــادر.
خ.الشريف ..... ع. اللواطي

مصرف الصحارى
SAHARA BANK

الإثنين 29 /مـ(05)مايو/2024م
اشاري: 0 55 / 05 / 2024

السيد/

مدير عام المصرف المكلف ،،،

بعد التحية،،،

بالإشارة إلى واقعة الهجوم الإلكتروني التي تعرض لها موقع مصرف الصحارى والشكوى التي تقدمنها بها باسم المصرف أمام **السيد/ اللواء دكتور. المهدي محمد حمد بيانكو. مدير إدارة مكافحة الجرائم الاقتصادية وغسل الأموال.**

عليه، نحيل إلى سيادتكم الإفادة الصادرة عن **السيد/ مدير إدارة مكافحة الجرائم الاقتصادية وغسل الأموال** تحت الإشاري رقم 3-47، قيد 218 والمؤرخة في 2024/05/29 والموجهة لسيادتكم بالخصوص.

كما نرفق لسيادتكم نسخة من رسالتنا رقم 548 والمؤرخة في 2024/05/29 **للسيد/ مدير الإدارة العامة لمباحث الأموال العامة** بشان تكليف **السيد/ امراجع عبدالقادر حسين إبراهيم**، رئيس وحدة الشؤون القانونية بإدارة الفروع الشرقية بمتابعة مستجدات الموضوع مع الجهات ذات العلاقة للتفضل بأخذ العلم.

والسلام عليكم ،،،

د. خالد أحمد الشريف
مساعد مدير إدارة الفروع للمنطقة الشرقية

مصرف الصحارى
Sahara Bank
إدارة الفروع
الشرقية

:
السيد/ م.م.ع. للأعمال المصرفية.
السيد/ مدير إدارة الفروع.
السيد/ مدير إدارة الشؤون القانونية.
السيد/ مدير إدارة أمن المعلومات.
الصادر.
خ.الشريف ..... ع. اللواطي

وزارة الداخلية
Ministry of the interior
إدارة مكافحة الجرائم الإقتصادية وغسل الأموال
Management Combating Economic Crimes
and Money Laundering

الرقم الاشاري: 47-3 القيد: 218 التاريخ: 2024/5/29

السيـــــــد / مدير عـــــام مصـــــرف الصحـــــــاري

تحية الأمن والسلام ،،

الموضوع /

واقعة الهجوم السيبراني ((اختراق)) موقع مصرف الصحاري

بالإشـــارة إلي الشـــكوى المقدمة من مســـاعد مدير إدارة فروع المنطقة الشـــرقية بالواقعة المذكـــــورة أعلاه ضد جهـــــة مجهولـــــة .

عليه نفيدكم بأن تم الاستدلال في الواقعـــة وعرض المحضـــر علي السيـــــد مدير نيابة مكافحـــة جرائم الفســـاد بنغازي .

للتفضل بالاطلاع

والسلام عليكم ورحمة الله وبركاته

مدير الادارة

لـــواء / دكتور

المهدي محمد حمد بيانكو

مدير إدارة مكافحة الجرائم الاقتصادية وغسل الاموال

منه الى :
السيد / مدير نيابة مكافحة جرائم الفساد / بنغازي / للعلم .
السيد / رئيس قسم التحقيق والتحـــري بالإدارة / للمتابعة .
الملـــــف الدوري العـــــــام / للحفظ .
البرغثي . م . / إينـــاس السعيطـــــي .

المباشر / 061 222 7696 ((Direct)) الفاكس 061 222 6084 ((Fax))
Email : lydpacec@gmail.com
بنغازي - ليبيا TEL : 218614703571 / TEL : 218614747431 Benghazi-Libya
Management of Anti Economic Crimes and Money Laundering