السيد/ مدير مكتب النائب العام

بعد التحية ،،،

بالإشارة،،، الي كتاب السيد مدير نيابة مكافحة جرائم الفساد رقم (159/3/1) والمؤرخ في 2024/03/05م الوارد عام رقم (4146) بشأن التحقيقات الجارية في واقعة الشروع في الاستيلاء علي المال العام والكسب غير المشروع وذلك لقيام المتهمين بزرع جهاز بمنظومة المصرف التجاري الوطني لغرض اختراقها والاستلاء علي مبالغ مالية منها.

عليه

نحيل،،، إليكم التقرير الفني مرفق بقرص مدمج يحتوي علي جميع البيانات التي تم استخراجها والتي تتعلق بواقعة الاختراق للمنظومة المصرفية وذلك لإحالتها للنيابة المختصة.

والسلام عليكم

المرفقات:

- جهاز كمبيوتر نوع (hp) + الشحن الخاص بالجهاز.
- جهاز مزود انترنت نوع (iku) + مدرج به شريحة اتصالات نوع ليبيانا.

نائب النيابة

عمر محمد اسكيليح

(رئيس قسم ضبط شؤون المعلوماتية والاتصالات)

صورة إلى:

- الأستاذ المستشار النائب العام.
- وحدة الوارد العام والتوثيق.
- وحدة المعلومات والتوثيق.
- الملف الدوري بالأرشيف.

12

ليبيا

النيابة العامة

نيابة شمال بنغازي الأبتدائية

التاريخ : / /

الموافق : 05 /2024/03

الاشاري:3/1 قيد 159 ن م ج ف

مكتب النائب العام
11 -آذار- 2024
قسم المعلومات والتوثيق والاتصالات

الأستاذ// رئيس قسم الإتصالات والمعلوماتية بمكتب النائب العام

بعـــــد التحية ،،

إيمـاءً للتحقيقات الجارية في القضية رقم 2023/158 نيابة مكافحة جرائم الفساد .

والمتهم فيها "مؤنس جبريل عاشور وعلاء عبدالله الشيباني ومراجع الدرسي وساسي فونى وآخرين "بتهمة الشروع في الاستيلاء على المال العام والكسب غير المشروع وذلك لقيامهم بزرع جهاز بمنظومة المصرف التجاري الوطني وذلك لاختراق المنظومة وزرع مبالغ مالية وحسابات والاستلاء عليها عقب ذلك .

عليـــــه نحيل إليكم الاجهزة المستخدمة في عملية الاختراق وهو نوع :

HP –PRODESK600G3MINI

أسود اللون مع جهاز انترنت **(4GLTT)** لخبير الإتصال والمعلوماتية بمركز الخبرة القضائية والبحوث بنغازي وتعذر عليه تنفيذ المهمة المكلف بها نظراً لقلة الإمكانيات بحسب الثابت بكتاب مدير الخبرة القضائية الرقيم 24/133/11/1 المرفق منه صورة طية كتابنا هذا.

عليه ونأمل منكم فحصها وتفريغ محتواها وبيان آلية عملها وكافة المعلومات والبيانات المخزنة عليها وإي معلومة حيال عملية اختراق منظومة مصرف التجاري الوطني .

مكتب النائب العام
وحدة الوارد العام
2024 -03- 11
رقم التسجيل ..... 4146 .....

وشاكرين لكم حسن تعاونكم
وتقبلوا فائق الاحترام والتقدير ،،

والســـ عليكم ورحمة الله وبركاته ـــــلام

مكتب النائب العام
قسم المعلومات والتوثيق
12. 03. 2024
الوارد العام
تـــم التوثيـــق

ملاحظة: المتهمين على ذمة القضية قيد الحبس الاحتياطي من تاريخ 2023/2/28

(12)

أ. عبدالناصر محمد العرفي
مدير نيابة مكافحة جرائم الفساد

صورة منه إلى
الملف الدوري العام للحفـــــظ.
أ . الفرجاني

العنوان : شارع جمال عبدالناصر سابقاً بجوار ميدان الشجرة– بنغازي / ليبيا
الهاتف : 218619080165 + الفاكس : 218619092356

State Of Libya
Ministry Of Justice
Judicial Expertise and Research Center

دولة ليبيا
وزارة العدل
مركز الخبرة القضائية والبحوث

التاريخ : ..... / ..... / .....

الموافق : 20 / 02 / 2024

الإشاري : 24/133/11/1

السيد // مدير نيابة مكافحة جرائم الفساد

الأستاذ // عبد الناصر محمد العرفي

بعد التحية.

بالإشارة . إلى كتابكم ذو رقم اشاري 1/1 قيد 46 ن م ج ف والمؤرخ في 2024/01/11م بخصوص القضية رقم (2023/158) نيابة مكافحة جرائم الفساد.

نحيل.. إليكم جهاز نوع **(HP-PRODESK 600 G3 MINI)** أسود اللون مع جهاز إنترنت **(4G LTT)**، وقد تم تشغيله وتبين بأن نظام تشغيله ويندوز **(WINDOWS)** ويمكن الدخول إليه كمسؤول **(Administrator)** وكمستخدم **(User)** وكلا النافذتين تحتوي على كلمة مرور **(Password)**، ولم نقوم بأي محاولة لكسر كلمات المرور وتجاوزها خوفا من فقدان بعض البيانات والمعلومات التي قد تكون بغاية الأهمية. حيث أن الجهاز المذكور أعلاه هو الجهاز الذي يحوي المعلومات التي قد تؤدي إلى الشخص الذي يتحكم في الجهاز عن بُعد، لذلك فأنسب طريقة لكشف بيانات الجهاز دون فقدان أي معلومة منها باستخدام جهاز نوع **(Oxygen Forensic Kit)** **عليه ..** نحيطكم علماً بأن هذا الجهاز لا يتوفر لدينا حاليا نظراً لقلة الإمكانيات.

والسلام عليكم ورحمة الله وبركاته

مدير مركز الخبرة القضائية والبحوث - بنغازي

عقيد / خبير محمد حسن البرغثي

صورة إلى:
- ملف الدوري العام للحفظ.

JE.ARC64@GMAIL.COM
021 - 3344270 & 3333112
021 - 3335762

دولة ليبيا

مكتب النائب العام

قسم ضبط شؤون المعلوماتية والاتصالات

رقم التقرير	2024/3/45
التاريـــخ	25 / 03 / 2024م

التقريـــــر الفنـــــي

نوع الجهاز // كمبيوتر موديل الجهاز // HP-PRODESK 600 G3 MINI لون الجهاز // أسود

الرقم التسلسلي // 8CG8156HDZ

مساحة الذاكرة الداخلية// G.B 512

رمز قفل الجهاز // لا يوجـــــد

الموضوع // قضية رقم (2023/158) نيابة مكافحة جرائم الفساد الوارد عام (4146)

=	ملاحظات عن حالة المبرزة عند استلامها
1	مرفق بالمبرزة الشحن الخاص بالكمبيوتر.
2	مرفق بالمبرزة جهاز مزود انترنت نوع (iku).
3	مدرج بجهاز مزود الانترنت شريحة اتصالات نوع ليبيانا تعمل.

اعتماد رئيس قسم ضبط شؤون المعلوماتية والاتصالات
بمكتب النائب العام

إعداد:12

الملخص العام للتقرير الفني

باجراء الكشف الفني علي المبرزة المحالة إلينا نوع (HP-PRODESK 600 G3 MINI) تبين لنا وجود عدد (2) حسابات للمستخدمين الأول يحمل صفة المسؤول (Admin) تحت أسم (hp) والثاني مستخدم بدون صلاحيات يحمل اسم (hp1) وكلا الحسابين يحتويان علي كلمة مرور (Password) وبتخطي كلمة المرور باستخدام برنامج (PassFab 4WinKey) وهو تطبيق معتمد من شركة مايكروسوفت تمكنا من فتح جهاز الكمبيوتر المذكور دون فقد للبيانات وتبين لنا التالي:-

1	قيام مستخدم المبرزة (المتهم) بتعطيل خاصية الحماية للجدار الناري وحماية الشبكة والحماية من الفيروسات (Virus & threat Protection) (Firewall & Network Protection) حيث يتم تعطيل خواص الحماية المذكورة في حالة استخدام البرمجيات الضارة في الاختراق والتلاعب بالبيانات التي يتم تداولها عبر الشبكات وقواعد البيانات المتصلة بالمبرزة.
2	قيام مستخدم المبرزة (المتهم) بطمس الصوت ومنع الاشعارات ومنع التحديث التلقائي لنظام التشغيل تحسباً من قيام المبرزة بتصحيح الأخطاء وتحديث النظام مما ينتج عنه مسح البرمجيات الضارة التي تم تثبيتها من قبل المستخدم.
3	قيام مستخدم المبرزة (المتهم) بتثبيت نظام تشغيل لينكس (Linux) على بيئة (VirtualBox) كنظام وهمي بجانب النظام الأساسي الويندوز وهو نظام تشغيل مفتوح المصدر يستخدم في التعامل وتحكم في قواعد البيانات والشبكات الرقمية المختلفة.
4	قيام مستخدم المبرزة (المتهم) بتثبيت توزيعة كالي لينكس (kali linux) والتي تحتوي علي العديد من أدوات القرصنة والاختراق والتصيد للبيانات من الأجهزة او حسابات او مواقع المرتبطة بالشبكات وقواعد البيانات دون اخذ الاذن من النظام الأساسي وبدون علم المستخدمين الذين لا يمتلكون الخبرة في طرق كشف الاختراق.
5	قيام مستخدم المبرزة (المتهم) بتثبيت عدد (2) برامج تحكم عن بعد (AnyDesk) (TeamViewer) وهي برامج يتم تثبيتها علي نظام التشغيل الأساسي الويندوز لغرض التحكم بجهاز الكمبيوتر عن بعد عن طريق شبكة الانترنت. وبمجرد تشغيل المبرزة تبين لنا عمل البرامج المذكورة بشكل فوري.
6	قيام مستخدم المبرزة (المتهم) بتثبيت برنامج (qBittorrent v4.6.0) وهو برنامج يتم تثبيته علي نظام التشغيل الأساسي الويندوز لغرض إرسال واستقبال البيانات عبر شبكة الانترنت من والي المستخدم. وبتشغيل البرنامج (دون الولوج الي الانترنت) تبين لنا قيام (المتهم) بتحميل أكثر من (13 G.B) من البيانات عبر توزيعات الكالي لينكس المثبتة علي المبرزة.

اعتماد رئيس قسم ضبط شؤون المعلوماتية والاتصالات
بمكتب النائب العام

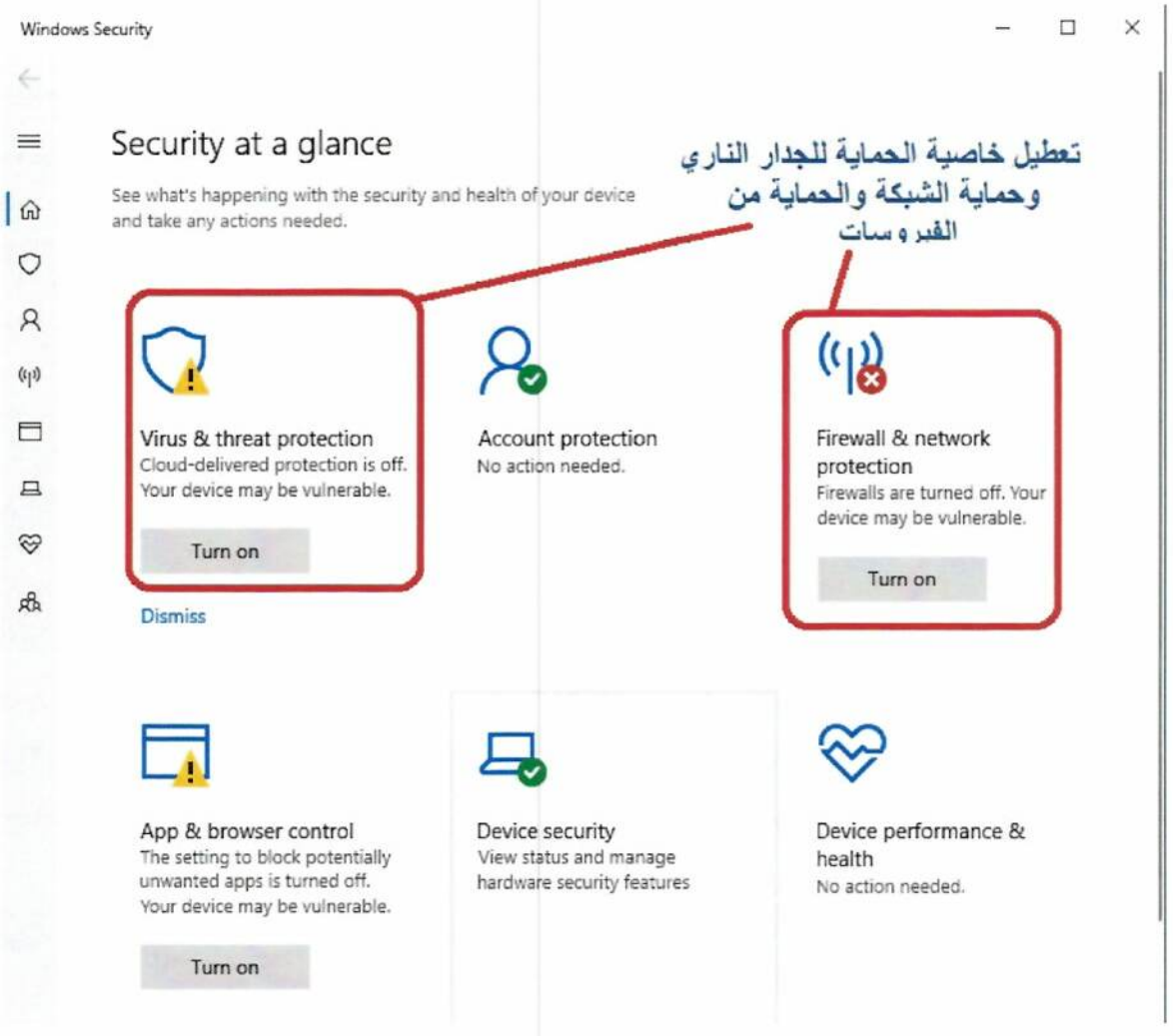
إعداد:12

7	قيام (المتهم) بتثبيت أداة (Nmap Zenmap GUI) علي توزيعة كالي لينكس علي النظام الأساسي ويندوز وهي تعتبر من أشهر أدوات التي يستخدمها الهاكر في إجراء المسح الكامل لمحتويات الشبكة وتحديد الثغرات ومواطن الضعف علي الشبكة ويعمل على استكشاف الأجهزة أو التعرف على عنوان الإنترنت (IP) الخاص بها بالإضافة إلى تتبع العمليات التي يقوم بها المستخدمين علي الشبكة والحصول علي كلمات المرور الخاصة بهم وغيرها من المفاتيح التي تمكن المخترق من التحكم في قاعدة البيانات والشبكة بشكل عام.
8	بإجراء التدقيق الفني علي جهاز مزود الانترنت (4G LTT) المرفق بالمبرزة تبين لنا أنه يحتوي علي شريحة اتصالات نوع (ليبيانا) تحمل رقم (0920989329) وبالدخول علي بيانات المستخدم لشريحة بالشركة المزودة للخدمة تبين لنا: أسم المستخدم : محمد سيف الدين محمد العرفي. العنوان : بنغازي. الرقم الوطني : 120060066135 تاريخ الميلاد 2006/11/24م
	عدد صفحات التقرير (8).

اعتماد رئيس قسم ضبط شؤون المعلوماتية والاتصالات
بمكتب النائب العام

إعداد:12

قيام مستخدم المبرزة (المتهم) بتعطيل خاصية الحماية للجدار الناري وحماية الشبكة والحماية من الفيروسات (Firewall & Network Protection) (Virus & threat Protection)

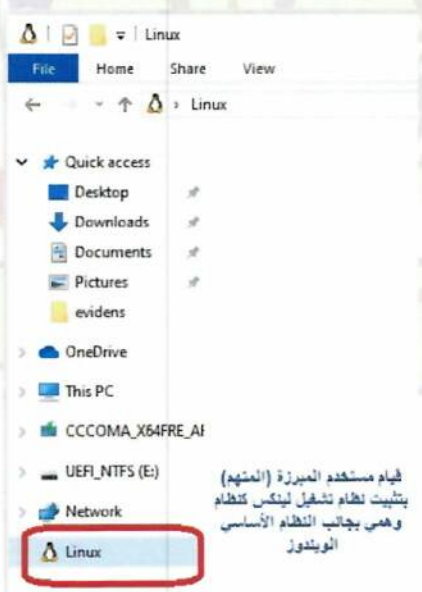


اعتماد رئيس قسم ضبط شؤون المعلوماتية والاتصالات
بمكتب النائب العام

إعداد:12

قيام مستخدم المبرزة (المتهم) بطمس الصوت ومنع الاشعارات ومنع التحديث التلقائي لنظام التشغيل

قيام مستخدم المبرزة (المتهم) بتثبيت نظام تشغيل لينكس (Linux) على بيئة (VirtualBox) كنظام وهمي بجانب النظام الأساسي الويندوز



اعتماد رئيس قسم ضبط شؤون المعلوماتية والاتصالات
بمكتب النائب العام

إعداد:12

قيام مستخدم المبرزة (المتهم) بتثبيت توزيعة كالي لينكس (kali linux) والتي تحتوي علي العديد من أدوات القرصنة والاختراق والتصيد للبيانات

قيام مستخدم المبرزة (المتهم) بتثبيت عـدد (2) برامـج تحكـم عـن بعـد

(TeamViewer) (AnyDesk)

وهي برامج يتم تثبيتها علي نظام التشغيل الأساسي الويندوز لغرض التحكم بجهاز الكمبيوتر عن بعد عن طريق شبكة الانترنت.

برنامج AnyDesk للتحكم عن بعد عبر شبكة الانترنت

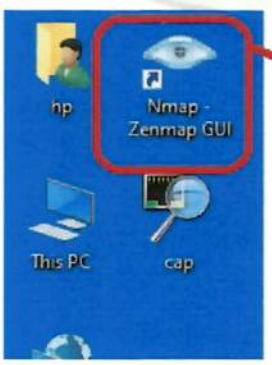
برنامج تيمفيور للتحكم عن بعد

اعتماد رئيس قسم ضبط شؤون المعلوماتية والاتصالات
بمكتب النائب العام

إعداد:12

قيام مستخدم المبرزة (المتهم) بتثبيت برنامج (qBittorrent v4.6.0) وهو برنامج يتم تثبيته علي نظام التشغيل الأساسي الويندوز لغرض إرسال واستقبال البيانات عبر الانترنت من والي المستخدم

قيام (المتهم) بتثبيت أداة (Nmap Zenmap GUI) علي توزيعة كالي لينكس علي النظام الأساسي ويندوز وهي تعتبر من أشهر أدوات التي يستخدمها الهاكر

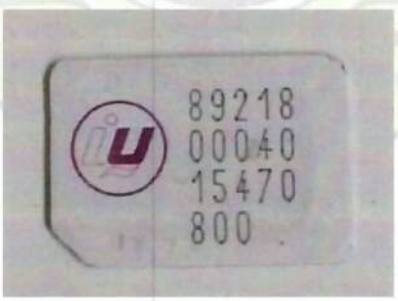


قيام (المتهم) بتثبيت أداة (Nmap Zenmap GUI) علي توزيعة كالي لينكس علي النظام الأساسي ويندوز وهي تعتبر من أشهر أدوات التي يستخدمها الهاكر

اعتماد رئيس قسم ضبط شؤون المعلوماتية والاتصالات
بمكتب النائب العام

إعداد:12

جهاز مزود الانترنت (4G LTT) المرفق بالمبرزة تبين لنا أنه يحتوي علي شريحة اتصالات نوع (ليبيانا) تحمل رقم (0920989329)



ملاحظـــــة:

مرفق بالتقرير قرص مدمج (CD) يحتوي على جميع البيانات التي تم استخراجها من المبرزة.

إعداد:12

اعتماد رئيس قسم ضبط شؤون المعلوماتية والاتصالات
بمكتب النائب العام