الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

انتشار البرمجية الخبيثة BlackNET من خلال أداة مكافحة فيروس كورونا المزيفة

قرر مجموعة من قراصنة الإنترنت وعن طريق المزاح إنشاء موقعين يهدفان للإعلان عن نوع من أدوات الحماية من الفيروسات التي من المفترض أنها تحمي المستخدمين من المرض واسع الانتشار، وهما:

antivirus-covid19.site ، corona-antivirus.com

وكما هو معروف أن هذا الهدف غير واقعي تماماً، والأهداف المعلنة لتلك البرمجيات لا يمكن فعلاً تحقيقها، إذ لا يمكن لبرنامج حاسوبي أن يقي الإنسان من الإصابة بفيروس عضوي، ومع ذلك ادعى هؤلاء القراصنة أن هذه البرمجيات يمكن أن تقدم:

- حماية فعالة من الفيروس عن طريق الجهاز المحمول الخاص بك.
- هاتفك النقال يحميك من الفيروس طالما أن التطبيق يعمل.

وهذا أمر طريف ومضحك ...

✓ يجب أن يبقى في ذهنك أنه ليس هناك وسيلة إلكترونية لحماية نفسك من العدوى بفيروس covid-19، ما تستطيع فعله حقاً هو القيام بالإجراءات الوقائية كالحد من أوقات الخروج من المنزل، ارتداء الأقنعة الواقية، غسل اليدين .....إلخ

وقد رُصِد موقع corona-antivirus.com المشبوه لأول مرة من قبل فريق باحثين في مجال الأمن السيبراني واسمه malwarehunterteam والذي أعلن النتائج التي توصل إليها على موقع تويتر في بداية شهر آذار.

هذه النطاقات وغيرها، بما فيها النطاق antivirus-covid19.site كانت قد اكتُشفت أيضاً من قبل مختصيّ تقييم البرمجيات الخبيثة، إن الموقع antivirus-covid19.site غير نشط حالياً، بينما الموقع corona-antivirus.com مازال الوصول إليه ممكناً، ولكن أُلغِيت كافة روابط البرمجيات الخبيثة منه، ولكن قد تتكرر هذه الهجمات مستقبلاً وبنفس الأسلوب.

البرنامج الخبيث BlackNET RAT يمكنه القيام بعدة أنشطة على الجهاز المصاب

إن الهدف الرئيسي للأشخاص الذين قاموا بإنشاء المواقع التي تحوي برامج مكافحة الفيروسات ليس مساعدة المستخدمين على حماية أنفسهم من المرض لكن لتثبيت أداة الوصول البعيد BlackNET RAT من خلال روابط التحميل.

يتضمن الملف التنفيذي للبرنامج الذي يتم تحميله محتوى تجاري معروف باسم Themida بالإضافة للبرنامج الخبيث، وعند تنصيبه يقوم بتحويل نظام الحاسب إلى نظام روبوت شبكي (botnet) مبرمَج لأخذ أوامره من الموقع instaboom-hello.site الذي تستخدمه البرمجية الخبيثة BlackNET.

هنالك العديد من الأنشطة التي يمكن لهذه البرمجية الخبيثة القيام بها بمجرد الإصابة ومنها:

- تسخير موارد الحاسب لشن هجمات حجب الخدمة الموزعة DDOS Attacks.
- سرقة كلمات السر التي يتم حفظها على الجهاز وملفات الارتباط من متصفح الويب.
- تسجيل كافة النقرات التي يقوم بها المستخدم على لوحة المفاتيح.
- أخذ لقطات للشاشة، تشغيل أكواد برمجية خبيثة أخرى.
- التحكم بتشغيل وإطفاء وظائف الجهاز ..

✓ **كن يقظاً للقراصنة الذين يريدون استغلال جائحة كورونا الرهيبة:**

إن استغلال جائحة كورونا في نشر برمجية BlackNET ليس المحاولة الوحيدة للإساءة للمستخدمين، فمنذ أن بدأ انتشار المرض بدأ قراصنة الإنترنت بإطلاق حملات التصيُّد التي تسعى لإصابة المستخدمين بأشكال متعددة ببرمجيات خبيثة خطيرة، وأحد المحاولات الأخيرة كان نشر أداة Crimson RAT، وقد بدأت هذه الحملة من قبل مجموعة القراصنة المعروفة باسم

ATP36. حيث قاموا بإعطاء نصائح صحية وهمية في صيغة ملفات تنفيذية من خلال رسائل التصيد الإلكتروني التي شملت برمجيات خبيثة.حالما يقوم المستخدم بتنصيب الملف الخبيث فإن المحتوى الضار سينفَّذ على الحاسب المستهدف وتحدث الإصابة.

- ✓ إن أفضل طريقة لحماية نفسك من هذه البرامج الضارة هي تجنُّب تحميل وتثبيت ملفات غير معروفة من الإنترنت. إذا قمت بتحميل ملف إلى جهاز الكمبيوتر الخاص بك، فإنك بحاجة إلى فحصه أولاً بواسطة برنامج مكافحة البرمجيَّات الضارّة للتأكد من أنه لا يحمل أي محتوى خبيث مخبأ ضمنه.

مع تمنياتنا لكم بالصحة والسلامة

إعداد

م. رشا العجي

مركز أمن المعلومات