تحذير أمني حول فيروسات الفدية RANSOMEWARE

**يستهدف هذا التحذير الأمني المؤسسات والشركات العامة والخاصة والأفراد**

مركز أمن المعلومات

6\_9\_2021

**مقدمة:**

نظراً لازدياد معدل الهجمات السبرانية باستخدام فيروسات الفدية حول العالم، والتطور المستمر في تقنيات وأساليب الهجوم، وتسجيل العديد من الإصابات التي طالت شركات عالمية كبرى، ورضوخ هذه الشركات لمطالب المهاجمين، وتزايد عدد حالات الإصابة بهذه الفيروسات على الشبكة السورية، حيث تبلغ مركز أمن المعلومات بالعديد من الإصابات (خمس حالات إصابة خلال شهر آب فقط) طالت مؤسسات وأفراد، وفي إطار مهام مركز أمن المعلومات في التحذير المبكر من الأخطار المعلوماتية والتوعية الأمنية وجدنا أهمية بالغة في إعادة التحذير من مخاطر هذه البرمجيات الخبيثة وتوعية مستخدمي الشبكة السورية حول أفضل الطرق والممارسات للوقاية منها.

**فما هي فيروسات الفدية وطرق انتشارها وكيف نحمي أنفسنا منها؟**

**فيروس الفدية:** وهو نوع من أنواع البرمجيات الخبيثة تعمل عند الإصابة على تشفير كافة البيانات الموجودة على نظام الضحية (سواء كان حاسب أو مخدم أو هاتف ذكي) وتمنعه من الوصول إليها أو استخدامها، وبعد الانتهاء من عملية تشفير الملفات تظهر رسالة للضحية محتواها أنه يجب دفع مبلغ مالي (فدية) للحصول على مفتاح لفك تشفير الملفات وإتاحة إمكانية الوصول إليها مرة أخرى.

تتسبّب بشكل أساسي في فقدان البيانات وتوقف الأعمال، وخسائر مادية ومعنوية، بالإضافة إلى مخاطر تشويه السمعة وتراجع ثقة العملاء بالخدمات، والتكاليف التي يتطلبها استعادة النظام من وقت وجهد ومال.



**طرق الإصابة:**

نعرض فيما يلي أشهر طرق الإصابة بهذه البرمجيات الخبيثة:

1. تحميل وتثبيت برمجيات (برامج-أدوات-ألعاب....) غير نظامية أو مجانية على النظام مباشرة من مواقع ويب غير آمنة أو زائفة.
2. تصفّح المواقع الإباحية أو الإعلانات والتي يتم من خلالها إعادة توجيه المتصفح (redirection) إلى صفحات لم يطلبها المستخدم قد تحتوي على برمجيات خبيثة.
3. فتح المرفقات والروابط في البريد الالكتروني والتي ترد من عناوين مجهولة (Spam).
4. فتح الروابط الواردة في رسائل تطبيقات المحادثة الفورية أو ضمن المنشورات أو التعليقات على وسائل التواصل الاجتماعي.
5. فتح الروابط التي تصل عبر رسائلSMS من عناوين خارجية مجهولة.
6. تداول أقراص التخزين القابلة للإزالة (HD, Flash Memory, CD , DVD).
7. تجاهل التحذيرات الأمنية التي تطلقها تجهيزات أو برمجيات أو ميزات الحماية الأمنية.
8. استخدام بروتوكولات تخاطب غير آمنة مثل بروتوكول الاتصال بسطح المكتب عن بعد (RDP) على نظم تشغيل ويندوز، ووجود ثغرات أمنية في النظم المعلوماتية يتم استغلالها لاختراق هذه النظم وزرع البرمجيات الخبيثة.

**طرق الوقاية:**

من الصعب جداً معالجة آثار الإصابة بفيروسات الفدية مالم تتخذ الإجراءات الوقائية، وتعتبر الإصابة بالإصدارات الحديثة منها، أو التي تعتمد منهجية التشفير بالاتصال المباشر (Online) مستحيلة العلاج كما تؤكد شركات عالمية متخصصة بالحماية، وفي حالات خاصة قليلة جداً يمكن استعادة البيانات بعد تشفيرها، الكثير من فيروسات الفدية المنتشرة حالياً تقوم بتعطيل أو تخريب كافة الحلول الممكنة التي تتيحها الشركات المطورة لاستعادة الملفات أو النظام.

وطالما أننا مضطرون لاستخدام البرمجيات الغير مرخصة (cracked) أو المجانية، وعدم وجود خبرة كافية لدى أغلب مستخدمي شبكة الانترنت، وإغفال أهمية الأمن السبراني لدى الكثير من الجهات العامة والخاصة، فنحن معرضون في أي لحظة للإصابة بفيروسات الفدية أفراداً أو مؤسسات، وعليه فإن اتخاذ مجموعة من الإجراءات الوقائية هو أفضل طرق الحماية ويسهل عملية المعالجة بعد الإصابة وتخفيف الأضرار الكارثية الناجمة عنها، وأهمها:

1. تنصيب برامج مضادة للبرمجيات الخبيثة ذات تصنيف عالمي جيد وتحديثها بشكل مستمر وعدم تجاهل التحذيرات التي تعرضها للمستخدم، وأقل الإيمان تفعيل كافة ميزات الحماية التي توفرها نظم التشغيل مثل windows security.
2. عدم فتح أي مستندات أو روابط أو ملفات مرفقة من البريد الإلكتروني دون التأكّد من مصدر تلك الملفّات أولاَ، وإعلام مدير الشبكة أو مسؤول أمن المعلومات في المؤسسة أو استشارة شخص خبير في هذا المجال.
3. إنشاء بيئة افتراضية معزولة (VMware \_ VBox) لتجربة الكراك أو الباتش أو لفتح الملفات المحمّلة عبر البريد الالكتروني، هذه الطريقة تضمن عدم تعرّض الحاسب للإصابة بالفيروس بل تبقى الإصابة محصورة في البيئة الافتراضية.
4. فحص أقراص التخزين القابلة للإزالة باستخدام برنامج مضاد الفيروسات، والتأكد من خلوّها من البرمجيات الخبيثة قبل استخدامها.
5. أخد الحيطة والحذر في تصفّح الانترنت، وعدم زيارة المواقع الغير موثوقة، والحذر من النوافذ المنبثقة التي تجبر الضحية على خيار واحد لإغلاق النافذة المنبثقة، وهنا يجب التنويه إلى أنه يجب إغلاق هذه النوافذ من زر الإغلاق حصراً ويجب عدم ضغط أي زر ضمن النافذة وفي حال لم يتمكن المستخدم من معرفة ما الذي يجب فعله فيجب عليه إغلاق المتصفح بشكل كامل.
6. النسخ الاحتياطي لنظام التشغيل، وحفظ النسخة على وسائط تخزين خارجية، ليتمكّن المستخدم من استعادة النظام لما كان عليه قبل الإصابة، وتحديث نظم التشغيل بشكل مستمر.
7. إنشاء نسخ احتياطية من الملفّات المهمّة وقواعد البيانات بشكل دوري وحفظها على وسائط تخزين خارجية وعدم وصلها بأي جهاز حاسوبي قبل التأكد من سلامته.
8. عدم استخدام خدمة الاتصال بسطح المكتب عن بعد (RDP) -خصوصاً لمخدمات نظم التشغيل ويندوز- إلا ضمن الشبكات الافتراضية المحلية .(VPNs)
9. استخدام نظم تشغيل لينوكس بتوزيعاتها المتعددة والتي تعتبر أقل تعرضاً للإصابة، والاستغناء قدر الإمكان عن استخدام نظم تشغيل ويندوز خصوصاً لتشغيل الخدمات الحساسة أو إدارتها عن بعد، وإيلاء نفس الأهمية لحماية الطرفيات المستخدمة للولوج للخدمات، كما توفر العديد من توزيعات لينوكس إمكانية الوصول للخدمات عن طريق بروتوكولات آمنة مثل SSH أو عن طريق متصفحات الويب أو أدوات أخرى.
10. تطوير سياسات التحكم بالنفاذ وتطبيقها، والمراقبة والمتابعة للالتزام بها.
11. التوعية الأمنية المستمرة للموظفين بمختلف مستوياتهم الإدارية والفنية حول طرق الحماية والاستخدام الآمن لشبكة الانترنت والحد من مخاطر الهندسة الاجتماعية.
12. يجب على المؤسسات والشركات وقطاعات الأعمال والمصارف التي تقدم خدمات أو تمتلك بيانات حساسة أن تطور حلولاً أمنية متقدمة متناسبة مع درجة حساسية البيانات التي تمتلكها مثل نظام إدارة التهديدات والحوادث الأمنية SEIM، وأن تطور نظام إدارة أمن المعلومات ISMS المتناسب مع طبيعة عملها.

**إعداد**

**م. سُليمه كنينه**

**رئيس مركز أمن المعلومات**

**المهندس سلمان سليمان**