NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

استمرار الهجمات السيبرانية

رسائل تصيد الكترونية من جهات حكومية

EG|CERT
المركز الوطني للإستعداد لطوارئ
الحاسبات والشبكات

المقدمة

تحث وحدة البرمجيات الخبيثة والحماية التابعة لمركز المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) القائمين على الدفاع عن الأمن السيبرانى وتأمينه أتخاذ الاحتياطات والتدابير الأمنية اللازمة للحد من احتمالية حدوث اى اختراق ضار للمؤسسات فلقد أعلن المركز الأوكراني للاتصالات الاستراتيجية وأمن المعلومات الأوكراني أن الهجوم السيبراني العنيف والشامل الذي تعرضت له شبكات المؤسسات والهيئات الحكومية فى أوكرانيا يومي 13 و14 من شهر يناير الماضي لا يزال مستمرًا.

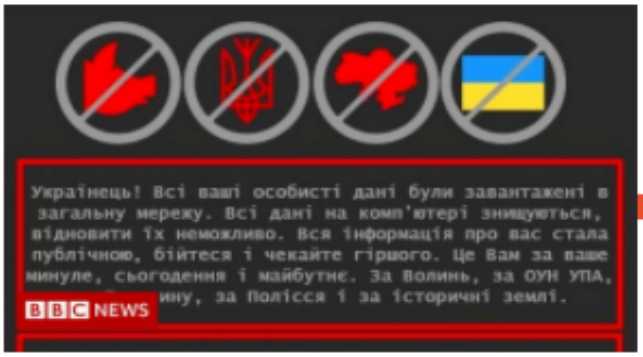
حيث أنه يتم ارسال عدة رسائل الكترونية من عناوين رسمية تتبع السلطة القضائية ، تحتوى تلك الرسائل على روابط ضارة حيث يتم تنزيل البرامج الضارة من خلال تلك الروابط. ويزيد من خطورة الموقف أن البريد يأتي من الخوادم الحقيقية للسلطة القضائية، وبالتالي، تمر الرسائل بمرشحات البريد العشوائي بشكل طبيعى وتوحي بالثقة .

في حالة الضغط على الرابط الضار يتم تنزيل محتويات الملفات المضغوطة وفكها وتشغيلها بهدف التحكم عن بعد والذي سيُمكن المهاجم من الوصول الخفي عن بُعد إلى الجهاز.

تسلسل الهجوم السيبرانى

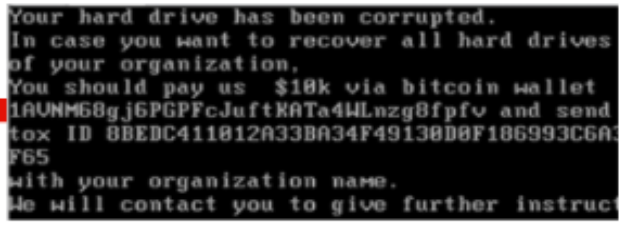
١٣ يناير

تشويه صفحات مواقع حكومية أوكرانية واظهاررسالة تدعو الأوكرانيين إلى "الخوف وتوقع الأسوأ"



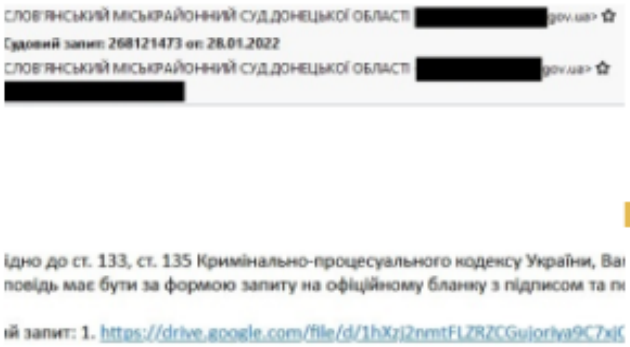
١٦ يناير

اعلنت شركة Microsoft عن استهداف مؤسسات حكومية أوكرانية باستخدام برمجية خبيثة (Whispergate) تهدف الى اظهار رسالة الفدية للمستخدمين ومسح ال Master Boot Record (MBR) بهدف مسح البيانات وتعطيل الأجهزة



٢٨ يناير

استمرار الهجوم السيبرانى على أوكرانيا حيث يتم ارسال رسائل الكترونية من عناوين الكترونية حقيقية للسلطة القضائية تحتوى على روابط ضارة يتم من خلالها تحميل برمجيات خبيثة بهدف تثبيت برنامج Remote Utilities سليم يُمكن المهاجم من الوصول الخفي عن بُعد إلى الجهاز



معلومات تقنية

كان فريق الاستجابة لطوارئ الحاسب الأوكرانى CERT-UA قد ذكر أن رسائل تم إرسالها بشكلٍ جماعي عبر البريد الإلكتروني من عناوين صحيحة تتبع السلطة القضائية و تحتوي تلك الرسائل على روابط يتم من خلالها تحميل ملفات مضغوطة محمية بكلمات مرور "إعلان المحكمة 9978364774635676778282.rar_pass_123.zip" المنشور على الخدمات العامة Google Drive و DropMeFiles.

في حالة تنزيل محتويات حزم الملفات المضغوطة وفكها وتشغيلها سيتم تثبيت برنامج Remote Utilities أصلي وسليم على جهاز كمبيوتر الضحية والذي سيُمكن المهاجم من الوصول الخفي عن بُعد إلى الجهاز؛ ثم يتم تحقيق استمرارية إضرار البرنامج بالجهاز وقدرته استئناف نشاطه الخبيث بعد إعادة تشغيل الجهاز) من خلال إنشاء خدمة RManService.

يتم تنفيذ مثل هذه الهجمات الإلكترونية كنشاط مُنظم يُشن على المؤسسات والهيئات الحكومية في أوكرانيا وقد تمتد لمؤسسات وجهات أخرى؛ وكان فريق (CERT-UA) قد تمكن من تعقبها ومنحها المعرف UAC-0096.

From СЛОВ'ЯНСЬКИЙ МІСЬКРАЙОННИЙ СУД ДОНЕЦЬКОЇ ОБЛАСТІ [redacted]gov.ua>
Subject **Судовий запит: 268121473 от: 28.01.2022**
Reply to СЛОВ'ЯНСЬКИЙ МІСЬКРАЙОННИЙ СУД ДОНЕЦЬКОЇ ОБЛАСТІ [redacted]gov.ua>
To [redacted]

Reply | Reply List | Forward | More
07:32

УКРАЇНА
СЛОВ'ЯНСЬКИЙ МІСЬКРАЙОННИЙ СУД ДОНЕЦЬКОЇ ОБЛАСТІ

Відповідно до ст. 133, ст. 135 Кримінально-процесуального кодексу України, Вам не обходимо надати фінансово господарську документацію зазначену в судовому запиті, у разі не надання документації ви будите піддані приводу до СУДУ. Звертаємо Вашу увагу що відповідь має бути за формою запиту на офіційному бланку з підписом та печаткою.

Судовий запит: 1. https://drive.google.com/file/d/1hXzj2nmtFLZRZCGujoriya9C7xjQ51V0/view?usp=sharing

2. https://dropmefiles.com/nIVc4

З метою інформаційної безпеки встановлено код доступу: 2022

З повагою,
Суддя,
СЛОВ'ЯНСЬКИЙ МІСЬКРАЙОННИЙ СУДУ
В.І. Старовецький

التوصيات

- يجب فحص الأجهزة باستخدام دلالات الإصابة المذكورة للتأكد من عدم إصابتها .
- يجب مراجعة وفحص سجلات الدخول على الأنظمة وخاصة الحسابات التي تعتمد على أنظمة
- يجب الأعتماد على المصادقة متعددة العوامل وخاصة فى حالة الاتصال عن بعد.
- اتخاذ التدابير الأمنية اللازمة لحماية الخوادم الحكومية لتقليل احتمالية استغلالها فى تنفيذ أي هجوم سيبراني.

إن وحدة تحليل البرمجيات الخبيثة والحماية بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) على أتم الاستعداد لمساعدة المؤسسات والجهات الحكومية المصرية في حمايتها من أي تهديدات سيبرانية ومعاونتها في تعزيز نظام الأمن السيبراني من خلال خبراءها المكلفين بذلك وبواسطة الخدمات التي تقدمها. وفي حالة تعرض أي مؤسسة لأي هجوم سيبراني، يمكننا تقديم المساعدات اللازمة لها واستخدام المعلومات الخاصة بالحادث ومؤشرات الاختراق (indicators of compromise) والبصمات التعريفية للبرمجيات الخبيثة لحماية المؤسسات الأخرى حتى لا تقع ضحية لمثل هذه الحوادث في المستقبل.

دلالات الاصابة

Files:

dcd23078da37d0054cc75fb45e9d095 Судовий запит №997836477463567677828 2.rar_pass_123.zip
b0e4a2cd59c4620b794ecda351c736a2 Судовий запит №997836477463567677828 2.rar
a02df1ad79381a269843c831fb8a48b0 Судовий запит №9978364774635676782828.pdf.rar
f360827a30f1267a3170ad6f7c160730 Судовий запит №9978364774635676782828.pdf.exe

Domains:

101.99.93[.]49
rmssrv2[.]ru
rmssrv3[.]ru
rmssrv4[.]ru

Registries:

HKLM\SYSTEM\ControlSet001\services\RManService
HKLM\SOFTWARE\Usoris\Remote Utilities Host\
%PROGRAMFILES(X86)%\Remote Utilities - Host\

Malware Removal:

stop the RManService service,

delete the directory% PROGRAMFILES (X86)% \ Remote Utilities - Host \,

delete the registry key HKLM \ SOFTWARE \ Usoris.

المصادر

- https://cert.gov.ua/article/18163
- https://arabic.rt.com/world/1319436-%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D9%87%D8%AC%D9%88%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D9%85%D8%B3%D8%AA%D9%85%D8%B1/
- HTTPS://WWW.CSHUB.COM/ATTACKS/NEWS/UKRAINE-CONTINUES-TO-CONTEND-WITH-CYBER-ATTACKS
- https://www.bloomberg.com/news/articles/2022-01-28/recent-hacks-in-ukraine-meant-to-spread-chaos-minister-says
- https://www.cnet.com/tech/services-and-software/ukrainian-government-networks-infected-with-malware-microsoft-warns/