دليل جمعية الامل العراقية في

الأمن الرقمي

للمدافعين عن حقوق الإنسان

www.iraqi-alamal.org

www.iraqi-alamal.org

دليل جمعية الامل العراقية في
الأمن الرقمي للمدافعين عن حقوق الإنسان
إصدار جمعية الامل العراقية 2022

www.iraqi-alamal.org

تم إنتاج هذا المطبوع بدعم مالي من الاتحاد الأوروبي محتوياتها هي من مسؤولية (جمعية الأمل العراقية)
ولا تعكس بالضرورة وجهات نظر الاتحاد الأوروبي

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of
(Iraqi Al-Amal Association) and do not necessarily reflect the views of the European Union

This project is funded by the European Union

جمعية الأمل العراقية
Iraqi Al-Amal Association

دليل جمعية الامل العراقية في

الأمن الرقمي

للمدافعين عن حقوق الإنسان

This project is funded by the European Union

جمعية الأمل العراقية
Iraqi Al-Amal Association

www.iraqi-alamal.org

مقدمة

يستعمل المدافعون عن حقوق الانسان الحاسوب وشبكة الانترنت بشكل مستمر في حياتهم العملية والاجتماعية وبما أن امكانية الوصول الى التكنلوجيا لاتزال مسألة قائمة حول العالم، أصبح تخزين وتبادل المعلومات بالوسائل الإلكترونية أكثر شيوعاً لدى منظمات حقوق الإنسان، إلا أن بعض الحكومات هي الأخرى تقوم بدورها في تطوير القدرة على العبث بالمعلومات الإلكترونية، ومراقبتها وتخريبها. وقد زادت عمليات المراقبة والرقابة وحالة انعدام أمن المعلومات المخزنة أو المتبادلة إلكترونياً فغدت مشكلة أساسية للمدافعين عن حقوق الإنسان في بعض من البلدان مثلاً "(النموذج الصيني) مثال على عدم احترام الخصوصية في تحقيق هدف الأمن، فإن ذلك يعني سيطرة الحكومة الكاملة على جميع موارد الإنترنت" ، لذلك تم اعداد هذا الدليل الذي يعتبر مدخل بسيط للأمن الرقمي الخاص بالمدافعين عن حقوق الانسان وهو يحميهم لاسيما في اوقات الازمات وايضا يساعدهم في اتخاذ الاحتياطات وحماية الملفات الخاصة بهم من الاختراق يقدم الدليل ايضا ارشادات ونصائح من اعداد جمعية الامل العراقية / مشروع النماء لحقوق الانسان وقد استند في اعداد مصادره الى موقع الحماية الرقمية للمدافع البحريني و مستشار الأمن الرقمي محمد المسقطي .

عن جمعية الأمل العراقية

جمعية الأمل العراقية، منظمة غير حكومية، إنسانية، تنموية، لا حزبية وغير ربحية، تستند إلى العمل التطوعي لتحقيق المنفعة العامة للمواطنين العراقيين كافة دون تمييز، تأسست في العام 1992 في خضم الظروف المروعة التي شهدتها البلاد أعقاب حرب الخليج الثانية، بهدف توفير العون لتخفيف معاناة الشعب العراقي، وإقامة مجتمع عادل وديمقراطي في العراق، بدأت الجمعية عملها في منطقة كردستان، حيث تم تنفيذ العديد من البرامج والمشاريع، وفي أيار 2003 أفتتح المكتب الرئيس لها في بغداد، وتقدم نشاطاتها وخدماتها في جميع أنحاء العراق.

كيف تهدد سياسات الأمن الرقمي حقوق الإنسان

العرب الثلاثاء 27/10/2020

للمزيد حول موقع الحماية الرقمية
www.digital-protection.tech

للمزيد حول مدافع حقوق الانسان البحريني محمد المسقطي
www.digital-protection.tech/about-us

للمزيد من المعلومات زيارة الموقع الالكتروني الخاص بالجمعية
www.iraqi-alamal.org

www.iraqi-alamal.org

عن/مشروع النماء لحقوق الإنسان

مشروع النماء لحقوق الإنسان، هو أحد مشاريع جمعية الأمل العراقية وبتمويل مباشر من الاتحاد الأوروبي، فكرة وطموح منذ العام 2004 لم تجد طريقها للدعم والتمويل حتى 2013، عن طريق أقامة برنامج "بناء قدرات منظمات المجتمع المدني العراقية في مجال حقوق الإنسان" والذي استمر لغاية العام 2017، و برنامج حماية المدافعين عن حقوق الإنسان في مرحلته الثانية التي بدأت في العام 2018 وسيستمر حتى بداية العام 2023، يعمل المشروع بتخصص في موضوع تقديم الدعم والحماية وتطوير وبناء قدرات المدافعين/ات عن حقوق الانسان، وكذلك زيادة إنتاج التقارير الموضوعية والتعاقدية من قبل المشمولين بالمشروع بغية تحسين وضع حقوق الإنسان في العراق وتعزيزها واحترامها والحد من حالات انتهاك حقوق الإنسان.

هدف الدليل

يأتي هدف هذا الدليل في إطار برنامج حماية المدافعين عن حقوق الانسان الممول من الاتحاد الاوروبي والمنفذ من قبل جمعية الامل العراقية / مشروع النماء لحقوق الانسان لنشر الوعي في مجال الأمن الرقمي والحماية ضمن فئات المهتمين والمهتمات في النشاط المدني، لاسيما المدافعين والمدافعات عن حقوق الانسان الذين يعملون في إطار توثيق انتهاكات حقوق الإنسان ومنظمات المجتمع المدني والفرق التطوعية.

وقد جاء هذا الدليل كحصيلة لمجموعة من الورشات والخبرات التي تراكمت منذ سنوات عديدة، إذ تضمّنت تلك الورشات والخبرات طرح مفاهيم أساسية حول "الأمن الرقمي" بالإضافة لشرح خطوات عملية وتطبيقية حول تثبيت واستخدام أدواته الأكثر أهمية، إلى جانب عرض الحلول التي يمكن الاعتماد عليها بهدف الحفاظ على الخصوصية الرقمية وحماية المعلومات الحساسة، مما يتيح العمل في بيئة أمنة بعيدة عن مختلف انواع التهديدات من جهات عديدة ، ففي الوقت الذي أصبح فيه استخدام شبكة الإنترنت ووسائل التواصل الاجتماعي على وجه الخصوص حاجة يومية يستحيل الاستغناء عنها، برزت تحديات أمنية جديدة أمام المستخدمين، تكمن في حماية أنفسهم من منظومة مراقبة وتعقّب قامت بالتعدّي على خصوصياتهم،وحوّلت معلوماتهم الشخصية وبياناتهم اليومية إلى سلعة تجارية ربحيّة أحياناً، وإلى أدوات لتهديد استقرار دول والتدخّل في شؤونها في أحيان أخرى.

www.iraqi-alamal.org

ما الصلة بين الأمن الرقمي وحقوق الإنسان؟

لقد وفَّر الانترنت عدداً لا حصر له من طرق التواصل الجديدة والوصول إلى المعلومات، وأصبحنا اليوم على اتصال ببعضنا البعض أكثر من أي وقت مضى، وفي كل مرة نستخدم فيها الانترنت، سواء بتنزيل تطبيق ما على هاتفنا المحمول، أو بإرسال رسالة إلكترونية أو نشر تعليق على وسائل التواصل الاجتماعي، فإننا نبثُّ معلومات عن أنفسنا.

إن رسائلنا الإلكترونية والنصية ومكالماتنا الهاتفية قد تبدو غيرمهمة وغير مترابطة، ولكنْ إذا تم تجميع هذه الأمور الصغيرة في حياتنا، فإنها يمكن أن تُستخدم لتكوين صورة تفصيلية عنا: معتقداتنا، هويتنا، ما نحب، ما نكره، المكان الذي نعيش فيه، تنقلاتنا، الجمعيات التي ننتسب لها، وغير ذلك وعلى الرغم من أن بعض الأشخاص ربما يكون لديهم فهم عميق لكيفية عمل التكنولوجيا، فإنهم ربما لا يتمتعون بفهم عميق لحقوق الإنسان وبالمثل، فإن الأشخاص الذين يتمتعون بمعرفة معمقة لحقوق الإنسان، قد لا يفهمون فعلاً كيف تؤثر التكنولوجيا عليهم. إن حقوقنا الإنسانية تواجه مخاطر حقيقية في الحقبة الرقمية، إننا جميعاً بحاجة ملحَّة للتعلم واكتساب الأدوات والاستراتيجيات من أجل تعزيز أمننا الرقمي والدفاع عن أنفسنا في مواجهة الأنواع الجديدة من التهديدات.

عن الحق في الخصوصية

"لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمسّ شرفه وسمعته، ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات."

المادة 12 من الإعلان العالمي لحقوق الإنسان

أهمية الأمن الرقمي

تأتي أهمية الأمن الرقمي لحماية بياناتنا من التهديدات الالكترونية المتمثلة بما يلي:

1 البرمجيات الخبيثة : Malware

هي برمجيات مصممة للقيام بأفعال غير مرغوب بها على جهاز المستخدم دون علمه أو موافقته بهدف إيذائه، وقد تعمل هذه البرامج على سرقة كلمات السر أو تسجيل أنشطة المستخدم بشكل سري أو حذف بياناته، ويتراوح أذاها بين مجرد عرض الإعلانات، إلى تدمير القرص الصلب وعرقلة نظام التشغيل، ومن أشهرها: الفيروسات، والديدان، وأحصنة طروادة.

2 برمجيات التجسس Spyware

وهي البرامج التي تنقل معلومات من جهاز المستخدم إلى مكان آخر عبر شبكة الإنترنت دون علمه، عبر مراقبة الكتابة، أو المواقع الإلكترونية التي يزورها، وتجميع المعلومات الشخصية المتنوعة عنه، وقد يكون ذلك بهدف سرقة المعلومات مثل كلمة المرور، أو التجسس لأغراض تجارية وهي ليست برامج نقوم بتنصيبها، وإنما إحدى الإضافات التي قد تكون موجودة مع برنامج آخر، وتكون عادًة مخفيّة عن أنظار المستخدمين.

3 التصيد Phishing

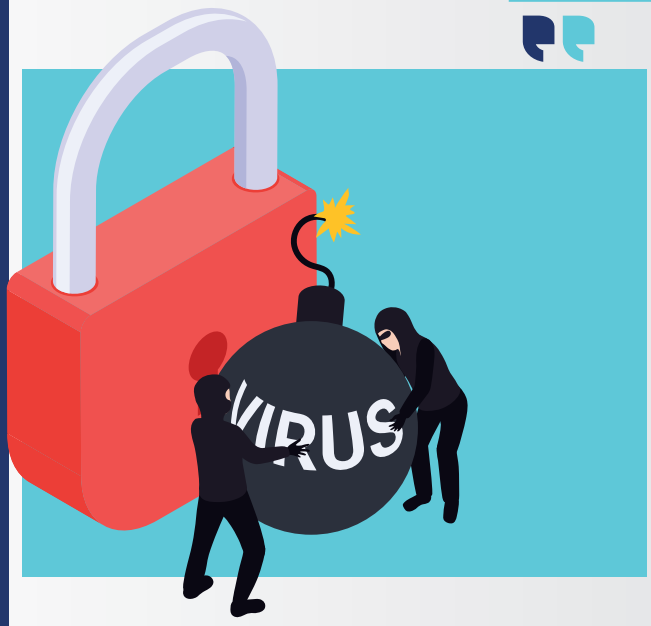
وهو محاولة للحصول على معلومات شخصية أو مالية للشخص المستهدف، عن طريق إرسال رسائل إلكترونية زائفة قد تحتوي على روابط تقوم بتوجيه المستخدم إلى مواقع الكترونية مُصمّمة خصيصاً لسرقة معلومات المستخدم، كما قد يقوم المتصيد بتحميل برامج خبيثة على جهاز الضحية تسمح له بالوصول إلى معلوماته، أو قد يستخدم أسلوب الهندسة الاجتماعية دون اللجوء إلى أي أدوات وذلك عبر خداع الضحية واستدراجه للحصول على المعلومات المطلوبة

4 هجمات الفدية attacks Ransom

سُمّيت بذلك لأنها تعمل على تشفير بيانات حاسوب الضحية يتبعها عملية ابتزاز للضحية لدفع مبلغ من المال مقابل فك التشفير، بدون وجود أي ضمانات حقيقية لفك التشفير في حال إرسال المبلغ.

ومن الطرق التي يعتمدها القراصنة للإختراق:

رسالة بريد إلكتروني تتضمّن مرفقًا مُلوثًا بالفيروس، الروابط الملغومة، المواقع الوهمية.



5 انتحال الشخصية Identity User Falsifying

"(ع.س) ناشطة من محافظة ديالى، كانت احدى ضحايا انتحال الشخصية، حيث قام احد الاشخاص بأنتحال صفتها واسمها وصورها واستخدمها في مواقع التواصل الاجتماعي مع اشخاص تعرفهم بالحقيقة مما كان عرضها حينها لبعض المخاطر، لكن استطاعت بغلق الحساب من خلال التبيلغ عليه." يعمد منتحل الشخصية إلى استخدام هوية شخص آخر في العالم الافتراضي، وذلك بهدف الحصول على معلومات سرية أو أمنية أو مبالغ مالية مستخدمًا معلومات غير صحيحة أو غيرها من المعلومات التي قد تكون متاحة على مواقع التواصل الاجتماعي، والتي يرى فيها المنتحلون كنزاً معروضًا أمامهم لاستخدامها في عملياتهم الاحتيالية، أو قد يقوم المنتحل بإرسال رسالة تتضمن روابط صفحات مشابهة تمامًا للموقع الأصلي طالباً من المستخدم معلومات معيّنة عنه، كأن يطلب تحديث بياناته البنكية أو معلومات سرّية أخرى، وفي أحيان أخرى قد يلجأ المنتحل إلى الاتصال المباشر بالشخص المستهدف وطلب معلومات سرية بحجة أنه بحاجة إليها لتحديث النظام كونه يعمل في شركة الاتصالات.

الخصوصية والسرية

من حقّ كلّ شخص الاحتفاظ بمعلوماته مخفية عن الآخرين الا ما ارتضى إظهارها، كما من واجب الآخرين الاعتراف له بهذا الحق وحفظه، ولكن استخدام الحاسوب والانترنت على نحو واسع أتاح الدخول السهل والسريع للمعلومات، وحتى ما هو منها خصوصي أو سري صار بإمكان المتطفلين أو ذوي النوايا الخبيثة الوصول إليه واستغلاله لغايات استفزازية أو ربحية.

وتؤدي مثل هذه الانتهاكات والتي تعتمد على الاستخدام السلبي للإنترنت ووسائل التواصل الاجتماعي واستغلالها لأغراض غير قانونية وغير أخلاقية إلى إلحاق الضرر بالأفراد، ويتعدّاه ذلك إلى الضرر العام بالدول، إذ أصبحت المواقع الإلكترونية الحساسة مثل تلك الخاصة بأجهزة الدولة والتي تحمل ملفات سرية في غاية الأهمية، عرضة للاختراق، الأمر الذي حوّل هذه الاعتداءات إلى حروب إلكترونية بين الدول.

وفي حين تسعى قوانين الجرائم الإلكترونية المطبّقة في بعض الدول للحفاظ على الخصوصية والأمان لمستخدمي الإنترنت، تبقى هذه القوانين غائبة في دول أخرى، وبشكل عام تقع على مستخدمي الإنترنت مسؤولية حفظ أمنهم الرقمي بشكل شخصي وحماية معلوماتهم الخاصة والسرية عن طريق أخذ الاحتياطات اللازمة.

للمعلومات مستويات عدة تتراوح بين العام والخاص والسري، وإن كل المعلومات مهما كانت طبيعتها قابلة للاستخدام، لذلك فمن الضروري الأخذ بعين الاعتبار تمييز مستوى المعلومة حسب المتلقي، وعدم الاستهتار بأية معلومة يمكن خسارتها.

"يُجرّم القانون في العديد من الدول درجات معينة من انتهاك الخصوصية الفردية، بينما تقوم حكومات كثيرة في نفس الوقت بانتهاك خصوصية الأفراد من خلال التجسس عليهم"

يمكن التفريق بين مفهومي الخصوصية والسرية الإلكترونية على النحو التالي:

السرية : هي حالة حفظ أو الاحتفاظ بالمعلومة مخفية إلا عن الأشخاص المخوّلين بالاطلاع عليها. ومن الأمثلة على المعلومات التي يجب الحفاظ على سريتها: كلمات مرور الحسابات الالكترونية والبنكية.

الخصوصية : هي الحد الذي يفصل بين ما يحق للمجتمع (الآخرين (معرفته عن حياتنا الخاصة وما لا يحق لهم معرفته. وفي تعريف آخر: هي قدرة أو حق شخص أو مجموعة أن الأشخاص في البت بما يمكن نشره من معلومات عنهم على العلن وما لا يمكن نشره.

ويمكن للخصوصية على الإنترنت أن تتضمن معلومات محددة لشخصية مستخدم الإنترنت كتاريخ ميلاده وعنوانه ورقم هويته أو جواز سفره، أو معلومات غير محددة للشخصية مثل سلوك زائر ما لموقع ما على الإنترنت.

رغم اهتمام وسائل التواصل الاجتماعي بإعدادات الخصوصية واعتمادها آليات لتأمين هذه المواقع، إلا أنه لا توجد وسيلة لتوفير الحماية الكاملة لها، ويبقى من الضروري اتخاذ خطوات احترازية.

قد يستخدم المخترقون حيلًا للحصول على المعلومات السرية للأشخاص عبر حساباتهم على مواقع التواصل الاجتماعي، واستخدامها في أغراض غير مشروعة قد تصل إلى ارتكاب جرائم كالابتزاز والاحتيال المصرفي والاستغلال الجنسي.

وتحتوي وسائل التواصل الاجتماعي على ثغرات تمكن من يمكن اعتبارهم طرفًا ثالثًا من الوصول إلى المعلومات الخاصة.

فعلى سبيل المثال: تتضمن الخصوصية على موقع فيس بوك اختيار فيما إذا كنا نريد أن يكون المنشور عاماً أو مقتصراً على الأصدقاء، الا أن غالبية الأشخاص لديه عدد كبير من الأصدقاء الافتراضيين دون معرفتهم في العالم الحقيقي، ومن الصعب التعرف على من قد يقوم بانتهاك خصوصية معلوماتنا كإعادة نشرها أو استخدامها دون معرفتنا.

الهندسة الاجتماعية

"(س.ص) ناشطة في مجال حقوق الانسان من محافظة (ا) تقوم بنشر كافة المعلومات عن حياتها الشخصية وتقوم بتسجيل الدخول على مواقع التواصل الاجتماعي بأستمرار، تعرضت فيما بعد بسبب هذه السلوكيات الى هجمة تصيد الكترونية كادت ان تشكل خطر على حياتها، لولا انها تلافت الهجمة بالاجراءات والنصائح المتبعة لحمايتها." لذا قد لا يكفي تحصين أجهزتنا ببرمجيات الحماية من القرصنة ومكافحة الفيروسات وغيرها لحمايتها من الاختراق الإلكتروني، فمع كل ما يمكن لمطوّري النظم الأمنية ابتكاره في هذا المجال، يبقى لجانب آخر ربما يكون أكثر أهمية دورًا في ذلك وهو العنصر البشري المتمثل بالمستخدم.

وقد يعتمد المخترق على العنصر البشري فقط للوصول إلى ما يريده من معلومات سرية مستخدمًا أساليب الحنكة والمكر، ومن دون أن تتوافر لديه بالضرورة معرفة تقنية عميقة، هذا الأسلوب هو ما بات يعرف بالهندسة الاجتماعية.

يمكن تعريف الهندسة الاجتماعية في سياق أمن المعلومات على أنها استخدام الخداع للتلاعب بالأفراد من أجل الكشف عن معلوماتهم السرية أو الشخصية والتي يمكن استخدامها لأغراض احتيالية.

وفي الأساس تُعرّف الهندسة الاجتماعية على أنها فن الوصول إلى المباني أو الأنظمة أو البيانات عن طريق استغلال علم النفس البشري بدلً من استخدام تقنيات القرصنة التقنية.

يُطوّر "المهندسون الاجتماعيون" بشكل مستمر أساليب جديدة لخداع ضحاياهم ومن أساليب الهندسة الاجتماعية:

1 استغلال الشائعات: يستغل المهندسون الاجتماعيون الشائعات والتي تنتشر بشكل سريع على وسائل التواصل الاجتماعي، كغلاف جذاب لتمرير محتواهم الخبيث، ليصبح كل من يساهم في نشر الشائعة عرضة لاختراق حساباته الاجتماعية وربما أجهزته.

2 استغلال عواطف الضحية وطباعه الشخصية: يستغل المهندس الاجتماعي عواطف الضحية من أجل جمع بيانات عنه، واستخدام هذه البيانات في الدخول إلى حساباته الشخصية ومواقع التواصل الاجتماعي الخاصة به. كأن يستخدم نصوصاً أو صوراً تخاطب عاطفة الضحية)انتقام، حقد، حب، شوق)،و تؤجج مشاعره الدينية أو القومية، وتوقعه في فخ فتح الرابط الخبيث.

3 استغلال المواضيع الساخنة: يستغل المهندسون الاجتماعيون المواضيع الساخنة التي تنتشر على شكل أخبار عاجلة بوسائل الإعلام لتمرير عملياتهم الاحتيالية، مستفيدين من اهتمام الجمهور بها مما يجعلها طعمً ملائمًا لإيهام الضحية بأنها روابط آمنة

4 استغلال موضوع الأمن الرقمي وضعف الخبرة التقنية للضحية: قد يعمد المهندس الاجتماعي لإنشاء حساب مستعار للتحايل على الضحية، كما قد يستغل ضعف خبرة الضحية بموضوع الأمن الرقمي عبر دفعه لفتح رابط أو ملف خبيث على أنه آمن.

5 انتحال الشخصية: يعمد المهندس الاجتماعي للتواصل المباشر مع الضحية عبر الهاتف أو من خلال إنشاء حسابات وهمية مطابقة لإسم صديق أو مقرب من الضحية ليقوم بعدها بالاستجرار التدريجي للمعلومات.

6 استغلال السمعة الجيدة لتطبيقات معينة: يقوم المهندس الاجتماعي بالإيحاء للضحية بأنّ ملفًا أو رابطًا هو نسخة محدّثة عن تطبيق معين بينما يكون رابطًا خبيثًا.

7 اصطياد كلمات السر: يعمد المهندس الاجتماعي إلى الخداع من أجل الحصول على كلمة سر الضحية، فقد يرسل إلى الضحية صفحة من تصميمه تشبه صفحة تسجيل الدخول لأحد المواقع الشهيرة من حيث الشكل، لكنها تحمل عنوانًا مختلفًا عن العنوان الأصلي، وعندما يُدخل الضحية كلمة السر للولوج في حسابه تصل بكل بساطة إلى المخترق ويكون الضحية قد وقع بالفخ دون أن يشعر بالخداع.

8 استغلال التواجد الفيزيائي للمهاجم قريبًا من الضحية: فعندما يتواجد المهندس الاجتماعي والضحية في نفس المكان يتمكن المهاجم من الوصول إلى جهاز الضحية عبرالحنكة. فقد يترك المهندس الاجتماعي نقطة الوصول WIFIمفتوحة عمدًا حتى يتصل بها الضحية فيخترق حاسوبه، أو قد يطلب منه توصيل بطاقة ذاكرة مع جهازه مما يفسح المجال أمام الملفات الخبيثة للانتشار في نظام الحاسوب وتدمير البيانات.

9 خيانة الثقة: قد يكون المهندس الاجتماعي صديقًا أو زميلً في العمل، يستغل الثقة الممنوحة له من الضحية لاختراق جهازه والتلصص عليه.

ماذا أفعل عند الوقوع ضحية للهندسة الاجتماعية؟

عادة يترافق الهجوم بأساليب الهندسة الاجتماعية بهجوم آخر ببرمجيات خبيثة مثلا، لذلك عندما يقع المستخدم ضحية للهندسة الاجتماعية عليه أن يقوم بخطوات تختلف تبعا لنوع الهجوم.

لكن بشكل عام يمكن القيام بالخطوات التالية:

- **إعلام الشخص المسؤول عن الأمن الرقمي في المؤسسة أو الزميل المختص بموضوع الأمن الرقمي**
- **تقييم الضرر والأشخاص المتأثرين**
- **إزالة آثار الهجوم**
- **إعلام الجهات**

(مؤسسات، زملاء، أصدقاء، معارف، أفراد عائلة) والتي من الممكن أن تكون قد تضررت أو تأثرت بسبب وقوع المستخدم ضحية للهجوم.

نصائح للحماية من الهندسة الاجتماعية:

- **التثقيف بمجال الأمن الرقمي وأساليب الاختراق المتجددة.**
- **تجنب إعطاء أي معلومات سرية أو بيانات شخصية إلا بعد التأكد من هوية الشخص المتحدث، وأن الاتصال تم من جهة رسمية أو معروفة.**
- **تجنب الحديث في الأسرار الشخصية مع الأصدقاء المجهولين عبر وسائل التواصل الاجتماعي.**
- **عدم فتح مرفقات البريد الإلكتروني المرسل من أشخاص غير معروفين.**
- **العمل على تأمين هواتفنا أو حواسيبنا واستخدام برامج لمكافحة الفيروسات.**

التصيد Phishing

هو محاولة الحصول على المعلومات الخاصة بمستخدمي الأنترنت سواء أكانت معلومات شخصية أو مالية، عن طريق الرسائل الإلكترونية أو مواقع الأنترنت التي تبدو وكأنها مبعوثة من شركات موثوقة أو مؤسسات مالية وحكومية، كالبنوك و غيرها و هي في الحقيقة مواقع وهمية و زائفة .

العديد من الأشخاص وقعوا ضحايا إلى الهجمات التي تسمى بالتصيد Phishing ومما أدى إلى أن يمنعوا من الوصول إلى حساباتهم و خصوصا على وسائل التواصل الاجتماعي .

Spear phishing

يتم توجيه الهجمات إلى أفراد أو شركات محددة، وعادة ما تستخدم المعلومات الخاصة بالضحية التي تم جمعها لتمثيل الرسالة بشكل أكثر نجاحًا باعتبارها أصلية.

قد تتضمن رسائل البريد الإلكتروني الخاصة بـ Spear phishing إشارات إلى زملاء العمل أو المديرين التنفيذيين في منظمة الضحية، وكذلك استخدام اسم الضحية أو موقعها أو غيرها من المعلومات الشخصية.

Whaling attacks

هي نوع من هجوم Spear phishing الذي يستهدف بشكل خاص كبار المديرين التنفيذيين داخل المؤسسة، وغالبًا ما يهدف إلى سرقة مبالغ كبيرة.

أولئك الذين يقومون بإعداد حملة للتصيد الاحتيالي يبحثون عن ضحاياهم بالتفصيل لإنشاء رسالة أكثر واقعية، حيث أن استخدام المعلومات ذات الصلة أو الخاصة بالهدف يزيد من فرص نجاح الهجوم.

Pharming

هو نوع من الخداع يعتمد على إعادة توجيه المستخدمين من موقع شرعي إلى موقع احتيالي، وخداع المستخدمين لاستخدام بيانات اعتماد تسجيل الدخول الخاصة بهم لمحاولة تسجيل الدخول إلى الموقع المخادع.

Voice phishing

المعروف أيضًا باسم vishing ، هو شكل من أشكال الخداع الذي يحدث عبر وسائط الاتصالات الصوتية، بما في ذلك الصوت عبر بروتوكول الإنترنت (VoIP) أو (POTS (خدمة الهاتف القديمة العادية، تستخدم عملية احتيال نموذجية برنامجًا لتركيب الكلام لترك رسائل البريد الصوتي المزعومة لإخطار الضحية بالنشاط المشبوه في أحد الحسابات المصرفية أو الائتمانية، وتطلب من الضحية الاستجابة إلى رقم هاتف ضار للتحقق من هويته.

SMS phishing

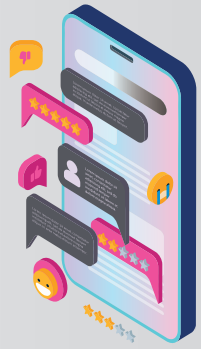
والذي يطلق عليه أحيانًا اسم SMishing أو SMShing ويستخدم الرسائل النصية لإقناع الضحايا بالكشف عن بيانات اعتماد الحساب أو تثبيت البرامج الضارة

DIGITAL PROTECTION
الحماية الرقمية

الوقاية منه

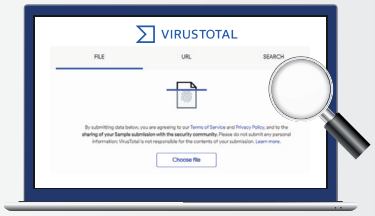
1 في الرسائل الإلكترونية للتصيد، قد يشجعك المهاجم على النقر على رابط أو فتح مرفق وقد يطالبك بتحديث بيانات من المهم التحقق من سلامة الروابط والملفات التي يتم إرسالها لك عبر البريد الإلكتروني أو الدردشة خصوصا اذا كانت من مصادر غير موثوقة لك.

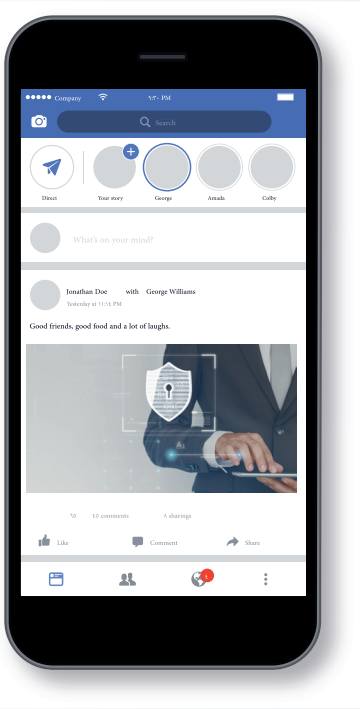
يستخدم موقع virustotal لفحص الروابط والملفات والتأكد من نظافتها من الفايروسات والبرامج الخبيثة ينصح باستعماله قبل فتح الروابط والملفات غير الموثوقة وكالتالي:



لفحص ملفات اضغط على تبويب File وقم بتحميل الملف عبر الضغط على Upload and scan file ان لا يتجاوز حجم الملف 125MB ثم سيقوم الموقع بتحميل الملف واجراء مسح عليه مجموعة من برامج مكافحة الفايروسات تقريبا 58 برنامج وبعدها يقوم بإعطاء تقرير لك يبين ان الملف نظيف او مصاب.

لفحص الروابط اختار تبويب URL وقم بنسخ الرابط ووضعة في المكان المخصص واضغط على Scan وسيقوم الموقع بفحص الرابط ويظهر لك تقرير يبين اذا كان

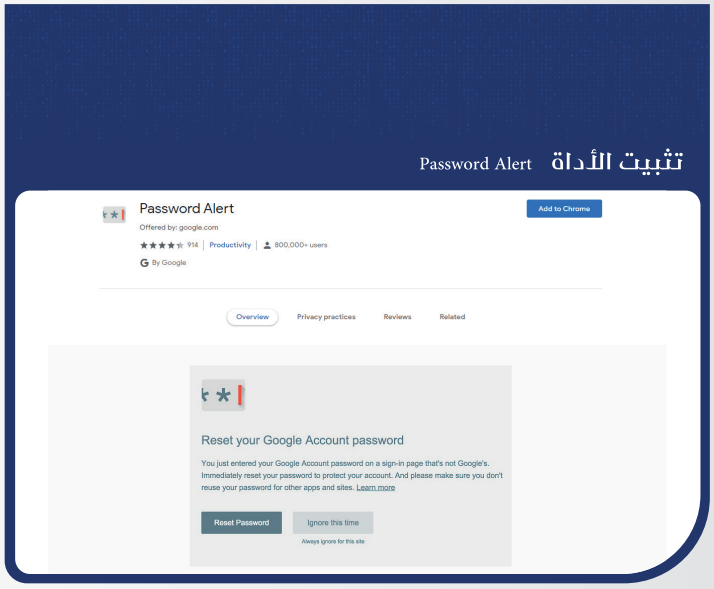




2 يجب التأكد من عناوين البريد الالكتروني المستلمة ومن اسماء المواقع الالكترونية للتأكد من انها صحيحة قد، قد تصلك رسالة مزيفه من تويتر تطالبك بتحديث بياناتك وعند قراءة البريد المرسل تجده no-replay@ttwiter.com حيث ان اغلب الهاكر يستخدمون دومين مشابه لمحتوى الرسالة، يمكن لعناوين الويب في البريد الإلكتروني أن تكون خادعة. قد تبدو عناوين الويب على أنها تدل لموقع ما، ولكن إذا حركت مؤشر الماوس فوقها لترى أين تدل، قد تظهر واجهة أخرى كلياً او قد تجد احيانا فرق بين عنوان الموقع الاصلي والمزيف إذا دققت جيدا، مثلا تجد عنوان موقع الفيسبوك كالاتي https://www.faceebook.com/ لذلك يجب ان تعرف العنوان الصحيح من المزيف للمواقع التي تستعملها ومواقع التواصل الاجتماعي على الاقل، وفي هذه الحالات تجنب فتح هذه الايميلات او المواقع التي تسرق معلوماتك وخصوصا الايميلات التي تتضمن روابط عندما تفتحها تطالبك بإدخال الايميل والرقم السري ويقوم بسرقتها.

3 اذا كان هناك رابط بالايميل، عند التأشير عليه فقط ستجد الرابط الموجه اليه مختلف عن المكتوب بالرسالة.

4 ويمكن محاولة خداعك بطريقة أخرى عبر إرسال رابط لملف يُزعَم أنه مستضاف على خدمة مثل مستندات Google أو Dropbox وإذا فتحت الرابط قد تظهر صفحة تشبه صفحة تسجيل الدخول لتلك الخدمات، تدعوك لكتابة اسم المستخدم وكلمة السر. ولكن الرابط ربما يكون قد دل على موقع مزيف يحوي نسخة مماثلة لصفحة تسجيل الدخول. لذلك إذا كنت قد تبعت رابطاً يجب التحقق من شريط العنوان في المتصفح قبل كتابة أي كلمة سر. سيظهر الشريط العنوان الحقيقي الذي جاءت الصفحة منه. وإذا لم يطابق الموقع الذي يفترض أنك تقوم بتسجيل الدخول إليه، لا تتابع.



5 قد تصلك رسالة تنبهك بوجود فايروسات بجهازك ولابد من تحميل برنامج حماية ورابط لبرنامج معين لتثبيته، وللوقاية من المتصيدين يجب استخدام برنامج حماية من الفيروسات وجدار ناري (FireWall) مع تحديثه باستمرار والتأكد من تحديث نظام التشغيل والمتصفح باستمرار

والتأكد من الرابط دائما عند الدخول لأي موقع

يتطلب اسم مستخدم وكلمة مرور حيث تجد الرابط يبدأ بـ (https) وتعني التصفح الآمن بدون وجود حرف s في الأخير يكون التصفح غير امن و عدم فتح أي رابط تشك بعدم صحته سواء كان برسالة او بأي موقع من شخص مجهول هي إضافة الى متصفح كوكل كروم تساعدك على حماية حساب جوجل من السرقة أو الاختراق وذلك عن طريق عدم كتابة باسورد جوجل في أي موقع خلاف جوجل وبذلك تحميك من مواقع النصب وسرقة المعلومات الشخصية والتي تدعي أنها موقع جوجل الرسمي وتعمل على خداع المستخدم. فكرة عمل الإضافة هي التأكد من حماية المستخدم عن طريقة تنبيه يصلك يوضح أنك قمت بكتابة كلمة السر الخاصة بك في موقع خلاف جوجل وهو ما يحدث من بعض المجموعات والشركات الغير رسمية علي البريد الإلكتروني، حيث تعمل هذه الشركات علي خداع المستخدم عن طريق ادعاء انها شركة جوجل وتطلب البيانات الخاصة بالحساب.

وتقوم إضافة Password Alert كما يظهر من اسم الإضافة بإرسال تنبيه إليك يوضح لك "تم كشف باسورد جيميل في موقع أخر غير جوجل" وينصحك بضرورة تغير كلمة السر في الحال. ولكي تستفيد بالوظيفة التي توفرها الإضافة تحتاج بطبيعة الحال إلى متصفح جوجل كروم ثم تنصيب الإضافة من متجر كوكل بمجرد تنصيب الإضافة سوف تطلب منك تسجيل الدخول إلى حساب جوجل الايميل وكلمة السر.

ماذا تفعل إذا كنت ضحية "التصيد" Phishing؟

1. قم بتغيير كلمة السر حالا.
2. أبلاغ جميع الأصدقاء على وسائل التواصل الاجتماعي بهذه الحادثة والطلب منهم التوقف عن التواصل مع حسابك حتى يتم حمايته.
3. أطلب المساعدة من إدارة المواقع أو أتصل بالبنك لوقف الخدمة أو لإبلاغهم بالحادثة.
4. حاول تحذير الآخرين حول الموقع أو الخدمة أو البريد الإلكتروني الوهمي / الزائف الذي وصلك أو الذي قمت بالدخول إليه.

حماية حساباتك عبر تفعيل خاصية التحقق بخطوتين:

التحقق بخطوتين 2 step verification هي خاصية تساهم في تعزيز حماية حساباتك، إذ ان هذه الخاصية لا تسمح بالدخول الى الحسابات باستخدام كلمة السر فقط password بل تحتاج الى رمز إضافي بعد إدخالك الى كلمة السر الصحيحة ومما يساهم في منع اختراق حساباتك او الاستيلاء عليها.

التحقق بخطوتين بالإمكان تفعليها باستخدام عدة طرق :

رموز احتياطية Backup codes

تطبيق أداة المصادقة Authenticator app

الرسائل القصيرة SMS

مفتاح الأمان Security Key

رمز المرور Passcode

تطبيق
تنبيه كلمة المرور

التحقق بخطوتين FACEBOOK

الناشطة (ب،ق) من محافظة السليمانية لفترة طويلة تستخدم الفيسبوك لكنها قد انشاءت الحساب على رقم هاتف ولم تقم بخطوة التحقق بخطوتين، ورقم الهاتف قد بيع لشخص اخر وقد قام باسترداد رمز التفعيل وسرق حسابها، لكنها استطاعت استراجع حسابها باجراء التحقق بخطوتين ببقية الطرق

لذا اتبع الخطوات التالية:

1. قم بتسجيل الدخول الى حسابك في الموقع.
2. اذهب الى الاعداد واختار الأمان وتسجيل الدخول ثم اختار استخدام الطبقة الثنائية.
3. اختار نوع المصادقة الذي ترغب في تفعيله هناك عده انواع:
   - رسائل نصية.
   - مفتاح الأمان. وهو مفتاح يتم شراءه يكون usb .
   - أداة انشاء الرموز.
   - رمز الاسترداد.
4. يمكن تفعيل الخاصية بأحد الخيارات السابقة واذا اردت عبر برنامج Authenticator app من اختيار أداة انشاء الرموز اختار تطبيق خارجي واتبع الخطوات كما السابق لأضافه الرقم والتفعيل.

يمكن عمل التحقق بخطوتين للعديد من المواقع ومنها

لمراجعة الادلة التدريبية الخاصة بخاصية التحقق بخطوتين يرجى قراءة الباركود الخاص بكل برنامج .

تفعيل الخاصية في الواتسب Whatsapp

تفعيل الخاصية في الجيميل Gmail

تفعيل الخاصية في التويتر Twitter

تفعيل الخاصية في الفيسبوك Facebook

تفعيل الخاصية في انستغرام instagram

تفعيل الخاصية في الهوتميل Hotmail
اوت لوك Outlook

تفعيل الخاصية في السناب شات snapchat

www.iraqi-alamal.org

برنامج حفظ كلمات السر كي باس إكس KeePassx

كي باس اكس عبارة عن خزانة كلمات سر: أي برنامج يمكنك استخدامه من أجل تخزين كل كلمات السر الخاصة بك لكل المواقع والخدمات. خزانات كلمات السر ملائمة وتسمح بتنظيم كل كلمات السر في مكان واحد. خزانة كلمة السر أداة قوية لأنها تسمح باستخدام كلمات سر مختلفة يصعب تخمينها لكل الخدمات بدون الحاجة لتذكرهم. وبدلا من ذلك أنت تحتاج فقط إلي تذكر كلمة السر الرئيسية التي تسمح لك بفك شفرة قاعدة بيانات كلمات السر.

لتحميل البرنامج
من هنا

استخدام كي باس اكس:

بعد الانتهاء من تثبيت كي باس اكس قم بتشغيل البرنامج. بعد التشغيل، قم باختيار "قاعدة بيانات جديدة" من قائمة الملف. سيظهر صندوق حوار مطالبا بإدخال كلمة سر رئيسية و\أو استخدام ملف المفتاح. قم بتحديد الاختيار الأنسب لك. لاحظ إذا كنت تود رؤية كلمة السر التي تقوم بكتابتها (بدلا من تمويهها بنقط) قم بالنقر على الزر الذي يظهر رمز العين. لاحظ أيضا أن يمكنك استخدام أي ملف ليكون ملف المفتاح - صورة لقطة على سبيل المثال قد تستخدم كملف المفتاح. عليك التأكد فقط من أن الملف الذي قمت باختياره لا يتم تعديله لأنه إذا تم تغيير المحتوى فلن يعمل مرة أخرى لفك شفرة قاعدة بيانات كلمات السر. يرجى أيضا العلم بأن أحيانا فتح الملف على برنامج آخر قد يتسبب في تعديله. الممارسة الأفضل هو عدم فتح الملف إلا لفتح كي باس اكس. (ومع هذا فإن إعادة تسمية الملف أو نقله آمنا). بمجرد تهيئة قاعدة البيانات بنجاح، يجب عليك حفظها عن طريق اختيار حفظ قاعد البيانات من قائمة الملف.

للاطلاع على موضوع شامل عن كيفية استخدام البرنامج على الرابط وأيضا تتوفر مقاطع فيديو تعليمية عن البرنامج في اليوتيوب

(لاحظ أنه يمكنك نقل قاعدة بيانات كلمات السر لاحقا لأي مكان على القرص الصلب أو نقله إلي حواسيب أخرى حيث ستظل قادرا على فتح قاعدة البيانات باستخدام كي باس اكس وكلمة السر وملف المفتاح الذي قمت بتحديده من قبل).

// تنظيم كلمات السر"

يمكنك من خلال كي باس اكس من تنظيم كلمات السر إلي "مجموعات" وهي عبارة عن مجلدات. يمكن إنشاء وحذف وتعديل مجموعات أو مجموعات فرعية بالذهاب إلي مجموعات في شريط القوائم أو بالنقر يمينا على مجموعة في الجانب الأسير من نافذة كي باس اكس. إن تجميع كلمات السر في مجموعات لا يؤثر على أي من وظائف كي باس اكس حيث أنها مجرد أداة تنظيمية.

// تخزين\توليد\تحرير كلمات السر"

من أجل إنشاء كلمة سر جديدة أو تخزين كلمة سر تمتلكها، قم باختيار المجموعة التي تود أن تضيف لها كلمة السر وانقر يمينا واختر أضف مدخلة جديدة (ويمكنك أيضا اختيار "مدخلات" ثم أدخل مدخلة جديدة من شريط الأدوات). من أجل الاستعمالات الأساسية لكلمة السر، أتبع التالي:

- أدخل عنوان وصفي بحيث يمكنك من خلال حقل "العنوان" التعرف على كملة السر المدخلة.
- أدخل أسم المستخدم المرفق مع مدخلة كلمة السر في حقل أسم المستخدم (يمكنك ترك الحقل فارغا إذا لم يوجد اسم مستخدم.)
- أدخل كلمة السر في حقل "كلمة السر". إذا كنت تقوم بإنشاء كلمة سر جديد (على سبيل المثال: أنك تقوم بتسجيل الدخول إلي موقع جديد وتريد إنشاء كلمة سر جديدة وفريدة وعشوائية) قم بالنقر على زر "ولّد". هذا الزر سوف يفتح لك مولد كلمة السر في نافذة يمكنك من خلالها توليد كلمة سر عشوائية. توجد عدة خيارات في تلك النافذة من بينها أنواع الرموز التي تتضمنها كلمة السر والطول.

لاحظ أنه في حالة توليد كلمة سر عشوائية ليس عليك تذكرها (أو حتى معرفتها!). كي باس اكس يخزنها بالنيابة عنك وفي أي وقت تحتاج لها ستتمكن من نسخها ولصقها في البرنامج الملائم. وهذا هو الغرض الكلي من خزانة كلمات السر - إمكانية استخدامك لكلمات سر طويلة عشوائية لكل موقع\خدمة، دون حتى معرفة ما هي كلمات السر.

ولهذا السبب يتوجب عليك جعل كلمة السر طويلة بنفس الطول المسموح به على الخدمة، وأن تستخدم رموز متنوعة كلما أمكن.

بعد الانتهاء من تحديد الاختيارات المرضية لك، أنقر على "ولّد" ثم أضغط على تم. بعد ذلك سيتم كتابة كلمة السر التي تم توليدها في حقل كلمة السر وحقل إعادة الكتابة. (إذا لم تقم بتوليد كملة سر عشوائية، سيتعين عليك أن تقوم بكتابة كلمة السر المختارة مرة أخرى في حقل الإعادة.

أخيرا، أضغط على تم. الآن كلمة السر الخاص بك مخزنة في قاعدة بيانات كلمة السر. للتأكد من أنه تم حفظ التغييرات، تأكد من حفظ قاعدة بيانات كلمة السر المحررة بالذهاب إلي قائمة ملف ثم حفظ قاعدة البيانات. (إذا قمت بعمل خطأ يمكنك أن تغلق قاعدة البيانات وتعيد فتحها وسيتم تجاهل كل التغييرات).

إذا احتجت إلي تغيير\تحرير كلمة السر المخزنة، يمكنك اختيار المجموعة التي تنتمي لها كلمة السر ثم الضغط على العنوان مرتين في الجانب الأيمن، وسيظهر صندوق "مدخلة جديدة" مرة أخرى.

الاستخدام العادي

من اجل استخدام إحدى المدخلات في قاعدة بيانات كلمات السر، أنقر ببساطة يمينا على المدخلة وأختر "أنسخ أسم المستخدم إلي الحافظة الوسيطة" أو أنسخ كلمة السر إلي الحافظة الوسيطة" ثم أذهب إلي النافذة\الموقع حيث ستقوم بإدخال أسم المستخدم\كلمة السر وقم باللصق في الحقول الملائمة. (بدلا من النقر يمينا على المدخلة يمكنك القيام بنقرة مزدوجة على أسم المستخدم وكلمة السر في المدخلة، وسيتم نسخ أسم المستخدم أو كلمة السر تلقائيا في الحافظة الوسيطة).

الاستخدام المتقدم

واحدة من أكثر الميزات المفيدة في كي باس اكس هو إمكانية كتابة أسم المستخدم وكلمة السر تلقائيا في أي برنامج عندما تقوم بالضغط على مزيج واختصار خاص من المفاتيح على لوحة المفاتيح. يرجى ملاحظة أن هذه الميزة متاحة فقط على لينكس. وتوجد برامج أخرى لإدارة كلمات السر مثل كي باس (الذي بني عليه كي باس اكس) التي تدعم هذه الميزة على أنظمة تشغيل أخرى وتعمل على نفس النحو.

لتفعيل هذه الميزة، قم بالتالي:

قم باختيار Global Hotkey. ثم أختر الإعدادات من شريط الإضافات، ثم اختر "متقدم" على الجانب الأيسر. أنقر داخل حقل "Global Auto-Type Shortcut" ثم أضغط على المفاتيح المختصرة التي تود في استخدامها. (على سبيل المثال: يمكنك الضغط باستمرار على Ctrl وAlt وShift ثم أضغط على p، يمكنك استخدام أي مزج تفضله ما بين المفاتيح ولكن يتعين عليك التأكد من عدم تضاربه مع استخدامات مفاتيح مختصرة لبرامج أخرى. وبالتالي تجنب أشياء مثل Ctrl+X أو Alt+F4.) وبعد الانتهاء أضغط تم.

قم بإعداد Auto-Type for a Specific Password. تأكد من فتح النافذة التي تود إدخال كلمة السر فيها. ثم أذهب إلي كي باس اكس، أبحث عن المدخلة التي تود تفعيل Auto-Type خاص بها وثم قم بنقرة مزدوجة على عنوان المدخلة لتفتح صندوق "مدخلة جديد".

أضغط على زر Tools ثم اختر "Auto-Type: Select Target Window". ستظهر نافذة بها قائمة منسدلة، أنقر عليها واختر عنوان النافذة التي تود أن تدخل فيها أسم المستخدم وكلمة السر. بعد ذلك أنقر على تم، ثم أنقر على تم مرة أخرى، قم بتجربتها!.

الآن لكي تتمكن من كتابة أسم المستخدم وكلمة السر بشكل تلقائي اذهب إلي النافذة\الموقع الذي تريد من كي باس اكس أن يقوم بكتابة أسم المستخدم\كلمة السر بالنيابة عنك. تأكد من أن المؤشر في حقل أسم المستخدم، ثم أضغط على مزيج المفاتيح الذي قمت بتحديده منذ قليل. وسيتم إدخال أسم المستخدم وكلمة السر تلقائيا، طالما كان برنامج كي باس اكس مفتوحا (حتى لو لم يكن نشط أو نافذته مصغرة).

يرجى ملاحظة أن هذه الميزة قد لا تعمل 100٪ بشكل صحيح وذلك وفقا لكيفية بناء الموقع\النافذة (فقد تقوم على سبيل المثال بإدخال أسم المستخدم وليس كلمة السر). يمكنك التدخل لاكتشاف وحل المشكلة. لمزيد من المعلومات ننصح بالاطلاع على توثيق كي باس (بالرغم من وجود بعض الاختلافات بين كي باس وكي باس اكس، إلا أن الصفحة سوف تكون كافية لترشدك إلي الاتجاه الصحيح).

ينصح أن تقوم باستخدام مزيج من المفاتيح يصعب نقرهم بدون قصد. فأنت لا تريد أن تقوم بلصق كلمة السر الخاصة بحسابك البنكي في منشور على فيسبوك!.

ميزات أخرى

تستطيع القيام بالبحث في قاعدة البيانات بكتابة شيء في صندوق البحث (حقل النص الموجودة في شريط الأدوات على نافذة كي باس اكس الرئيسية). يمكنك أيضا ترتيب المدخلات بالضغط على رأس العمود في النافذة الرئيسية.

كما يمكنك "قفل" كي باس اكس بالذهاب إلي قائمة الملف ثم اختيار Lock Workspace، حتى تتمكن من ترك كي باس اكس مفتوحا وجعل البرنامج يطلب كلمة السر الرئيسية (و\أو مفتاح الملف) قبل النفاذ إلي قاعدة بيانات كلمات السر مرة أخرى.

ويمكنك إعداد قفل تلقائي في كي باس اكس ليعمل بعد مرور وقت من عدم النشاط، فهذا قد يمنع شخص آخر من النفاذ إلي كلمات السر إذا ذهبت بعيدا عن الحاسوب. لتفعيل هذه الخاصية قم باختيار قائمة "إضافات" من شريط الأدوات ثم اختار إعدادات من القائمة ثم أنقر على اختيارات الآمان. ثم قم بتفعيل زر الاختيار الذي يقول "Lock database after inactivity of {number} seconds".

كي باس اكس يمكن أن يقوم بتخزين أكثر من مجرد أسماء المستخدمين وكلمات السر. فعلى سبيل المثال، يمكنك إنشاء مدخلات لتخزين أشياء هامة مثل أرقام الحسابات أو أرقام منتج

أو أرقام متسلسلة أو أي شيء. لا يوجد شرط أن تكون البيانات التي تدخلها في حقل "كلمة السر" عبارة عن كلمات سر فعلية. قد تكون أي شيء تريده - قم بإدخال ما تريد حفظة في حقل "كلمة السر" بدلا من كلمة سر حقيقية (واترك حقل أسم المستخدم فارغا في حالة عدم وجود أسم مستخدم) وسيقوم كي باس اكس بتذكره بشكل آمن لك.

كي باس اكس سهل الاستخدام وبرمجية قوية، وننصح باستكشاف البرنامج لتعلم كل الأشياء المفيدة التي يمكن أن يقوم بها.

لتفعيل هذه الميزة، قم بالتالي:

قم باختيار Global Hotkey. ثم أختر الإعدادات من شريط الإضافات، ثم اختر "متقدم" على الجانب الأيسر. أنقر داخل حقل "Global Auto-Type Shortcut" ثم أضغط على المفاتيح المختصرة التي تود في استخدامها. (على سبيل المثال: يمكنك الضغط باستمرار على Ctrl وAlt وShift ثم أضغط على p، يمكنك استخدام أي مزج تفضله ما بين المفاتيح ولكن يتعين عليك التأكد من عدم تضاربه مع استخدامات مفاتيح مختصرة لبرامج أخرى. وبالتالي تجنب أشياء مثل Ctrl+X أو Alt+F4.) وبعد الانتهاء أضغط تم.

قم بإعداد Auto-Type for a Specific Password. تأكد من فتح النافذة التي تود إدخال كلمة السر فيها. ثم أذهب إلي كي باس اكس، أبحث عن المدخلة التي تود تفعيل Auto-Type خاص بها وثم قم بنقرة مزدوجة على عنوان المدخلة لتفتح صندوق "مدخلة جديد".

أضغط على زر Tools ثم اختر "Auto-Type: Select Target Window". ستظهر نافذة بها قائمة منسدلة، أنقر عليها واختر عنوان النافذة التي تود أن تدخل فيها أسم المستخدم وكلمة السر. بعد ذلك أنقر على تم، ثم أنقر على تم مرة أخرى، قم بتجربتها!.

الآن لكي تتمكن من كتابة أسم المستخدم وكلمة السر بشكل تلقائي اذهب إلي النافذة\الموقع الذي تريد من كي باس اكس أن يقوم بكتابة أسم المستخدم\كلمة السر بالنيابة عنك. تأكد من أن المؤشر في حقل أسم المستخدم، ثم أضغط على مزيج المفاتيح الذي قمت بتحديده منذ قليل. وسيتم إدخال أسم المستخدم وكلمة السر تلقائيا، طالما كان برنامج كي باس اكس مفتوحا (حتى لو لم يكن نشط أو نافذته مصغرة).

يرجى ملاحظة أن هذه الميزة قد لا تعمل 100٪ بشكل صحيح وذلك وفقا لكيفية بناء الموقع\النافذة (فقد تقوم على سبيل المثال بإدخال أسم المستخدم وليس كلمة السر). يمكنك التدخل لاكتشاف وحل المشكلة. لمزيد من المعلومات ننصح بالاطلاع على توثيق كي باس (بالرغم من وجود بعض الاختلافات بين كي باس وكي باس اكس، إلا أن الصفحة سوف تكون كافية لترشدك إلي الاتجاه الصحيح).

ينصح أن تقوم باستخدام مزيج من المفاتيح يصعب نقرهم بدون قصد. فأنت لا تريد أن تقوم بلصق كلمة السر الخاصة بحسابك البنكي في منشور على فيسبوك!.

كيف تعرف أن هاتفك مخترق او مراقب؟

في الفترة الاخيرة اصبحت عمليات الاختراق و المراقبة للهواتف الذكية في زيادة مستمرة مما يهددنا على المستوى العام والخاص, فهناك من يقوم بالاختراق للمراقبة وسرقة المعلومات والبيانات وتظهر المشكلة اذا كانت تلك المعلومات خاصة جدًا او سرية او اذا كانت معلومة مالية او تجارية او يكون الاختراق والمراقبة بغرض اللهو، هنا توجد معلومة خاطئة لدى البعض وهى اننا لا نستطيع معرفة هل الهاتف مخترق ومراقب ام لا و هي معلومة خطأ اذ نستطيع باتباع بعض الطرق معرفة ان الهاتف مخترق و مراقب، لكن يجب ان تتعرف ولو بشكل عام على ملف التجسس او الفيروس الذي يقوم بعملية الاختراق، هو عبارة عن ملف صغير الحجم يتم تثبيته في البرامج المحملة على الهاتف و غالبًا يأتي في شكل اعلانات لذا فإن الشركة المنتجة لبرنامج التشعيل اندرويد تحذر من تحميل اي برامج او تطبيقات خارج السوق المخصص للشركة وان فيروس او برمجية الاختراق يمكن ان تقوم بالتوجه الى الاستوديو والقيام بسرقة الصور والفيديوهات وجهات الاتصال كما يمكن ان يدخل الى المحادثات في الفيس بوك والواتس اب وتستطيع التعرف ان كان هاتفك مخترق و مراقب ام لا بأحدى الطرق التالية:

1- قم بفتح الهاتف الخاص بك وتوجه الى اعدادت الهاتف و منها توجه الى التطبيقات ثم الى ادارة التطبيقات وابدأ في البحث في التطبيقات على هاتفك وفي حال لاحظت وجود اي برنامج او تطبيق غريب انت لم تقم بتحميله على الهاتف قم بحذفه مباشرة.

2- قم بالدخول على اعدادات الهاتف ثم منها توجه الى عداد البيانات وهنا ستظهر امامك البيانات التي تعمل على استهلاك السرعة بشكل كبير في الانترنت فالفيروسات عادة تحتاج الى سرعة عالية حتى تقوم بتحميل مما يترتب عليه بطئ الانترنت وبعد ان حددت البيان او التطبيق المستهلكة للطاقة افتح الاعدادات ومنها افتح ادراة التطبيقات وتوجه الى التطبيق المستهلك للطاقة وقم بحذفه مباشرة، ونتيجة لانه يوجد اتصال مستمر بين جهازك وجهاز المخترق فإن باقة بيانات الانترنت تنفذ بشكل سريع.

3- توجه الى اعدادات الهاتف ومنها الى البطارية وراقب البرامج او التطبيقات ولاحظ اي منها يستهلك البطارية بشكل كبير وهنا قم بازالة التطبيق مباشرة.

4-. لاحظ دائمًا صوت رنين الهاتف عند الاتصال باي شخص فان كان الرنين متكرر او بمعنى ادق يوجد به ما يشبه الصدى اذا فهذا الهاتف مراقب و هنا يجب ان نعرف بأن تقنيات مراقبة الهواتف غالبًا لا يمتلكها الاشخاص وانما الحكومات.

5- الرسائل النصية الغريبة حيث ان المخترق يقوم بأرسال الأوامر او التعليمات الى هاتفك في شكل رسائل نصية على شكل ارقام وحروف غير مفهومة.

6- الارتفاع المفاجئ في درجة حرارة الهاتف فعادة ترتفع درجة حرارة الهاتف مع اللعب او الاستخدام الطويل للهاتف اما مع الارتفاع المفاجئ لحرارة الهاتف فإن ذلك مؤشر على احتمالية وجود اختراق للهاتف.

7- الهاتف يتصرف بغرابة حيث من الممكن ان تلاحظ ان الهاتف يضئ او ينطفئ اوتوماتيكيًا او يصدر اصوات غريبة.

8- سماع اصوات غريبة اثناء المكالمات كأن تسمع صوت نغمات متقطعة مما يدل على ان المكالمة يتم تسجيلها.

9- التأخر في اطفاء الهاتف حيث انه عندما تحاول إطفاء الهاتف اكثر من مرة وتلاحظ ان الهاتف يستغرق وقت طويل حتى يستجيب لامر الاطفاء فهذا يدل على ان هناك من يتحكم بالهاتف غيرك.

بالطبع لا يعني وجود اي علامة مما سبق ان الهاتف مخترق بشكل حتمي وانما وجودها يعني بأن هناك احتمال كبير بأن الهاتف مخترف او خاضع للمراقبة, لكن بصورة عامة لتحمي هاتفك من الاختراق او المراقبة حاول ان تقوم بعمل فورمات لهاتفك من وقت لآخر, راعي عدم تحميل البرامج العشزائية حتى وان كانت برامج حماية, هناك العديد من البرامج الخاصة بالاندرويد التي تستطيع الكشف ان كان الهاتف مراقب ام لا.

غالبًا ما تتضمن هذه الهجمات هجمات على حسابات عبر الإنترنت ، مثل Google أو Facebook أو Microsoft ، لأن هذه الحسابات تحتوي على الكثير من المعلومات وتسمح بالتواصل علنًا أو بشكل خاص مع مجتمعات كبيرة.

يمكنكم معرفة هذا الامر عبر دليل تدريبي يهدف إلى توفير منهجية للتحقق من بعض العناصر في الحسابات التي توضح تعرض الحساب للاختراق.

للاطلاع هذا الدليل يرجى قراءة الكود التالي

اندرويد: تعمية- تشفير- الصور والفيديو والبيانات في جهازك

في جميع أنحاء العالم، يواجه الصحفيون والمدافعون عن حقوق الإنسان مستويات متزايدة من القمع الجسدي، حيث يتم تفتيش الأجهزة المحمولة أو مصادرتها عند المعابر الحدودية والمطارات أو نقاط التفتيش أو في الشوارع أو في المداهمات المستهدفة. في الوقت نفسه، تهدد المراقبة والرقابة الرقمية تدفق المعلومات من المناطق القمعية، لاسيما بشأن العنف وانتهاك حقوق الإنسان أو الفساد، لذلك تم اعداد الدليل التدريبي من أجل حماية المعلومات في الهواتف التي تعمل بنظام Android ومن خلال تشفيرها بشكل سهل (الصور والفيديو والوثائق والتسجيلات الصوتية).

للاطلاع على الدليل
يرجى قـراءة الكـود ادناه

الحماية على أنظمة تشغيل أبل

لعدة سنوات ، كانت تعد أجهزة الآيفون من شركة أبل ، الأكثر أمانا من بين أجهزة الهواتف الذكية الأخرى. و لكن بالرغم من هذه السمعة ، فأن الاستهداف ضد الهواتف التي تعمل بنظام iOS لم يتوقف.

لهذا تعاني اليوم جميعا الهواتف بما فيها الآيفون إلى هجوم للبرمجيات الخبيثة و الاختراق .من خلال هذا الدليل التدريبي حيث ستجد نصائح أساسية لحماية البيانات الحساسة على هاتفك من أعين المتطفلين من المتسللين و المهاجمين.

هناك طرق للتأكد من أن جهازك الخاص بك آمن من المتسللين قدر الإمكان. إذا كانت لديك مخاوف بشأن سلامة بياناتك الخاصة ، والمعلومات الحساسة بما في ذلك تسجيلات موقع الويب وعناوين البريد الإلكتروني والرسائل النصية وحتى الصور ومقاطع الفيديو، والهدف من هذا المعلومات تقليل المخاطر و ليس الحماية الكاملة و الشاملة.

ملاحظات

1- تم إعداد هذا الدليل بأستخدام إصدار نظام التشغيلiOS13- لهذا
في الإصدارات القديمة قد تكون هناك تغييرات
2- تم أستخدام الفيديو في شرح العديد من فقرات الدليل التدريبي .

اختراق ، تعطيل ، إيقاف الحسابات- ماذا تفعل؟

العديد من الأشخاص تصيبهم الحيرة والقلق عندما تصادفهم مشاكل في مواقع التواصل الاجتماعي و ذلك عندما يتم قرصنة حساباتهم أو إغلاقها من قبل الشركة أو إيقافها.

يبحثون عن حلول من أجل استرجاع حساباتهم بكل طرق وقد يتم اللجوء إلى بعض الأشخاص الذي يطلبون أموال من أجل استرجاع الحسابات ويتضح لاحقا بأنها عملية نصب وسرقة .

هذا الدليل الهدف منه معرفة الخطوات التي تساعدك من أجل استرجاع الحساب كخطوة أولى قبل اللجوء إلى المنظمات أو الأشخاص.

أساسيات الحماية للحواسيب و الهواتف النقالة/المحمولة

الأجهزة الإلكترونية (لاسيما الحواسيب والهواتف النقالة) حساسة جدا لهذا تحتاج إلى عناية خاصة ولاسيما حمايتها ضمن نطاق البرمجيات على هذه الأجهزة وحمايتها من أية أخطار خارجية أو داخلية بسبب سوء استخدامها أو استخدام التطبيقات / البرمجيات .

لتقليل المخاطر الإلكترونية -ليس لمنعها بشكل كامل- بالإمكان استخدام هذه الإرشادات لمساعدتك. هذه الإرشادات لم يتم تصميمها إلى خبراء الحاسوب أو خبراء الحماية الرقمية بل تم تصميمها إلى المستخدمين End user الذين يريدون توفير حماية أساسية إلى حواسيبهم أو هواتفهم النقالة .تذكر دائما بأن هذه الإرشادات أقل ما يمكن عمله ودائما يجب عليك اتخاذ خطوات اكثر لحماية حاسوبك و هاتفك من الأشرار .

تحديث التطبيقات

البرمجيات و أيضا نظام التشغيل التي تستخدمها في جهازك بأستمرار

في بعض الأحيان تكتشف الشركات -او خبراء مستقلين- التي تصمم هذه التطبيقات / البرمجيات أو أنظمة التشغيل ثغرات أمنية في منتجاتها فتقوم بتحديثها من أجل منع أن يتم استغلال هذه الثغرات في الدخول إلى جهازك و معلوماتك الشخصية .

نظام التشغيل وندوز Windows

تحديث التطبيقات في نظام التشغيل وندوز Windows

تحديث نظام التشغيل اندرويد Android

تحديث التطبيقات في نظام التشغيل اندرويد Android

تحديث نظام التشغيل آي او اس iOS

تحديث نظام التشغيل الماك Mac و تطبيقات

استخدم التطبيقات / البرمجيات مفتوحة المصدر أو المجانية (بقدر الإمكان)

استخدام هذه التطبيقات / البرمجيات سوف يمنعك من استخدام الكراك Crack التي قد تحتوي على برمجيات خبيثة التي تسبب ضرر بالجهاز.

البرمجيات مفتوحة المصدر أو المجانية يتم أيضا تحديثها باستمرار لمعالجة الثغرات التي يتم اكتشافها.

يوفر موقع Alternativeto بدائل إلى التطبيقات/ البرامج التي يجب أن يقوم المستخدم بدفع أموال طائلة لأستخدامها.

قائمة بالتطبيقات المجانية التي بالإمكان استخدامها و قد تم تقسيمها بحسب الموضوع .

يرجى قراءة الكود أدناه:

استخدام كلمات سر قوية على الأجهزة

"(ع.ح) مدافع حقوقي من محافظة ميسان لجهازه لذلك فقد تم اختراق هاتفه بكل بساطة، وقد واجهة صعوبة بالغة لحين استعادة جهازه وملفاته."

تذكر ان العديد من المستخدمين لا يستخدمون خاصية التعمية / التشفير Encryption أو لا يضع كلمة سر على جهازه ولكن في المقابل أيضا العديد منهم يستخدم كلمات سر ضعيفة **(مثلا : 123456789 أو اسم زوجته أو أولاده أو الحيوان الذي يقوم بتربيته أو اسم احد أفراد العائلة و غيرها).**

العديد من الأشخاص يستخدم Pattern على هاتفه المحمول / النقال وهي بالنسبة لهم أسهل من أجل الوصول إلى بيانات الهاتف و لكن هذه الخاصية أيضا سوف تسهل عمل المتطفلين أو الأشخاص الذين يريدون الوصول إلى معلوماتك في الجهاز. أن كلمة السر هي خط الدفاع الأول ضد المتطفلين وغيرهم و أن استخدام كلمات سر ضعيفة - أو عدم تعمية / تشفير الجهاز - سوف يسهل عليهم هذه المهمة للوصول إلى معلوماتك الحساسة. لا ينصح باستخدام خاصية البصمة الإلكترونية (الوجه والأصابع) حيث يسهل فتح الهاتف باستخدام طرق مختلفة.

// حماية جهازك من الاختراق ومن البرامج الخبيثة وملفات التجسس "

(م.ز) ناشط من بغداد يستخدم جميع وسائل الحماية ويطبق جميع التعليمات الخاصة بالامن الرقمي وحماية الجهاز من الاختراق تعرض لمحاولة اختراق، لكنها فشلت بسبب الاجراءات السابقة التي قد استخدمها في حمايته".

اذا كنت تستخدم الحاسوب المحمول أو الهاتف النقال/ المحمول يجب عليك أن تتأكد بأنه لا يحتوي على البرمجيات الخبيثة والتي كنت قد تراقب وتجسس على كل ما تقوم به على الجهاز، ان البرمجيات الخبيثة Malware قد تؤدي وظائف عديدة في جهازك ومنها تدمير الجهاز او سرقة المعلومات او الربح المالي أو التحكم بالجهاز عن بعد.

ان العديد من المستخدمين لا يقومون بـ تثبيت / تنصيب برامج تحارب هذه البرمجيات الخبيثة وأيضا العديد من المستخدمين يستخدمون تطبيقات غير مجانية أو غير آمنة أو تم كسر حمايتها بأستخدام الكراك Crack، أن استخدام تطبيقات / برمجيات لم يتم تفعليها بشكل صحيح لن يساهم في تأدية الوظيفة التي من أجلها تم تثبيت تنصيب هذا التطبيق من أجله و هي "مكافحة البرمجيات الخبيثة.

من المعلومات وخصوصا المتعلقة بالمواقع الإلكترونية التي قمت بزيارتها أو المواقع التي قمت بالتفاعل فيها، لا يمكننا أن نمحي تماما أو نتخلص من البصمة الرقمية ولكن نحاول أن نقوم بتقليل توافر بصماتنا الرقمية في كل مكان، ننصح دائما باستخدام خاصية الشبكات الافتراضية VPN أثناء استخدام الأنترنت وتصفح المواقع المتصلة بالمنظمات الدولية أو إرسال رسالة إلكترونية إلى هذه المنظمات، يوجد العديد من الخدمات والمواقع التي تقدم هذه الخاصية و لكن بعض هذه الخدمات والمواقع غير آمنة وقد تتعاون مع السلطات في بلدك من أجل إعطاءهم معلوماتك الشخصية، بالإمكان استخدام احد التطبيقات الاتية لإخفاء مكانك الحقيقي والتقليل من بصمتك الالكترونية وأيضا لتجاوز الحجب الالكتروني لبعض المواقع وهي:

Psiphon

Tunnel bear

Cyber Ghost

ان هذه التطبيقات متوفرة لأنظمة التشغيل ويندوز وماك وللهواتف الذكية لتطبيقات اندرويد وIOS.

وكذلك يمكن استخدام متصفح تور Tor والذي يعتبر من اهم الأدوات في المجهولية ولكنه ليس VPN، بالإضافة إلى الخدمات المدفوعة والغير مجانية.

المتصفح الأمن Browser

العديد من المستخدمين يستخدمون متصفحات غير آمنة - مثلا Internet Explore/Edge- وهذه المتصفحات قد تكون السبب في إصابة جهازك بالبرمجيات الخبيثة Malware، العديد من الخبراء ينصحون باستخدام Firefox بسبب انه آمن ومفتوح المصدر.

ولكن لا يعني استخدام متصفح آمن انه يكفي من أجل حمايتك بل عليك التأكد من عدم فتح وصلات / روابط Link غير آمنة، وكذلك التأكد من عدم تنصيب/ تثبيت Install إضافات/ملحقات Add-ons غير آمنة في المتصفح.

وينصح بتنصيب / تثبيت الإضافات/الملحقات Add-ons التالية مع متصفح Firefox:

www.psiphon.ca

www.tunnelbear.com

www.cyberghostvpn.com/en_US/

لتنصيب المتصفح من الرابط التالي

Download Tor Browser

Self-destructing cookies

وهي إضافة ملحقة من أجل مسح الكوكيز Cookies بطريقة تلقائية بعد خروجك من الموقع يعني تقوم بمسح أي ملفات او معلومات عنك تم تسجيلها من قبل الموقع الذي قمت بزيارته.

UBlock Origin

وهي إضافة ملحقة لمنع الإعلانات المزعجة والتي قد تحتوي على برمجيات خبيثة Malware.

HTTPS Everywhere

وهي إضافة ملحقة لإجبار المواقع على إظهار شهادة الأمان SSL/TLS في مواقعهم إذا يملكون هذه الخاصية وهي شهادة لتعمية / تشفير الاتصال بين المستخدم والموقع.

كما يمكنك معرفة إذا كان بريدك الإلكتروني سبق واختراق عن طريق موقع يمكن وضع البريد الالكتروني به ويخبرك إذا كان موجد لديه في قاعده بيانات الموقع يعني سبق واخترق مما يتطلب منك ان تقوم بتغيير كلمة السر للتحقق عبر الكود :

نصائح

حرف مختلف بين رموز واحرف كبيرة وصغيرة وأرقام ولا يجب ان تحفظها في المواقع والمتصفحات.

ولمعرفة مدى قوة كلمة السر التي لديك استعمل الموقع التالي عبر وضع كلمة السر المراد فحص قوتها ويفضل التغيير فيها قليلا وعدم وضعها كما هي وبعد وضعها يقول لك الموقع كم يتطلب وقت لاختراق هذه الكلمة وكسرها اذا الوقت قليل ينصح بتغيير الكلمة ولكما كان الوقت أطول لكسر الكملة كلما كانت اكثر قوة

المسح الامن للملفات

حرف مختلف بين رموز واحرف كبيرة وصغيرة وأرقام ولا يجب ان تحفظها في المواقع والمتصفحات. ولمعرفة مدى قوة كلمة السر التي لديك استعمل الموقع التالي عبر وضع كلمة السر المراد فحص قوتها ويفضل التغيير فيها قليلا وعدم وضعها كما هي وبعد وضعها يقول لك الموقع كم يتطلب وقت لاختراق هذه الكلمة وكسرها اذا الوقت قليل ينصح بتغيير الكلمة ولكما كان الوقت أطول لكسر الكملة كلما كانت اكثر قوة

وهناك نسخة منه للهواتف المحمولة في المتجر تحمل نفس الاسم

CCleaner

بعد تشغيل CCleaner قد تفقد تأريخ تصفح الوب كله وتأريخ المستندات الأخيرة وكلمات السر المحفوظة؛ على أية حال، هذا هو الهدف من هذه الأداة بالضبط - لتقليل الطرق المختلفة التي تؤدي لإصابة أو اختراق نظام حاسوبك.

بعد تنصيب البرنامج ولغرض تتغير اعدادات البرنامج لكي يصبح الحذف أمن ولا يمكن إعادة الملفات المحذوفة يتم تغيير الاعداد كالتالي:

اذهب الى options ثم setting واذهب الى secure deletion واختار الخيار الثاني وهو (slower socure file deletion) ومن ثم في المربع غير الخيار من القائمة الى (7 complex overwrite passes) .

لدى البرنامج العديد من الوظائف لمسح ملفات الارتباط وسجلات المتصفح والملفات المؤقتة وغيرها يمكنك التحكم واختيار ما تحذفه من كلمات السر وغيرها من تبويب cleaner هناك نافذتين windows تتضمن فئات نظام التشغيل ويمكن وضع صح على المربعات للفئات التي تريد حذفها ورفع علامة الصح عن التي لا ترغب بحذفها والنافذة الثانية هي للبرامج بعنوان application ونفس الشي وبعدها اضغط على analyze وعند اكتمال التحليل ورغبتك بالحذف اختار Run cleaner ، كما يقوم البرنامج بمجموعة من الوظائف منها إزالة البرامج وكشف الملفات المكررة ويمكن تسريع الإقلاع عبر إيقاف بعض البرامج التي تعمل مع تشغيل النظام فضلا عن وظائف أخرى يمكن اكتشافها.

يمكن تثبيت البرنامج بقراءة الكود واستعمل الإصدار المجاني دون ترقية بعد التثبيت:

هو برنامج لأنظمة الويندوز ويمكّنكم من استعادة ملفاتكم المحذوفة، ووضعها مجدداً في جدول توزيع الملفات، حيث يقوم بإجراء عملية بحث عن الملفات غير المذكورة في الجدول وسؤالكم عمّا تريدون فعله بها. ستتمكّنون بهذه الطريقة بسهولة من استعادة هذه الملفات طبعا عدا الملفات التي تم حذفها عبر البرنامج السابق CCleaner.

Recuva

وهو برنامج مجاني وبإمكانكم تحميله من الرابط ادناه، وبعد إتمام عملية التنصيب وتشغيل البرنامج، سيتم عرض شاشة ترحيب ودليل يقودكم إلى عدد من الخطوات السهلة ويمكنكم اختيار نوع الملفات التي تبحثون عنها ومسار البحث وبعدها اين يتم خزنها.

Disk Drill

تطبيق مجاني لاستعادة الملفات على نظام الماك و تم تطويره من قبل شركة ويقوم على أساس استعادة الملفات التي تم مسحها او التي تم فقدها عن طريق الخطأ في محركات الاقراص الصلبة او وحدة التخزين USB ووحدة التخزين

جدار ناري GlassWire

تطبيق مجاني لاستعادة الملفات على نظام الماك و تم تطويره من قبل شركة ويقوم على أساس استعادة الملفات التي تم مسحها او التي تم فقدها عن طريق الخطأ في محركات الاقراص الصلبة او وحدة التخزين USB ووحدة التخزين

العديد من المستخدمين يقومون بتحميل التطبيقات / البرمجيات من مواقع غير آمنة أو غير معروفة ، وحيث أن هذه التطبيقات / البرمجيات قد تحتوي على برمجيات خبيثة Malware تسبب ضرر إلى جهازك .

تأكد بأن هذه التطبيقات / البرمجيات تم تحميلها من مواقعها الأصلية / الأساسية وليست مواقع بديلة غير آمنة أو غير معروفة .

لا تقم بتحميل تطبيقات/ برمجيات غير معروفة أو غير آمنة و ابحث عن آراء الخبراء حول هذه التطبيقات / البرمجيات على الأنترنت لان قد تكون هذه التطبيقات / البرمجيات تم تصنيفها بأنها "خطرة ".

// استخدام متصفح امن"

العديد من المستخدمين يستخدمون متصفحات غير آمنة – مثلا Internet Explore/Edge- و هذه المتصفحات قد تكون السبب في إصابة جهازك بالبرمجيات الخبيثة Malware .

العديد من الخبراء ينصحون بأستخدام Firefox – أو متصفح فايرفوكس فوكس على الهواتف– بسبب انه آمن و مفتوح المصدر .

و لكن لا يعني استخدام متصفح آمن يكفي من أجل حمايتك بل عليك التأكد من عدم فتح وصلات / روابط Link غير آمنة .

و كذلك التأكد من عدم تنصيب/ تثبيت Install إضافات/ملحقات Add-ons غير آمنة في المتصفح .

و ننصح بتنصيب / تثبيت الإضافات/ملحقات Add-ons آمنة :

غالبًا ما تتضمن كل من ملحقتي Oracle Java browser plugin و Adobe Shockwave Flash

على ثغرات أمنية من الممكن أن تتيح التحكم عن بعد بجهازك أو تثبيت برمجيات خبيثة عليه.

ننصح بشدة بتعطيل هاتين الملحقتين في فيرفكس Firefox

مكافح البرمجيات الخبيثة

ان البرمجيات الخبيثة Malware قد تؤدي وظائف عديدة في جهازك و منها تدمير الجهاز او سرقة المعلومات او الربح المالي أو التحكم بالجهاز عن بعد .

ان العديد من المستخدمين لا يقومون بـ تثبيت / تنصيب تحارب هذه البرمجيات الخبيثة و أيضا العديد من المستخدمين يستخدمون تطبيقات غير مجانية أو غير آمنة أو تم كسر حمايتها بأستخدام الكراك Crack .

أن استخدام تطبيقات / برمجيات لم يتم تفعليها بشكل صحيح لن يساهم في تأدية الوظيفة التي من أجلها تم تثبيت / تنصيب هذا التطبيق من أجله و هي "مكافحة البرمجيات الخبيثة " .

الشبكات الخاصة الافتراضية vpn

نحن دائما ما نحتاج أن نبقى متصلين بالإنترنت و دائما ما نبحث عن شبكات Wi-Fi في المنازل التي نزورها او في المطاعم و الآن ايضا نبحث عنها في الباصات و الطائرات .

و لكن نحن لا نعلم مخاطر استخدام شبكات الانترنت العامة Wi-Fi حيث قد تكون أداة للتجسس علينا و خصوصا بما يتعلق بنشاطنا على الأنترنت أو قد تكون أداة لنقل البرمجيات الخبيثة Malware او أداة لسرقة كلمات السر و المعلومات الحساسة .

1 لدينا تطبيقات / برمجيات مكافحة البرمجيات الخبيثة و تم تحديثها

2 نظام التشغيل لدينا محدث update

بالإضافة كل ما في الأعلى ، يجب تثبيت / تنصيب تطبيقات توفر لنا اتصال اكثر أمانا و هي التطبيقات التي توفر خاصية VPN . يوجد العديد من الخدمات و المواقع التي تقدم هذه الخاصية و لكن بعض هذه الخدمات و المواقع غير آمنة و قد تتعاون مع السلطات في بلدك من أجل إعطاءهم معلوماتك الشخصية.

وكذلك هذه مجموعة إرشادات من أجل تقليل المخاطر أثناء استخدام شبكة الأنترنت في المنزل

مجموعة من التطبيقات التي توفر لك VPN

بروتوكول نقل النصوص الفائقة Http وبروتوكول Https

عند قيام المستخدم بطلب عرض صفحة انترنت من موقع الكتروني فإن الخادم الخاص بالشبكة يتوقع من متصفح المستخدم تقديم معلومات معينة حتى يتمكن من تقديم الصفحة التي طلبها. كما سبق ذكرنا، فإن بروتوكل نقل النصوص الفائقة (HTTP) عبارة عن مجموعة من القواعد التي يتبعها كلاً من الخادم لشبكة الموقع وبرنامج المتصفح للإتصال فيما بينهما وتبادل المعلومات والبيانات. فمن أحد هذه المعلومات، عنوان الصفحة التي يريد المستخدم عرضها، وهي ماتوضحه عنوان ال (Uniform Resource Locator – URL).

عند تبادل المعلومات بين خادم الصفحة وبين المتصفح باستخدام بروتوكول Http، تنتقل البيانات دون تشفير.

أي أن أي خادم انترنت موجود على خط الاتصال بين خادم الصفحة (الذي قد يقع في الولايات المتحدة) والمتصفح (الذي قد يكون على جهازكم في سوريا) يستطيع معاينة البيانات المتبادلة. بما في ذلك مزود خدمة الانترنت خاصتكم.

أما عند استخدام بروتوكول Https يتم تشفير البيانات بين خادم الصفحة التي تدعم بروتوكول Https وبين متصفحكم. وبالتالي لا تستطيع الخوادم بين خادم الصفحة التي تزورونها ومتصفحكم معرفة المحتوى. إذا لا يستطيع مزود خدمة الانترنت خاصتكم معرفة محتوى التصفح إن كانت الصفحة التي تزورونها تستخدم بروتوكول Https لكن مزود الخدمة يستطيع تحديد الموقع الذي تزورونه مثلا موقع youtube.com أو موقع facebook.com لكن بدون معرفة المحتوى.

لا تدعم جميع المواقع بروتوكول Https لكن أغلب المواقع الهامة وجميع المواقع ذات الصيت الحسن التي تتطلب تسجيل الدخول تدعمه. إقرأ المزيد عن هذا الموضوع في المقالة الخاصة ببروتوكول Https.

أيضا قوموا باستخدام إضافة Https Everywhere التي تجبر التصفح على استخدام هذا البروتوكول عندما يكون البروتوكول متاحا. وتذكروا أن استخدام Https لا يحميكم من تتبع مزود الخدمة لأسماء المواقع التي تزورونها ولا لعاداتكم على الانترنت. وتذكروا أن هناك أساليب تسمح لمزود الخدمة بفك تشفير البيانات المتبادلة بين متصفحكم وخادم الصفحة التي تزورونها باستخدام تقنيات مثل Deep Packet Inspection أو مختلف هجمات الرجل في المنتصف Man in the Middle Attack. والتي يقي منها استخدام برامج مثل تور TOR أو برامج VPN وشبيهاتها حسنة الصيت مثل سايفون3 Psiphon3 أو هوتسبوت شيلد Hotspot Shield.

ملفات تعريف الارتباط (Cookies)

وهي عبارة عن تركيبة من المعلومات والتي تقوم مواقع الانترنت بارسالها إلى المتصفح عند قيام المستخدم بالدخول اليها. باستقبال المتصفح لهذه المعلومات، يقوم بتخزينها في محرك القرص الصلب لجهاز الحاسب (Hard Disk)، مالم يكن المتصفح لايدعم ملفات الكوكيز، مع العلم بأن أكثر برامج التصفح شيوعاً في الاستخدام تقوم بدعم ملفات الكوكيز.

وفي كل مرة يقوم المستخدم باستخدام جهاز الحاسب للدخول إلى صفحات الانترنت تلك مرة أخرى، فإن المعلومات المخزنة في ملفات الكوكيز تُرسل مرة أخرى إلى ذاك الموقع عن طريق المتصفح.

قد يتسأل البعض عن أهمية ملفات الكوكيز، ففي العموم، عندما يقوم مجموعة من الاشخاص بالدخول الى مواقع الانترنت عن طريق نقاط الدخول العامة (Public ISP)، فمن الصعب على مشغلات مواقع الانترنت الربط بين الطلبات على صفحاتها، بالاضافة إلى أن كل طلب لا يتضمن رقم تعريفي دائم خاص به. فتسمح ملفات الكوكيز لمشغلات مواقع الانترنت بإسناد أو تعيين رقم تعريفي خاص ودائم لكل جهاز، فتساعدها على ربط الطلبات على الموقع من ذلك الجهاز. تشير ملفات الكوكيز إلى مواقع الانترنت التي تمت زيارتها من قِبل المستخدم، وتسجيل أي الأجزاء من الموقع تمت زيارته. في حين أن ملفات الكوكيز نفسها لا تقوم بتعريف المستخدم، كالأسماء أو العناوين، ولكن يمكن ربطها بمعلومات تعريفية أخرى، فعلى سبيل المثال، عندما يقوم المستخدم بتقديم معلومات إضافية عن نفسه عند الشراء على الانترنت أو التسجيل في الخدمات المجانية، عندها بإمكان ملفات الكوكيز تكوين ملف شخصي عن المستخدم وإهتماماته وعاداته الشرائية. يستخدم أصحاب المواقع هذه المعلومات لتكوين عروض دعائية وإعلانات تناسب اهتمامات الشخص نفسه. قد يشعر البعض من متصفحي الانترنت بالانزعاج من استخدام القرص الصلب للأجهزة تهم من دون إذن منهم. هناك العديد من الأساليب التي يمكن القيام بها لمكافحة هذه الملفات إذا لم يكن المستخدم يشعر بالثقة تجاهها، وتشمل:

ضبط إعدادات المتصفح لجعل ملفات الكوكيز قابلة للقراءة فقط (Read Only)، وامكانية ذلك تعتمد على نظام التشغيل و نوع المتصفح. ولكن بجعلها قابلة للقراءة فقط، فإن هذه الملفات ستبقى في الجهاز فقط طالما برنامج المتصفح يقوم بالعمل. - ضبط جهاز الحاسب لمسح ملفات الكوكيز عند كل تشغيل لبرنامج المتصفح. - كثير من المتصفحات تسمح بإخطار المستخدم عند محاولة كتابة ملفات الكوكيز في جهاز الحاسب من قِبل مواقع الانترنت بالقبول أو الرفض، ولكن في كثير من الحالات، قد تكثر عدد الاخطارات بحيث تصبح مزعجة للمستخدم. - القيام بمسح ملفات الكوكيز من برنامج المتصفح بشكل دوري. - توجد بعض البرامج التي تقوم بالتحكم وادارة ملفات الكوكيز بدلاً من المستخدم نفسه، مثل Cookie Crusher و Cookie Pal و Cookie Cruncher. يمكن استخدامها عند الضرورة للتحكم بالكوكيز.

ما هو VPN

الشبكة الافتراضية الخاصة ، أو VPN ، هي اتصال معمى (مشفر) عبر الإنترنت من جهاز إلى شبكة. يساعد الاتصال المعمى على ضمان نقل البيانات الحساسة بأمان. يمنع الأشخاص غير المخولين من التنصت على حركة المرور و على ما يقوم به المستخدم على الانترنت .

يستخدم الاشخاص خدمة VPN ، تُعرف أيضًا باسم نفق VPN ، لحماية نشاطهم وهويتهم عبر الإنترنت. باستخدام خدمة VPN مجهولة ، تظل حركة مرور بيانات المستخدم معماة، مما يمنع المهاجمين من فحص نشاط الإنترنت للمستخدم. تعتبر خدمات VPN مفيدة بشكل خاص عند الوصول إلى نقاط اتصال Wi-Fi العامة لأن الخدمات اللاسلكية العامة قد لا تكون آمنة. بالإضافة إلى أمن Wi-Fi العام ، توفر خدمة VPN الخاصة للمستخدمين أيضًا إمكانية الوصول إلى الإنترنت دون رقابة ويمكن أن تساعد في منع سرقة البيانات وإلغاء حظر مواقع الويب.

بروتوكولات الشبكة الرئيسية

هناك ثلاثة بروتوكولات رئيسية للاستخدام مع أنفاق VPN. هذه البروتوكولات بشكل عام غير متوافقة مع بعضها البعض. وهي تشمل ما يلي:

حقائق حول الشبكة الافتراضية الخاصة : لا ينبغي الإيمان بالخرافات

الشبكة الافتراضية الخاصة (VPN) هي تقنية تتيح للمستخدم الاتصال بخادم بعيد واستخدام الإنترنت. في الآونة الأخيرة نشرت العديد من الادوات التي ممكن استخدامها ،و لكن هناك الكثير من الخرافات و المعلومات الغير صحيحة المحيطة بهذه التقنية التي تمنع العديد من الأشخاص من استخدامها.

الخرافة رقم 1 لا أفعل أي شيء غير قانوني ، لست بحاجة إلى الشبكة الافتراضية الخاصة VPN

أكثر خرافات VPN انتشارًا بين مستخدمي الإنترنت هي أنهم لا يحتاجون إلى خدمة VPN إذا لم يفعلوا أي شيء غير قانوني. ولكن ، يجب على المرء أن يفهم أن استخدام VPN لا يقتصر على تجاوز القيود الجغرافية أو تغيير عنوان IP. إذا كنت شخصًا يقدر الخصوصية ويرغب في تعمية (تشفير) الاتصالات لأغراض أمان البيانات ، فمن المستحسن استخدام خدمة VPN. الخصوصية هي الاساس - لا يحق لاحد ان يطلع على معلوماتنا.

الخرافة رقم 2 VPN يبطئ اتصال الإنترنت

في كثير من الأحيان ، يمتنع الناس عن استخدام خدمة VPN بالقول إن خدمة VPN ستعمل على إبطاء الاتصال. يمكن أن يكون صحيحا في بعض الحالات ولكن مثل هذه التعميمات هي خرافة. تعتمد السرعة الإجمالية لـ VPN على سرعة اتصالك بالإنترنت. خدمات VPN المجانية هي تلك التي تواجه غالباً سرعات أبطأ. عامل كبير آخر هو موقع Location خوادم VPN لمزود الخدمة الخاص بك. لذلك ، أثناء اختيار خدمة VPN ، تأكد من أن لديهم خدمات في العديد من المواقع Locations و أنها موزعة على عدة دول و مناطق .

الخرافة رقم 3 إذا كنت أستخدم VPN ، فبإمكاني القيام بأي شيء على الإنترنت

لا ، إنها خرافة . لا يمنحك استخدام الشبكة الافتراضية الخاصة (VPN) ترخيصًا للقيام بأي شيء على الإنترنت. هذا يعني أنك لن تكون آمنًا من البرامج الضارة Malware. لن ينقذك من عمليات الاحتيال أو التصيّد الاحتيالي أو هجمات الاختراق. لذا ، بالإضافة إلى استخدام الشبكة الافتراضية الخاصة ، من المهم أيضًا اتباع ممارسات أمان الإنترنت الأساسية الأخرى.

الخرافة رقم 4 يتم إنشاء جميع الشبكات الافتراضية الخاصة على قدم المساواة

غير صحيح ، مثل أي خدمة أخرى ، فإن بعض شبكات VPN أفضل من غيرها. وهي توفر خصائص مختلفة لأنظمة التعمية (التشفير). يجب إلقاء نظرة فاحصة على البروتوكولات التي تقدمها الشبكة الافتراضية الخاصة ، مثل OpenVPN أو PPTP. حاول تجنب تلك التي تستخدم PPTP لأنه بروتوكول قديم. هناك عامل آخر يجب مراعاته هو أن مقدم خدمة VPN لا يحتفظ بسجلات الجلسات و غيرها من المعلومات التي قد يستغلها مقدم الخدمة ضدك .

الخرافة رقم 5 VPN هي فقط للخبراء التقنيين

لن أقول إن إعداد VPN أمر سهل للغاية، ولكنه ليس مهمة مستحيلة. إنها خرافة- يقدم جميع مزودي خدمات VPN المعروفين تقريبًا مساعدة من أجل إعداد الشبكة الافتراضية الخاصة . هناك أيضًا الكثير من الأدلة التدريبية المتاحة على الإنترنت والتي يمكنك استخدامها لتسهيل أي عملية تثبيت و استخدام الخدمة.

الخرافة رقم 6 الشبكات الافتراضية الخاصة تحميك من تتبع الإعلانات التجارية

تخفي الشبكة الافتراضية الخاصة عنوان IP الخاص بك وتجعلك غير مرئي نسبيًا لمزود خدمة الإنترنت ، ولكنها لن تحظر ملايين متتبعي الإعلانات الآخرين على الإنترنت. عادةً ما تستخدم شبكات الإعلانات ملفات تعريف الارتباط Cookies بدلاً من عنوان IP لتحديد هويتك ، لذا إذا كنت تستخدم الشبكة الافتراضية الخاصة (VPN) للتخلص من تتبع الإعلانات ، فستصاب بخيبة أمل كبيرة. والأسوأ من ذلك هو أن بعض موفري VPN يقومون بالفعل بعرض إعلاناتهم الخاصة أو يبيعون بيانات التصفح الخاصة بك.

الخرافة رقم 6 الشبكات الافتراضية الخاصة تحميك من تتبع الإعلانات التجارية

تخفي الشبكة الافتراضية الخاصة عنوان IP الخاص بك وتجعلك غير مرئي نسبيًا لمزود خدمة الإنترنت ، ولكنها لن تحظر ملايين متتبعي الإعلانات الآخرين على الإنترنت. عادةً ما تستخدم شبكات الإعلانات ملفات تعريف الارتباط Cookies بدلاً من عنوان IP لتحديد هويتك ، لذا إذا كنت تستخدم الشبكة الافتراضية الخاصة (VPN) للتخلص من تتبع الإعلانات ، فستصاب بخيبة أمل كبيرة. والأسوأ من ذلك هو أن بعض موفري VPN يقومون بالفعل بعرض إعلاناتهم الخاصة أو يبيعون بيانات التصفح الخاصة بك.

الخرافة رقم 7 إخفاء الهوية بالكامل على الانترنت

قد لا يكون ذلك صحيحًا إذا كنت تستخدم خدمة VPN ، لان بعض الشركات تحافظ على السجلات أو تتبعك على للإنترنت بأي شكل من الأشكال. أكبر مشكلة في هذا هو أنه في حين أن معظم مقدمي الخدمة يدعون أنهم لا يقومون بتسجيل معلومات المستخدمين ، إلا أن بعضهم يقومون بذلك . أبحث عن هذه الخدمة قبل التعامل معها و تأكد بأن ليس لديها سوابق في التعاون مع السلطات المحلية .

// المجهولية على الانترنت "

هو برنامج تخفي على شبكة الإنترنت يعتمد الجيل الثاني
نظام التسيير البصلي وهو نظام يمكن مستخدميه من
بدون الكشف عن الهوية على شبكة الإنترنت

مفتوح المصدر : نعم

مجاني : نعم

أنظمة التشغيل

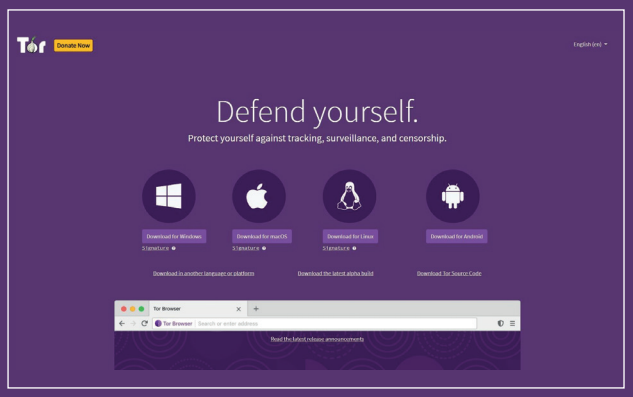
الوندوز Windows

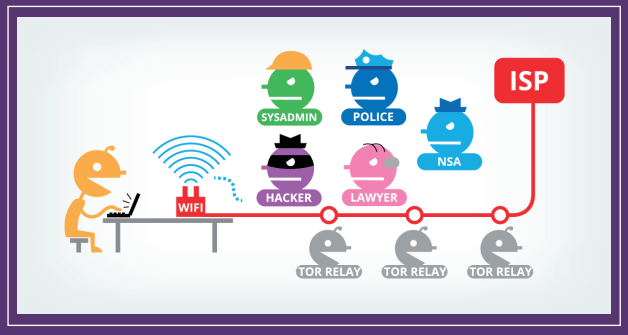
لينكس Linux

ماك Mac

أندرويد Android

آي أو أس iOS





www.iraqi-alamal.org

بعض البرامج الخبيثة وكيفية الوقاية منها

قد لا يكون ذلك صحيحًا إذا كنت تستخدم خدمة VPN ، لان بعض الشركات تحافظ على السجلات أو تتبعك على للإنترنت بأي شكل من الأشكال. أكبر مشكلة في هذا هو أنه في حين أن معظم مقدمي الخدمة يدعون أنهم لا يقومون بتسجيل معلومات المستخدمين ، إلا أن بعضهم يقومون بذلك . أبحث عن هذه الخدمة قبل التعامل معها و تأكد بأن ليس لديها سوابق في التعاون مع السلطات المحلية .

الفيروس Viruses:

فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات.

اي ان فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة.

تعتبر الروت كيت من البرامج الخبيثة و لكنها خطيرة لما يمكنها فعله بسرية و تفعيلها عن بعد و هذا يدل على احترافية مبرمجي هذه الفيروسات لهذا يجب تحديث مضاد الفيروس ليكون في قاعدة بيانات مضاد الفيروس اخر المعلومات فيما يخص الروتكيت لايجاده عند القيام بالفحص في جهاز الكمبيوتر رغم صعوبة العثور عليه. يتصف فيروس الحاسب بأنه:

- برنامج قادر على التناسخ Replication والانتشار.
- الفيروس يربط نفسه ببرنامج أخر يسمى الحاضن host.
- لا يمكن أن تنشأ الفيروسات من ذاتها.
- يمكن أن تنتقل من حاسوب مصاب لآخر سليم.

الديدان Worms:

دودة الحاسوب هي برامج صغيرة قائمة بذاتها غير معتمدة على غيرها صنعت للقيام بأعمال تدميرية أو لغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت أو إلحاق الضرر بهم أو بالمتصلين بهم، تمتاز بسرعة الانتشار ويصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة.

بعض البرامج الخبيثة وكيفية الوقاية منها"

قد لا يكون ذلك صحيحًا إذا كنت تستخدم خدمة VPN ، لان بعض الشركات تحافظ على السجلات أو تتبعك على للإنترنت بأي شكل من الأشكال. أكبر مشكلة في هذا هو أنه في حين أن معظم مقدمي الخدمة يدعون أنهم لا يقومون بتسجيل معلومات المستخدمين ، إلا أن بعضهم يقومون بذلك . أبحث عن هذه الخدمة قبل التعامل معها و تأكد بأن ليس لديها سوابق في التعاون مع السلطات المحلية .

الفيروس Viruses:

فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات.

اي ان فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة.

تعتبر الروت كيت من البرامج الخبيثة و لكنها خطيرة لما يمكنها فعله بسرية و تفعيلها عن بعد و هذا يدل على احترافية مبرمجي هذه الفيروسات لهذا يجب تحديث مضاد الفيروس ليكون في قاعدة بيانات مضاد الفيروس اخر المعلومات فيما يخص الروتكيت لايجاده عند القيام بالفحص في جهاز الكمبيوتر رغم صعوبة العثور عليه. يتصف فيروس الحاسب بأنه:

برنامج قادر على التناسخ Replication والانتشار.

الفيروس يربط نفسه ببرنامج أخر يسمى الحاضن host.

- لا يمكن أن تنشأ الفيروسات من ذاتها.
- يمكن أن تنتقل من حاسوب مصاب لآخر سليم.
-
-

الديدان Worms:

دودة الحاسوب هي برامج صغيرة قائمة بذاتها غير معتمدة على غيرها صنعت للقيام بأعمال تدميرية أو لغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت أو إلحاق الضرر بهم أو بالمتصلين بهم، تمتاز بسرعة الانتشار ويصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة.

كيف تعمل الديدان

تصيب الدودة الحواسيب الموصولة بالشبكة بشكل اوتوماتيكي، ومن غير تدخل الإنسان وهذا الامر يجعلها تنتشر بشكل أوسع وأسرع عن الفيروسات. الفرق بين الديدان والفيروسات هو أن الديدان لا تقوم بحذف أو تغيير الملفات بل تقوم بإنهاك موارد الجهاز خاصة الذاكرة حيث تقوم الديدان بحجز مساحات واسعة من الذاكرة الحية RAM للجهاز ما يؤدي إلى انخفاض ملحوظ في أدائه ينعكس في بطء استجابة الجهاز وبطئ عمل التطبيقات والبرامج التي تعمل على الجهاز بالإضافة لبطئ في سرعة انتقال البيانات على الشبكة. تختلف الديدان في عملها من نوع لآخر، فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة، بينما نجد بعضها يعتمد على البريد الالكتروني أو سكايب لإرسال نسخة عن نفسه إلى جميع الموجودين في دفتر العناوين أو لائحة التواصل على سكايب، حتى أن البعض منها يقوم بإرسال رسائل قذرة لعدد عشوائي من المسجلين في سجل العناوين مستخدما البريد الالكتروني لصاحب الجهاز المصاب ما يسبب بالإضافة لاستهلاك موارد الجهاز الكثير من الحرج.

خطورتها

تكمن خطورة الديدان باستقلاليتها وعدم اعتمادها على برامج أخرى تلتحق بها مما يعطيها حرية كاملة في الانتشار السريع، وبلا شك أن هناك أنواعا منها غاية في الخطورة، حتى أصبح بعضها كابوساً مرعباً يلازم كل مستخدم للشبكة، كدودة Tanatos الشهيرة التي ظهرت خلال شهر أكتوبر 2002م وانتشرت انتشار النار بالهشيم وخلفت ورائها آثاراً تدميرية هائلة.

أنواعها

- ديدان البريد: وتكون مرفقة في محتوى الرسالة وأغلب الأنواع من هذة الديدان تتطلب من المستخدم أن يقوم بفتح الملف المرفق لكي تصيب الجهاز وأنواع أخرى تكون تحتوي على رابط خارجي وبعد أن تصيب الجهاز تقوم بإرسال نسخ منها إلى جميع المضافين في القائمة البريدية باستعمال بروتوكول SMTP
- ديدان المراسلة الفورية: وهذا النوع من الديدان يقوم باستخدام أحد برامج المراسلة الفورية للانتشار وذلك عن طريق إرسال الرسائل إلى جميع المتواجدين.
- ديدان اي ار سي (IRC): وتقوم بالانتشار عن طريق نسخ نفسها في القنوات في حالة الدردشة باستعمال بروتوكول إي آر سي وإرسال روابط إلى العنوان المصاب بالدودة
- ديدان برامج مشاركة الملفات: وتنتشر عن طريق وضع نفسها قي مجلدات المشاركة حتى تنتشر بين المستخدمين الاخرين في حالة تحميل الملفات عن طريق برنامج بيتلورد.
- ديدان الإنترنت: وتقوم بالانتقال عن طريق بروتوكول TCP/IP مباشرة دون الحاجة إلى مستوى أعلى مثل البريد الإلكتروني أو برامج تشارك ملفات، ومن الأمثلة عليها هو دودة بلاستر التي تقوم عشوائيا بالانتشار عن طريق البحث عن عناوين يكون المنفذ رقم 135 مفتوحا لتقوم باستغلاله وإصابة جهاز الضحية.

سبل الوقاية منها

من المعلوم أن أشهر وسائل انتشار الديدان هو عن طريق الرسائل الإلكترونية المفخخة، والتي عادة ما تكون عناوين هذه الرسائل جذاباً كدعوة لمشاهدة صور أحد النجوم أو المشاهير، لذلك يجب الحذر حتى وإن كانت الرسائل من مصدر معروف لأن بعض الديدان تقوم بإرسال نفسها من أي بريد لجميع الايميلات المضافة بدفتر العناوين فلذا فلتكن حذرا ولا تفتح اي رسالة إلا بعد التأكد تماما من انها خاليه من اي ضرر وهناك موقع تم ذكرة في بداية الدليل للتاكد من الروابط . وأيضًا، فإنه من المهم تحديث نسخ النظام المستخدم في الجهاز كي يتم تجنب الديدان.

أحصنة طروادة Trojan Horses

هو برنامج متخفي يصيب جهاز الضحية من دون علمه ويتيح للمهاجمين التحكم أو التجسس أو استغلال الجهاز لأغراض غير شرعية دون علم صاحب الجهاز.

وسمي بهذا الاسم للطريقة التي استخدمها اليونانيون في فتح مدينة طروادة (Troy) التي ظلت محصنة أمامهم بقوة وعجزوا عن اقتحامها بالطرق التقليدية فقاموا ببناء مجسم كبير جدا على شكل حصان خشبي مفرغ من الداخل وقاموا بوضع داخله جنود وتركوه كهدية عند حصون المدينة وانسحبوا منها.

فقام أهلي المدينة بإدخال المجسم واعتبره رمز للانتصار على الأعداء وعند منتصف الليل قام الجنود بالخروج من المجسم وفتح أسوار المدينة للجيش الذي قام بالدخول ومن ثم احتلال المدينة.

إذن التروجان هو برنامج خطير جدا وتكمن خطورته في أنه يكون موجود على جهاز الضحية دون علم صاحبة مما قد يعرض صاحب الجهاز لمخاطر التجسس وسرقة المعلومات الشخصية أو الصور أو الملفات السرية أو إفسادها أو تعطيل الجهاز أو جمع كلماته السرية التي يستخدمها على شبكة الانترنت (مواقع البريد الالكتروني أو المواقع التجارية الالكترونية) ومن تم تغييرها واستخدامها كوسيلة للابتزاز... وغيرها من المخاطر المرعبة.

طريقة عمله

يتكون برنامج التروجان من نسختين: خادم و مستفيد. ويقوم المهاجم بنشر نسخة الخادم على الانترنت بعد ربطها مع أي ملف أو برنامج آخر (مثلا: لعبة أو عرض تشغيلي) وعندما يقوم المستخدم (الضحية) بتشغيل ذلك الملف يتم تحميل نسخة الخادم على جهازه من دون علمه (فهو لا يرى إلا البرنامج الأساسي ولا يعلم أن هناك برنامج تروجان ملحق معه)، وتقوم نسخة الخادم بفتح منفذ(ثغرة) على جهاز الضحية ليكون جاهز لاستقبال الأوامر من المهاجم الذي يقوم باستخدام نسخة المستفيد وإرسال الأوامر عن طريق الشبكة إلى جهاز الضحية. وقد تقوم نسخة الخادم بإرسال رسالة بريد الكتروني إلى المهاجم لإخباره عن معلومات الجهاز الضحية(اسم الجهاز وعنوانه على الشبكة) الذي تم تحميل نسخة الخادم عليه حتى يتمكن من معرفته. كما أن نسخة الخادم لها المقدرة على تشغيل نفسها حتى مع إعادة تشغيل الجهاز وحماية الدخول عليها بكلمة مرور حتى لا يستطيع أي مهاجم آخر من التحكم بجهاز الضحية.

أما عن طريقة انتشاره فهو ليس مثل الفيروسات التي تنتقل آليا وبدون تدخل العنصر البشري بل ينتشر التروجان عن طريق تبادل الملفات وتشغيلها من قبل المستخدمين دون علمهم أن هذه الملفات تحتوي على برامج التروجان.

عن ماذا يبحث المهاجم

يستخدم المهاجم برامج التروجان على جهاز الضحية للحصول على أمور عديدة منها:

- أرقام بطاقات الائتمان (الفيزا أو الماستركارد) سواء كانت مخزنة على الجهاز أو عندما يقوم المستخدم باستخدامها على الانترنت.
- أرقام حسابات والكلمات السرية سواء حساب بنك أو بريد الكتروني أو موقع تجارة الكترونية.
- وثائق أو ملفات أو معلومات سرية أو هامة.
- عناوين البريد الكتروني المخزنة في الجهاز.
- صور أو أفلام فيديو خاصة أو عائلية وقد يستخدمها لابتزاز صاحب الجهاز.
- استخدام جهاز الضحية لأغراض غير شرعية مثل اختراق مواقع أو تعطيل أجهزة أخري.
- تعطيل أو تخريب و إفساد جهاز الضحية.

أنواع التروجان

التروجان لها أنواع عديدة ولكن يمكن تصنيفها مجازا إلى ستة أنواع رئيسية:

حصان طروادة للتحكم عن بعد Remote Administration Trojan أو أداة التحكم عن بعد Remote Administration Tool: وهو أشهر أنواع التروجان وأكثرها انتشارا وخطرا ومن أشهر أمثلته (Poison Ivy.bifrost .Spt-Net.Lost Door) فيقوم هذا النوع من التروجان بإعطاء المهاجم كامل التحكم بجهاز الضحية ومزايا كثيرة لم تكن متوفرة أصلا للضحية مثل جمع الكلمات السرية أو جمع ما تم ضغطة من أزرار لوحة المفاتيح أو عكس اتجاه حركة الفأرة أو تشغيل البرامج عن بعد.

تروجان خادم الملفات (File Server Trojan): وهذا النوع يجعل من جهاز الضحية خادم للملفات (FTP Server) مما يتيح للمهاجم وضع الملفات (ملفات تروجان التحكم عن بعد) أو تحميلها باستخدام جهاز الضحية .

تروجان إرسال كلمات السر (Password Sending Trojan): وهذا النوع له هدف واحد فقط وهو سرقة وجمع جميع كلمات السر التي يقوم الضحية باستخدامها على جهازه ومن ثم إرسالها بواسطة البريد الالكتروني إلى المهاجم.

تروجان جمع ضغطات أزرار لوحة المفاتيح (Key Logger Trojan): وهذا النوع يقوم فقط بجمع كل الضغطات التي يقوم بها الضحية على لوحة المفاتيح ومن ثم إرسالها بالبريد الالكتروني للمهاجم أو تجميعها في ملف لكي يتم تحميله لاحقا من قبل المهاجم.

تروجان الهجمات الموزعة لتعطيل الخدمات (Distributed Denial of Service Trojan): وهو أحدث أنواع التروجان حيث يقوم المهاجم باستغلال هذا النوع في القيام بعمل هجمات موزعة لتعطيل خدمات هامة أو مواقع مشهورة أو أجهزة أخرى على الشبكة بحيث يكون مصدر هذه الهجمات أجهزة الضحايا وليس المهاجم نفسه. فيقوم المهاجم بتشغيل الهجمة على أجهزة الضحايا واحد تلو الأخر أو يقوم باستخدام جهاز معين يقوم بمخاطبة جميع الأجهزة آليا.

تروجان إرسال الرسائل المزعجة (Spam Relaying Trojan): ويقوم هذا النوع باستغلال جهاز الضحية وحسابه البريد وذلك بإرسال رسائل مزعجة عن طريق جهاز الضحية وباستخدام اسمه وهويته ومن دون علمه.

طرق الإصابة به

توجد عدة طرق للإصابة ببرامج التروجان وأود أن أنوه إلى أن المستخدم قد لا يشعر أبدا بأن جهازه قد أصيب أصلا، ولكن يمكن تلخيص بعض طرق ومصادر الإصابة ببرامج التروجان من خلال النقاط التالية:

- الملفات المنتشرة على الانترنت أو بواسطة البريد الالكتروني: وهذا يعد المصدر الرئيسي لانتشار التروجان بحيث يتم إلصاق برنامج التروجان بأي برنامج تشغيلي آخر فتكون المحصلة برنامج واحد على شكل لعبة أو لقطة متحركة أو حافظ شاشة أو برنامج مشهور ومن ثم إرساله إلى قائمة بريدية أو منتدى ليتم تداولها بين المستخدمين، وهذه بعض امتدادات الملفات المشهورة التي يستخدمها التروجان للتخفي بها (.exe, .com, .bat, .src).
- البرامج المنسوخة أو مفكوكة الحماية: وقد يقوم المهاجم بفك حماية أحد البرامج المشهورة والمطلوبة بكثرة وإلصاق التروجان بها ومن ثم وضعها على خادم ملفات أو موقع ليتم تحميلها فيما بعد من قبل المستخدمين.
- برامج المحادثة المشهورة مثل (ICQ) أو(IRC): استخدام نسخ غير محدثة من برامج المحادثة التي تسمح بتبادل الملفات قد تتيح للمهاجم إرسال ملف وتشغيله على جهاز الضحية دون علمه، كما أن استقبال الملفات من الأشخاص الغير معروفين يشكل خطرا كبيرا على المتلقي.
- الدخول المباشر على الجهاز: إذا كان الجهاز مشترك أو غير محمي بكلمة مرور فسيستطيع أي شخص الدخول على الجهاز حسيا ومن ثم تحميل برنامج التروجان على جهازك ومن دون علمك.
- وجود مشاكل أو ثغرات في برامج متصفح الانترنت أو برامج البريد الالكتروني: مما يتيح لأصحاب المواقع أو مرسلي البريد الالكتروني من استغلال هذه الثغرات وتحميل الملفات دون علم صاحب الجهاز.

طريقة الحماية منها

يجب توفر الوعي الأمني لدي مستخدمي الشبكة ومعرفة خطورة هذه البرامج وعدم إعطاء الثقة الزائدة على الشبكة لأي شخص أو لأي موقع حتى لا تقع فريسة سهلة للمهاجمين، ويمكن للمستخدم حماية جهازه من برامج التروجان وذلك بإتباع الخطوات التالية:

- استخدام برامج مكافحة التروجان و الفيروسات.
- استخدام برنامج الجدار الناري (Firewall) للتحكم بالبرامج التي تستخدم الشبكة.
- تحديث برامج مكافحة التروجان والفيروسات باستمرار وبشكل آلي.
- تحديث نظام التشغيل والتطبيقات باستمرار وبشكل آلي.
- تفحص الجهاز باستمرار وبشكل دوري ضد برامج التروجان.
- عدم تحميل أو فتح البرامج من المواقع أو الأشخاص الغير موثوق فيهم أو الغير معروفين.
- عدم استخدام البرامج المنسوخة أو الغير معروفة المصدر.
- عدم تشغيل الملفات المنتشرة على الانترنت إلا بعد التأكد من نوع الملف وأنه لا يحتوي على تروجان حتى ولو كان من صديق.
- تحميل الملفات والبرامج من الموقع الرسمي وليس من مواقع بديلة.
- الحذر كل الحذر من برامج فك الحماية أو توليد الأكواد أو الكلمات السرية.
- حماية جهازك بكلمة سرية حتى لا يتطفل علية الآخرين أو يقومون بتحميل البرامج دون علمك.

أداة التحكم عن بعد Remote Administration Tool

أدوات التحكم عن بعد Remote Administration Tools هي برمجيات يستطيع مستخدمها على جهازه التحكم بجهاز آخر سواء كان في الغرفة نفسها أو في البناء نفسه أو في بناء في دولة أخرى عبر استخدام شبكة الانترنت. تستخدم هذه الأدوات ضمن الشركات من قبل قسم الـ IT ضمن الشركة لإدارة الحواسب في الشركة وضمان تحديث أنظمة التشغيل ومساعدة الموظفين ضمن الشركة على تنصيب البرامج (خاصة أنهم عادة لا يملكون حقوق مدير Admin وأيضا لمساعدتهم في حال وجود مشكلة معينة. تستخدم أيضا للتحكم بالأجهزة التي لا يمكن الوصول إليها بشكل فيزيائي (مثلا التحكم بأجهزة بقمر صناعي في المدار أو مسبار في الفضاء البعيد...) وغير ذلك من الاستخدامات المشروعة. من هذه البرمجيات برنامج تيم فيوير TeamViewer.

إلا أن فئة من هذه البرمجيات تعتبر من أخطر بالبرمجيات الخبيثة. تسمى هذه البرمجيات Remote Administration Tool Trojans أو Remote Administration Trojans واختصارا يطلق عليها راتس RATs كناية عن الجرذان في إشارة إلى الشعور المقزز الذي يصيب خبراء الأمن عندما يسمعون عن إصابة أحد المستخدمين بها.

إذا فالراتس RATs تمنح مستخدمها الصلاحيات للولوج إلى النظام وملفات النظام بصلاحيات مدير النظام.

أي بكلمات أخرى تمنح مستخدمها إمكانية معاينة كامل الملفات والأفلام وملفات الصوت المخزنة على الحاسب وإرسال نسخ منها عبر الانترنت إلى المهاجم. كما تسمح له بتشغيل ميكروفون الحاسب المصاب وتسجيل الصوت وإرساله إلى مستخدم الرات أو تشغيل كاميرا الحاسب المصاب وتسجيل الصورة وإرسالها إلى صاحب الرات أو كليهما (صوت وصورة) طالما كان الحاسب المصاب يعمل سواء كان المستخدم جالسا أمام الحاسب أو لم يكن. وأيضا تعطي مستخدم الرات إمكانية معاينة شاشة الجهاز المصاب عن بعد كما في البث المباشر طالما كان الجهاز متصلا بالانترنت. وقد تعطي مستخدم الرات إمكانية معاينة حسابات المستخدم على الانترنت (إن لم يكن قد أخذ الاحتياطات مسبقا لحمايتها) وقد يمكنه ذلك من استخدام الجهاز المصاب لإرسال رسائل إلى أشخاص آخرين بهدف إصابتهم أو استخدام الجهاز المصاب لمحاولة اختراق أجهزة أخرى باستخدام برمجيات خبيثة يشغلها مستخدم الرات عن بعد. ويحدث كل هذا دون علم صاحب الحاسب بذلك وغالبا دون إمكانية أن يعرف صاحب الحاسب حدوث ذلك. والقصص حول المصائب التي سببتها هذه البرمجيات كثيرة. وهي بذكل تشبه كثيرا برمجيات الروتكيتس Rootkits.

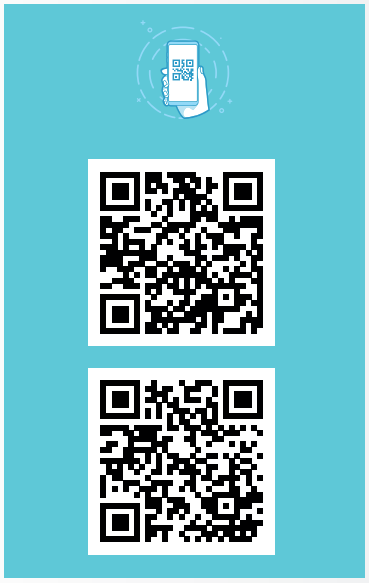
بالمختصر تعتبر الروتكيتس Rootkits ومثلها الراتس RATs على أنواعها من أخطر البرمجيات الخبيثة وأسوأها آثارا، بسبب خطورتها وبسبب صعوبة التعامل معها، سنناقش فيما يلي عددا من النقاط التي نعتقد أنها ستفيد القراء في فهم الأساليب الأكثر شيوعا بين المهاجمين لإصابة حواسب الضحايا بالروتكيتس (وأيضا بأحصنة طروادة للتحكم عن بعد Remote Administration Trojans والتي تعرف اختصارا بالـ راتس RATs)، وأيضا سنحاول توضيح ماذا يفعل المهاجم بعد أن ينجح في تنصيب الروتكيت على جهاز الضحية. ثم سننتقل لمناقشة أساليب الوقاية من الإصابة بالروتكيتس وسنسرد أساليب إدارة الخطورة Risk Management المتعلقة بكارثة الإصابة بروتكيت وفي النهاية كيف نتصرف في حالة الشك أو اليقين بالإصابة بها. قبل المتابعة يجب الإشارة بأن يجب التعامل مع حالة الشك بالإصابة بالروتكيت كما في حال اليقين بالإصابة بالروتكيت، أي يكفي الشك بالإصابة لأخذ كامل الخطوات التي نأخذها في حال التأكد من الإصابة.

استراتيجيات المهاجم لإصابة الجهاز الهدف برات RAT أو بروتكيت Rootkit:

يحتاج المهاجم إلى تنصيب الرات RAT أو الروتكيت Rootkit على الحاسب الهدف لذلك يحتاج للحصول على صلاحيات مدير للنظام لتنفيذ هجومه. يعتمد المهاجمون استراتيجيات مختلفة للوصول لتنصيب الرات أو الروتكيت على الحاسب الهدف.

نورد هنا عددا من هذه الاستراتيجيات:

استغلال ثغرات في نظام التشغيل المتصل مع شبكة الانترنت. يقوم المهاجم هنا باستغلال ثغرة ما في نظام تشغيل الجهاز المتصل بالانترنت ويقوم المهاجم بذلك عن بعد عبر الانترنت. يقوم المهاجم بعد استغلال الثغرة بتنصيب الرات أو الروتكيت ومتابعة هجومه. تقوم شركات الأمن الرقمي باكتشاف الثغرات والاعلان عنها مشجعة بذلك الشركات المسؤولة عن أنظمة التشغيل أو التطبيقات إلى سد الثغرات لكن المشكلة تحدث عندما يكتشف المخترقون الثغرات قبل أن تقوم شركات الأمن الرقمي بالاعلان عنها، أو عندما لا يقوم مدراء الأنظمة في المؤسسات أو الشركات أو الأفراد بسد الثغرات في أنظمة التشغيل التي يديرونها. يمكن معاينة لوائح الثغرات بشكل مستمر عبر مواقع مختصة بذلك مثل:



استغلال أساليب الهندسة الاجتماعية Social Engineering لخداع المستخدم وإقناعه بتشغيل ملف على حاسبه (مثلا يقوم الضحية بتشغيل ملف مرفق في إيميل يبدو سليم لكنه في الحقيقة خبيث) يؤدي بالنتيجة إلى تنصيب الرات أو الروتكيت على الحاسب ليتابع المهاجم بعد ذلك هجومه. تحتاج هذه الاستراتيجية قدرات تقنية متواضعة بالمقارنة مع الاستراتيجية السابقة. تعتبر هذه الطريقة من أكثر الطرق شيوعا للإصابة بالراتس بالروتكيتس. والطريقة الوحيدة التي يستخدمها الجيش السوري الالكتروني لتنصيب برمجية روتكيت خبيثة على أجهزة ضحاياهم. لذلك نجد أنه من المهم قراءة المقالة التالية حول الهندسة الاجتماعية Social Engineering.

ماذا يفعل المهاجم بعد إصابة الجهاز الهدف مباشرة Attacker's next steps:

بعد أن يتمكن المهاجم من تنصيب الرات أو الروتكيت على الحاسب وتشغيله

يقوم المهاجم عادة (سواء بشكل مؤتمت أو بشكل يدوي).

يقوم المهاجم بمحاولة إخفاء آثار الاختراق كي لا يتيح للضحية ملاحظة أن جهازه مخترق وبحيث يعمل المهاجم بشكل سري وخفي. فاكتشاف حدوث التدخل أو أي نشاط أو حدث على الحاسب الضحية سيساعده على معالجة المشكلة وأيضا على تجنب المشكلة في المرات القادمة. تقوم الروتكيتس عادة بهذا العمل وبما أن سجلات الوصول للموارد access logs هي أهم الملفات التي يلجأ لها الضحية لكشف الولوج الغير شرعي لحاسبه.

لذلك يعمد المهاجم على حذف المعلومات التي تشير إلى دخوله إلى الحاسب من هذه السجلات وأي سجلات أخرى التي تشير للعمليات التي تم إجراؤها على الحاسب. فعلى سبيل المثال تقوم الروتكيت بحذف أي تسجيل أو بند في سجلات النظام لأي عملية process تم تشغيلها عليه، كما قد يستخدم لإخفاء بعض الملفات التي أنشأها المهاجم أو تعديل بعض أوامر النظام لتعطي نتائج مزورة للمستخدم بحيث لا يتم اكتشاف أي تغيير تم حدوثه على ملفات النظام.

يقوم المهاجم بفتح بوابات خلفية Backdoors في النظام كي يقوم المهاجم عبرها بإرسال البيانات والتحكم بالجهاز وبالرات وبالروتكيت. من أكثر الأساليب شيوعا بالنسبة للروتكيتس هي فتح قناة اتصال إس إس إتش SSH إذ أن هذه القناة تمنح المهاجم إمكانية الوصول إلى الحاسب والتحكم به بالإضافة لإمكانية تشفير البيانات التي تمر عبر قناة الاتصال هذه ما يساعد في منع تحليلها من قبل أنظمة كشف التدخل Intrusion Detection Systems IDSs و أجهزة تجنب التدخل Intrusion Prevention Systems IPSs.

يقوم المهاجم بمعاينة الحاسب ومعاينة الملفات الموجودة ليعرف إن كان هناك ملفات مهمة وإن كان استمرار الهجوم موضوع مهم.

يقوم المهاجم بمحاولة معاينة حسابات الضحية أونلاين (إذا كانت كلمات سرهم محفوظة في المتصفح مثلا أو عبر متابعة شاشة الضحية بشكل مباشر أيضا لتقييم الفائدة التي استخدامه لصلاحيات وصول لموارد إدارية privileged access، قد يمنحه هذا إمكانية التدخل بالحاسب الهدف أو الشبكة أو الأجهزة الأخرى المتصلة بالحاسب.

يقوم المهاجم بمتابعة الهجوم بالشكل الذي يناسبه أهدافه

الوقاية من هذا الهجوم

بناء على ما ورد سابقا من استراتيجيات إصابة الضحية بهجوم رات RAT أو بهجوم روتكيت Rootkit ، نورد فيما يلي عددا من النصائح الموجهة للمستخدمين:

احرص على تحديث نظام التشغيل بشكل دوري لتتمكن من تغطية الثغرات الأمنية. ومن الممكن أن يتم ذلك بشكل تلقائي عبر تفعيل خاصية التحديث التلقائي.

قم باستخدام "حساب غير مدير" للاستخدام اليومي حتى تتجنب تحميل برامج غير مرغوب بها. وعند استخدامك "حساب مدير" كن حذرا عند تنصيب أية برامج إضافية. فعند استخدام حساب غير مدير لا يمكن لك تنصيب برنامج بصلاحيات مدير للنظام بطريق الخطأ. ما قد يساعدك على ملاحظة هجوم برات وإفشاله.

إستخدم كلمات سر قوية لمنع الآخرين من الوصول إلى جهازك الشخصي.

لا تقع ضحية لأساليب الهندسة الاجتماعية

انظر بعين الشكل إلى كل الملفات المرفقة ضمن البريد الالكتروني ووسائل الاتصال

الأخرى مثل سكايب. احذر بشكل خاص من الملفات ذات اللواحق التالية

. Exe .cmd .bat .vbs .js .mdb .doc .xls .lnk .zip .scr .wsf .rar

لا تقم بفتح هذه الروابط حتى بعد التأكد من مصدرها ومرسلها (إذ قد يكون مرسلها قد أصيب والمهاجم يحاول استغلال ثقتك بالضحية الأولى لإصابتك).إن كنت مضطرا لتحميل أحد هذه الملفات أو المرفقات قم باستخدام موقع http://www.virustotal.com للتأكد من عدم احتوائه إلى رات Rat أو روتكيت Rootkit أو ملف خبيث آخر معروف.

ثم بدل تشغيل الملف على جهازك مباشرة قم بتجربة الملف على حاسب افتراضي Virtual Machine بحيث تقلل بذلك إمكانية إصابة نظام التشغيل الأساسي لديك بالرات أو الروتكيت وتقتصر الإصابة عندها على الحاسب الافتراضي Virtual Machine التي يمكن بسهولة حذفه (مع الرات أو الروتكيت). إن استخدام برمجيات sandbox أو البيئة الافتراضية لتنصيب البرمجيات تساعد على عزل البرمجيات التي قد تكون مصابة بالرات أو بالروتكيت عن نظام التشغيل و بالتالي تعمل على منع إصابة النظام الأصلي به.

- استخدم تطبيق جدار ناري Firewall معد بشكل صحيح ومناسب
- **قم بعمليات إصلاح أمنية دورية للنظام**
- إن كنت من مطوري البرمجيات أو كان جهازك يتضمن مترجمات برمجية compilers قم بالحد من إمكانياتها على الأجهزة المستضيفة، العديد من برمجيات الرات RAT أو الروتكيت Rootkit تحتاج إلى مترجمات compiler و مكتبات libraries ليتم تنصيبها، فالحد من وجودها على أنظمة الجهاز الهدف يمنع من تنصيب بعض الروتكيت.
- لا تقم أبدا بتحميل تطبيقات أو برامج من مصادر غير موثوقة على الإنترنت أو من أقراص مضغوطة أو فلاش ميموري. وتأكد عند تحميل التطبيق من أن الـ Checksum الخاص بالتطبيق مطابق للـ Checksum المذكور في الموقع (للتأكد أن ملف التطبيق هو الملف الأصلي وغير مزور)
- تأكد دوما من قفل جهازك وعدم تركه بمتناول الآخرين.

الاستعداد لكارثة الإصابة Preparing for a catastrophy

تعتبر الإصابة سواء برات أو بروتكيت إحدى أسوأ الكوارث التي قد تصيب الحاسب. بالوقت نفسه هي أكثر أساليب الهجوم الالكتروني انتشارا منذ بداية الأزمة في سوريا. نلاحظ في فريق سلامتك بشكل مستمر محاولات المهاجمين سواء من الجيش السوري الالكتروني أو من غيرهم للسيطرة على حواسب ضحاياهم عبر استخدما مختلف أساليب الهندسة الاجتماعية Social Engineering لتنصيب الراتس RATs أو الروتكيتس Rootkits على أجهزة الضحايا.

ولأن احتمال الإصابة بها وارد جدا. نرى أن الاستعداد لكارثة من هذا النوع أمر مهم جدا لتفادي نتائجه. لا نتحدث هنا عن أساليب الوقاية من الإصابة ولا عن أساليب العلاج عند الإصابة أو الشك بالإصابة. نتحدث عن تقليل أضرار الإصابة بروتكيت في حال حدوثها رغم احتياطات الوقاية. أي علينا أن نعالج الموضوع كما يعالج اليابانيون موضوع الزلازل في بلادهم. فالزلازل تقع في اليابان ومع ذلك عدد ضحاياها وآثارها منخفض للغاية. السبب هو أن اليابانيين وضعوا الآليات المناسبة للتعامل مع هذا النوع من الكوارث بحيث أنه عندما تقع الكارثة يكون كل شئ في مكانه لتقليل آثارها. من الجدير بالذكر يسمى هذا النوع من التحليل تحليل الخطورة Risk Analysis أما تقييم الخطورة Risk Assessment وتسمى الاجراءات التي يتخذها المرء للتقليل من آثار الكارثة بتخفيف الخطورة Risk Mitigation والمصطلح الذي يشمل تحليل الخطورة وتقييمها والاجراءات الازمة لتقليل الخطورة وغيرها من النواحي التي تعنى بالخطورة بمصطلح إدارة الخطورة Risk Management. وهو فرع مهم جدا من فروع الإدارة وأيضا من فروع إدارة أمن المعلومات Information Security Management.

إذا كيف نقلل من أضرار كارثة الإصابة بروتكيت أو برات؟ أو كيف نخفف من الخطورة؟

- تقسيم القرص الصلب إلى جزء لنظام التشغيل وجزء للملفات.
- إجراء النسخ الاحتياطية لنظام التشغيل.
- إجراء نسخ احتياطية للملفات.
- عدم حفظ كلمات سرّ الحسابات في المتصفح. ننصح هنا باستخدام تطبيق كي باس KeePass
- استخدام ميزة التحقق بخطوتين أينما توفّرت Two Factor Authentication
- الاحتفاظ بالملفات المهمة بشكل مشفر.
- تغطية الكاميرا عند عدم استخدامها.
- فصل الميكروفون عند عدم استخدامه.
- جعل محتوى الحاسب يبدو وكأن الحاسب لا يستحق جهد المخترق ووقته.

اكتشاف إصابة الحاسب بالروتكيت Rootkit attack detection

ليس من السهل اكتشاف الروتكيت و ذلك لأن المهاجمين يعملون على إخفاء آثار الاختراق وآثار الهجوم والروتكيت تستخدم تقنيات مختلفة لإخفاء نشاطها على الحاسب الضحية. على الرغم من ذلك يعتقد البعض بأنه لا يمكن أن يتواجد مهاجم باحترافية عالية جداً لدرجة عدم ترك أي دليل على حدوث التدخل و هو ما يتم استخدامه لاكتشاف الروتكيت عادة.

وبما أن من الصعب على المستخدم العادي اكتشاف الروتكيت بنفسه فعليه الاستعانة إما بخبراء لاكتشافه أو ببعض الأدوات، لذلك ننصح بدل الانتظار للتأكد بالإصابة بروتكيت والتصرف بعدها بأخذ الاحتياطات الكاملة للوقاية من الإصابة بروتكيت والمذكورة في هذه الدليل وأيضا اتخاذ الاجراءات التي تخفف من آثار كارثة الإصابة المذكورة في هذه الدليل وأيضا القيام بالإجراءات العلاجية بمجرد الشك بالإصابة. نورد فيما يلي بعض الإيضاح حول صعوبة اكتشاف الروتكيت.

برمجيات للكشف عن الروتكيت

لا تتوفر حاليا أدوات أو برمجيات تمتلك القدرة الكاملة على التقاط كل أنواع الروتكيت على الأجهزة. إلّا أنه هناك عدد من الأدوات التي قد تستطيع اكتشاف المشهور منها قبل تنصيبها على أنظمة التشغيل ويندوز Windows مثل حزم مضادات الفيروسات. لذلك إن كان المستخدم يستخدم برمجية روتكيت مشهورة في هجومه قد يستطيع مضاد فيروسات اكتشافه قبل حدوث الضرر لكنه من الصعب جدا أن يكتشفه بعد حدوث الضرر بسبب تقنيات التخفي التي تستخدمها معظم برمجيات الروتكيت لتفادي الاكتشاف من مضاد الفيروسات.

يوجد أيضا أدوات منفصلة عن حزم مضادات الفيروسات تساعد على التخلص من روتكيتس معينة مثل DarkComet RAT Remover وهي أداة خاصة لاكتشاف وإزالة أحد أنواع الروتكيت والذي يطلق عليه اسم DarkComet.

هناك أيضا أنظمة التقاط التدخل Intrusion Detection system وأنظمة تجنب التدخل Intrusion prevention Systems خاصة بالشبكات يمكن تحليل بياناتها لالتقاط أي حركة مشبوهة من قبل أي نظام تم استهدافه. وهو الطريقة التي تعتمدها الشركات والمنظمات الكبيرة لكشف كارثة حدوث اختراق بروتكيت.

أما بالنسبة لأنظمة التشغيل لينوكس Linux بالتحديد أو الشبيهة بها يتوفر عدد إضافي من الأدوات التي تكشف الشهير من أنواع الروتكيت المشهورة مثل برنامج Chkrootkit و برنامج Rootkit Revealer ويجب التأكيد على القيام بتحديث هذه البرمجيات والأدوات بشكل دائم كحال مضاد الفيروسات.

اكتشاف الروتكيت بشكل ظرفي

أيضا يمكن كشف وجود روتكيت على جهاز ما أو الشك بوجوده بشكل ظرفي, فمثلا:

- وصول رسالة بريد الكتروني من جهة A إلى جهة B على الرغم أن A أكد لـ B أنه لم يرسل أي بريد الكتروني توحي أن حساب الجهة A مخترق وربما سبب الاختراق وجود روتكيت على جهاز الجهة A.
- ملاحظة كمية كبيرة من المعلومات المرفوعة مع الانترنت على الرغم من عدم رفع أي ملف إلى الانترنت يشير إلى أن هناك من يرسل من حاسبك حجما كبيرا من المعلومات قد يكون الـ روتكيت
- يقوم نظام التشغيل بتسجيل عمليات تسجيل الولوج وعمليات الوصول للموارد والعمليات الهامة التي تجري عليه عادة. تسمى هذه السجلات بشكل عام System Logs. قد يستطيع الخبير من قراءة سجلات نظام التشغيل أن يكتشف حدثا يشير إلى وجود روتكيت على الجهاز أو قد يلاحظ أن حدثا ما قد اختفى من جداول سجلات نظام التشغيل ما يشير إلى وجود شئ ما يحاول إخفاء آثاره وقد يكون الروتكيت.

معالجة الإصابه أو الشك بالإصابة برات أو روتكيت Dealing with a Rootkit or RAT attack

عند الإصابة أو الشك بالإصابة بروتكيت أو برات على المستخدم القيام بالخطوات التالية:

تغطية الكاميرا بغطاء ما (إن كان للجهاز كاميرا مدمجة) أو فصل الكاميرا المتصلة بالجهاز (إن وجدت)

تغطية الكايكروفون (إن كان للجهاز مايكروفون مدمج) أو فصل المايكروفون المتصل بالجهاز (إن وجد)

فصل الجهاز عن الانترنت عبر فك كابل الانرتنت LAN أو عبر وقف تشغيل الـ Wireless Router أو وضع الجهاز خارج نطاق الوصول للانرتنت اللاسلكي في حال لم يكن بالإمكان وقف تشغيل الـ Wireless Router لقطع إمكانية التواصل بين البرمجية الخبيثة والمهاجم. تبليغ المختصين بموضوع الأمن الرقمي (سواء مدير الأمن الرقمي في المؤسسة التي تعمل ضمنها) أو الزميل أو الصديق الذي تستشيره في موضوع الأمن الرقمي عن حدث الإصابة أو الشك بالإصابة عبر استخدام جهاز آخر للتبليغ (إما بشكل مباشر، أو عبر الهاتف أو عبر الانترنت (لكن لا تستخدم الجهاز المصاب في ذلك الغرض).

إن كان القرار إزالة الرات أو الروتكيت من الجهاز

تأكد مجددا من أن الجهاز غير متصل بالانترنت عبر فك كابل LAN أو عبر وقف تشغيل الـ Wireless Router أو وضع الجهاز خارج نطاق الوصول للانرتنت اللاسلكي في حال لم يكن بالإمكان وقف تشغيل الـ Wireless Router

حاول تقدير متى تمت الإصابة بالروتكيت.

ابحث عن نسخة احتياطية Backup لنظام التشغيل تحمل تاريخ قبل التاريخ المقدر للإصابة.

قم باستعادة النظام Recovery باستخدام النسخة الاحتياطية إلى مرحلة ما قبل الإصابة بالروتكيت وفي حالة الشك في توفر نسخة نظيفة من النظام يمكن استعادتها، على المستخدم أن يقوم بإعادة تنصيب النظام و البرمجيات من جديد للتأكد من أن الحاسب قد تمت معالجته تماماً من الإصابة.

يجب بعد ذلك أن يقوم المصاب بمحاوبة كتابة تقرير يشمل مصدر الإصابة "البرمجية الخبيثة"، نوع الإصابة "الملفات المتضررة.."، الهدف من الإصابة "المعلومات و البرمجيات المستهدفة" ، و الجهات المهاجِمة و المستهدَفة، والاستفادة من هذا التقرير لإعلام الجهات التي قد تكون قد تأثرت بسبب الإصابة وبسبب فقدان سرية المعلومات مثلا.

وأيضا من المهم إعلام المختصين التقنيين مثل إخبار العاملين في مشروع سلامتك SalamaTech عن الروتكيت كي يقوم الخبراء بمحاولة توعية بقية المجموعات العاملة والشركات التقنية والمستخدمين حول وجود التهديد الجديد وأيضا معاينة الملف الذي يحتوي البرمجية الخبيثة وتحليل عملها (ضمن بيئة آمنة في مختبراتها) وفي النهاية إعلام شركات مضادات الفيروسات ومخدمات الانترنت والشركات صاحبة أنظمة التشغيل بوجود تهديد جديد لتشمل تحديثاتها إغلاق الثغرات التي تستغلها البرمجية الخبيثة الجديدة وللكشف عنها ضمن الملفات المرفقة من قبل مضادات الفيروسات.

مصادر الدليل

موقع الحماية الرقمية

www.iraqi-alamal.org

الفهرست