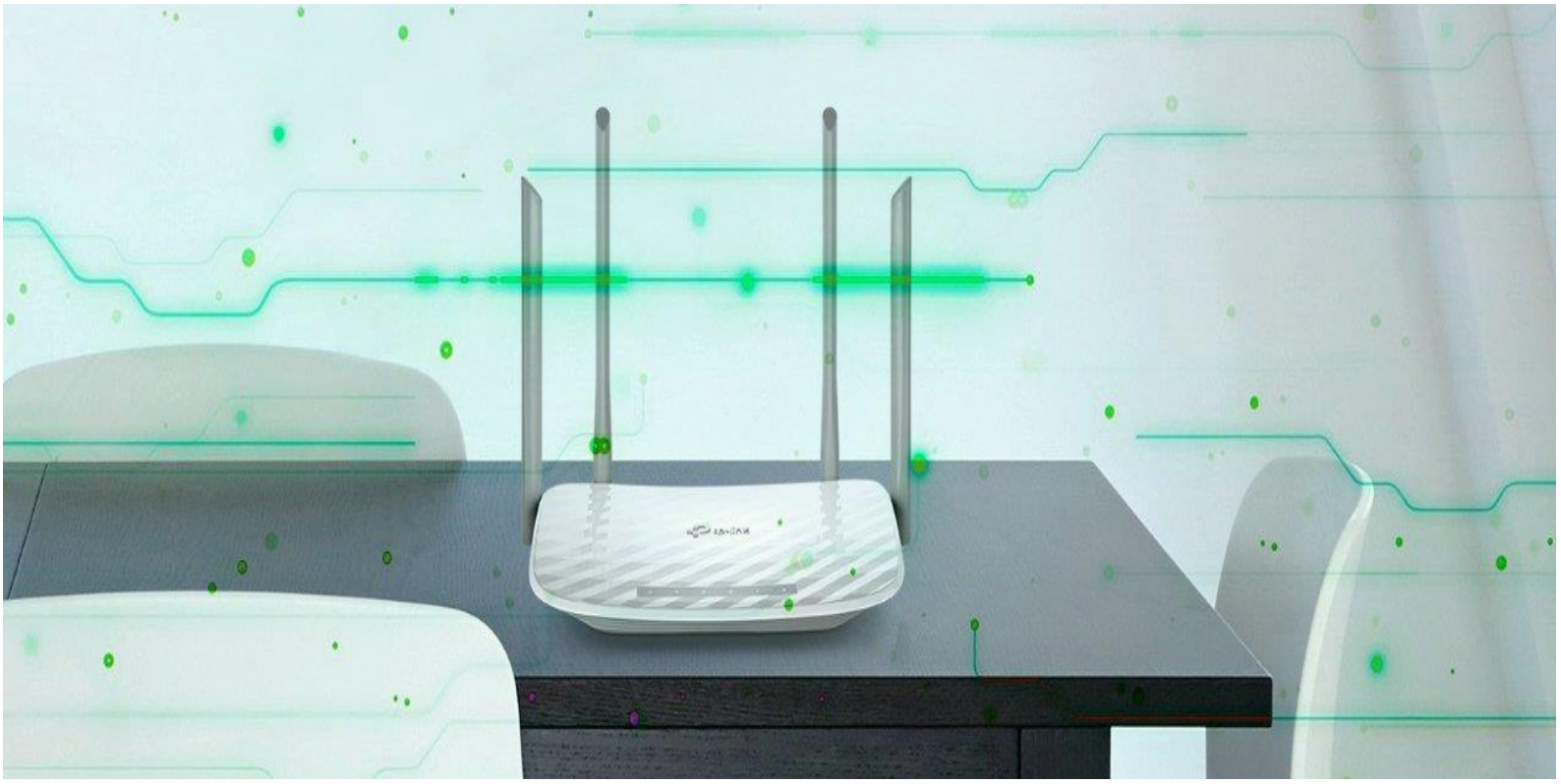
الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

المخترقون يسرقون موجهات DNS لنشر تطبيقات COVID-19 الخبيثة



إعداد
قسورة ع. عيسى
مركز أمن المعلومات

هجوم إلكتروني جديد هو اختراق إعدادات DNS الخاصة بالموجه، بحيث تعرض متصفحات الويب تنبيهات لتطبيق COVID-19 المزيف من معلومات منظمة الصحة العالمية، وهو برنامج Oski الخبيث لسرقة المعلومات. على مدى الأيام الخمسة الماضية، أبلغ الناس عن أن متصفح الويب الخاص بهم يفتح من تلقاء نفسه ويعرض رسالة تطالبهم بتنزيل "COVID-19 Inform App" الذي يزعم أنه من منظمة الصحة العالمية (WHO) .

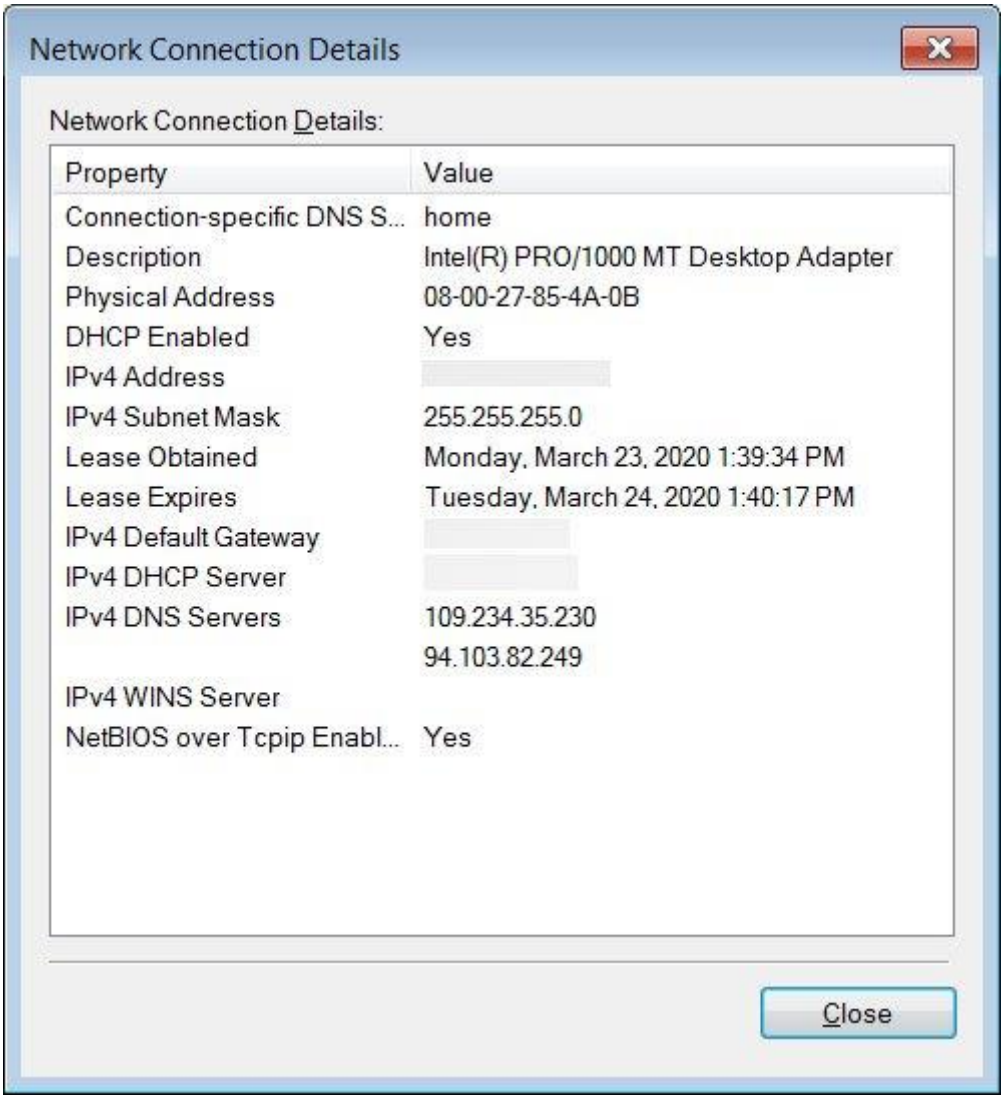
بعد إجراء مزيد من البحث، تم تحديد أن هذه التنبيهات كانت ناتجة عن هجوم أدى إلى تغيير خوادم DNS التي تم تكوينها على أجهزة توجيه D-Link أو Linksys المنزلية الخاصة بهم لاستخدام خوادم DNS التي يديرها المهاجمون.

نظراً لأن معظم أجهزة الكمبيوتر تستخدم عنوان IP ومعلومات DNS التي يوفرها جهاز التوجيه الخاص بها، كانت خوادم DNS الخبيثة تعيد توجيه الضحايا إلى محتوى ضار تحت سيطرة المهاجم.

خطف نقاط سبر ويندوز NCSI النشطة

في الوقت الحالي، من غير المعروف كيف يحصل المهاجمون على حق الوصول إلى أجهزة التوجيه لتغيير تكوين DNS الخاص بهم، ولكن بعض المستخدمين يذكرون أن لديهم وصولاً بعيداً إلى جهاز التوجيه ممكّناً بكلمة مرور مسؤول ضعيفة.

بمجرد وصول المهاجمين إلى جهاز التوجيه، سيقومون بتغيير خوادم DNS المكونة إلى 109.234.35.230 و 94.103.82.249 ، والتي سيتم تكوينها أيضًا على معظم أجهزة الكمبيوتر التي تتصل بجهاز التوجيه.



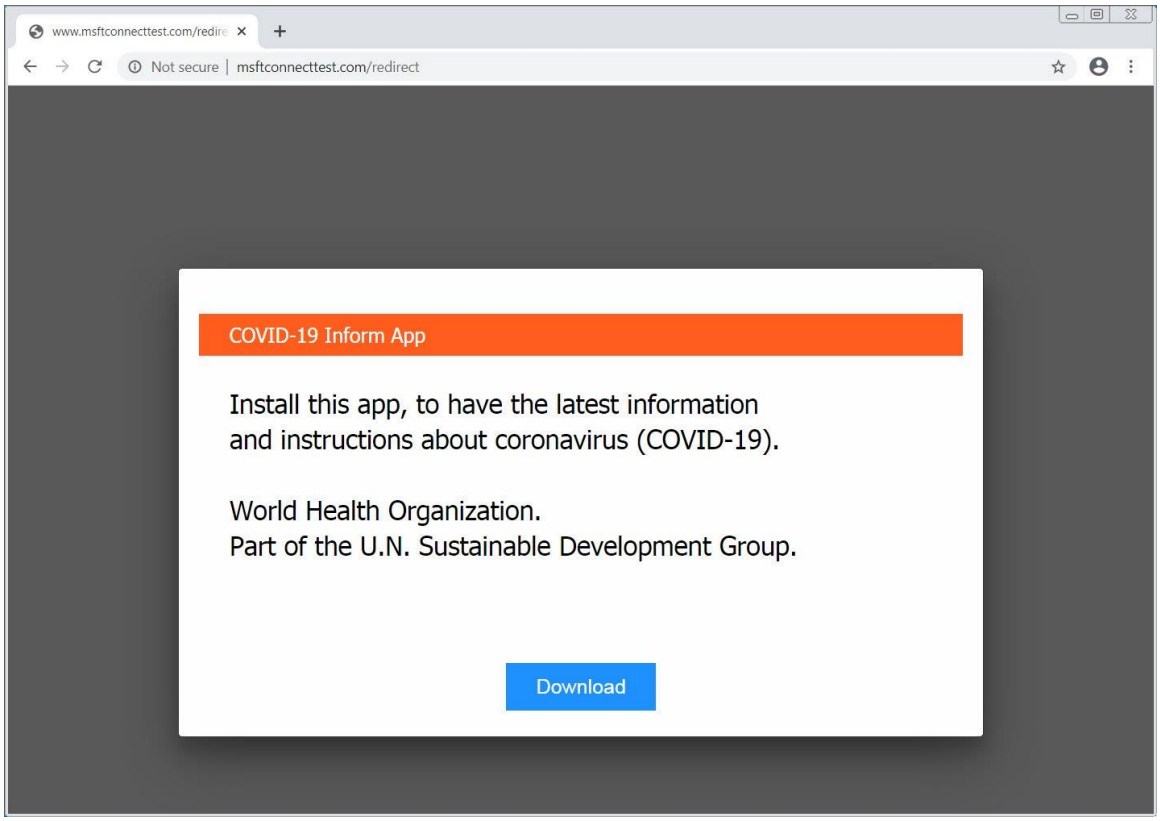
عندما يتصل جهاز حاسوب بشبكة، تستخدم Microsoft ميزة تسمى "مؤشر حالة اتصال الشبكة" Network Connectivity Status Indicator (NCSI) التي يتم استخدامها لتشغيل الاختبارات بشكل دوري للتحقق مما إذا كان جهاز الحاسب متصلاً بالإنترنت بشكل نشط.

في Windows 10، سيكون أحد هذه الاختبارات النشطة الاتصال بموقع http://www.msftconnecttest.com/connecttest.txt والتحقق مما إذا كان المحتوى الذي تم إرجاعه يحتوي على السلسلة "Microsoft Connect Test".

إذا حدث ذلك، فسيكون الحاسب متصلاً بالإنترنت وإذا لم يكن كذلك، يحذر Windows من عدم إمكانية الوصول إلى الإنترنت.

بالنسبة لضحايا هذا الهجوم، عندما يقوم Windows بإجراء تحقيق NCSI النشط هذا، بدلاً من الاتصال بعنوان IP الرسمي لمايكروسوفت 13.107.4.52، ترسلك خوادم DNS الضارة إلى موقع ويب موجود على 176.113.81.159.

نظراً لأن عنوان IP هذا تحت سيطرة المهاجم، فبدلاً من إعادة ملف نصي بسيط، يعرضون صفحة تطالب الضحية بتنزيل وتثبيت "COVID-19 Informator" أو "COVID-19 Inform App" الطارئ من منظمة الصحة العالمية كما هو موضح أدناه.



إذا قام المستخدم بتنزيل التطبيق وتثبيته، فبدلاً من تلقي تطبيق معلومات COVID-19، سيتم تثبيت Oski information-stealing Trojan على جهاز الكمبيوتر الخاص به.

عند تشغيله ، سيحاول هذا البرنامج الضار سرقة المعلومات التالية من كمبيوتر الضحية:

- ملفات تعريف ارتباط المتصفح (browser cookies)
- تاريخ المتصفح (browser history)

- معلومات دفع المتصفح (browser payment information)
- بيانات اعتماد تسجيل الدخول المحفوظة (saved login credentials)
- محافظ العملات المشفرة (crypto currency wallets)
- ملفات نصية (text files)
- معلومات الملء التلقائي لنموذج المتصفح (browser form autofill information)
- قواعد بيانات المصادقة Authy 2FA (Authy 2FA authenticator databases)
- لقطة شاشة لسطح المكتب في وقت الاعتداء، والمزيد.

سيتم بعد ذلك تحميل هذه المعلومات إلى خادم بعيد بحيث يمكن للمهاجمين جمعها واستخدامها لتنفيذ المزيد من الهجمات على حساباتك عبر الإنترنت.

قد يكون هذا لسرقة الأموال من الحسابات المصرفية، أو القيام بسرقة الهوية، أو المزيد من هجمات التصيد الاحتيالي.

ما يجب عليك فعله إذا تأثرت بهذا الهجوم

إذا كان متصفحك يفتح بشكل عشوائي على صفحة تروج لتطبيق معلومات COVID-19، فأنت بحاجة إلى تسجيل الدخول إلى جهاز التوجيه الخاص بك والتأكد من تكوينه لاستقبال خوادم DNS الخاصة به تلقائياً من مزود خدمة الإنترنت ISP.

نظراً لأن لكل جهاز توجيه طريقة مختلفة لتكوين خوادم DNS، فمن غير الممكن إعطاء طريقة محددة حول كيفية القيام بذلك.

بشكل عام، ستحتاج إلى اتباع الخطوات التالية:

1. سجل الدخول إلى جهاز التوجيه الخاص بك
2. ابحث عن إعدادات DNS وتأكد من عدم وجود خوادم، خاصة 109.234.35.230 و 94.103.82.249، تم إعدادها يدوياً. إذا كانت كذلك، فقم بتعيين إعداد خوادم DNS على "تلقائي" أو مزود خدمة الإنترنت المعين.
3. ثم احفظ التكوين الخاص بك.

يجب أن تكون قادرًا الآن على إعادة تشغيل أجهزتك المحمولة ووحدات تحكم الألعاب وأجهزة الحاسب بحيث تستخدم إعدادات DNS الصحيحة من مزود خدمة الإنترنت.

نظراً لأن الأشخاص يبلغون عن اعتقادهم بأن إعداداتهم قد تغيرت بسبب ضعف كلمة المرور وتم تمكين الإدارة متحكمة عن بُعد، فمن المهم تغيير كلمة المرور الخاصة بك إلى شيء أقوى وتعطيل الإدارة عن بُعد من التحكم بجهاز التوجيه.

أخيراً، إذا قمت بتنزيل تطبيق COVID-19 وتثبيته، فيجب عليك إجراء فحص فوري للحاسب بحثاً عن البرامج الخبيثة malware .

بمجرد التأكد من السلامة، يجب عليك تغيير جميع كلمات المرور للمواقع التي يتم حفظ بيانات اعتمادها في المتصفح الخاص بك ويجب عليك تغيير كلمات المرور لأي موقع قمت بزيارته منذ لحظة الاعتداء.

عند إعادة تعيين كلمات المرور الخاصة بك ، تأكد من استخدام كلمة مرور فريدة في كل موقع.