أهم البرمجيات الضارة التي يجب عليك إزالتها فورًا

الجمعة 20 نوفمبر 2020 10:11 م

لقد ولت الأيام التي كانت تعمل فيها مجموعات البرمجيات الضارة وبرامج الفدية من خلال إطلاق حملات للبريد الإلكتروني العشوائي على أمل إصابة المستخدمين العشوائيين عبر الإنترنت.

واليوم، تطوّر مشغلو برامج الفدية من مجموعة من عصابات البرمجيات الخبيثة إلى سلسلة من عصابات الجرائم الإلكترونية المعقدة بمهارات وأدوات وميزانيات مجموعات القرصنة المدعومة حكوميًا.

وفي الوقت الحاضر، تعتمد عصابات برامج الفدية على شراكات متعددة المستويات مع عمليات جرائم الإنترنت الأخرى. وتعمل هذه المجموعات، التي يطلق عليها (سماسرة الوصول الأولي)، كسلسلة إمداد للجريمة السرية، وتوفر لعصابات برامج الفدية وغيرها إمكانية الوصول إلى مجموعات كبيرة من الأنظمة المخترقة.

وتتكون هذه الأنظمة المخترقة نقاط النهاية لـ (بروتوكول سطح المكتب البعيد) Remote Desktop Protocol، وأجهزة الشبكات ذات الأبواب الخلفية، وأجهزة الحاسوب المصابة بالبرمجيات الضارة، وهي تسمح لعصابات برامج الفدية بالوصول بسهولة إلى شبكات الشركات، وتصعيد وصولها، وتشفير الملفات للمطالبة بفدية ضخمة.

ويعد (سماسرة الوصول الأولي) جزءًا مهمًا من مشهد الجريمة الإلكترونية. واليوم، تبرز ثلاثة أنواع من السماسرة كمصادر لمعظم هجمات الفدية، وهم: بائعو نقاط النهاية المخترقة لـ (بروتوكول سطح المكتب البعيد)، وبائعو أجهزة الشبكات المخترقة، وبائعو أجهزة الحاسوب المصابة سابقًا ببرمجيات ضارة.

وغالبًا ما تكون الحماية من هذه الأنواع الثلاثة من اتجاهات الوصول الأولي هي أسهل طريقة لتجنب برامج الفدية الضارة. وفي حين أن الحماية من الأمرين الأوليين تتضمن عادةً ممارسة سياسات جيدة لكلمات المرور، والحفاظ على المعدات مُحدَّثة، فإنه يصعب الحماية من المتجه الثالث منه. وهذا لأن مشغلي الروبوتات الخبيثة يعتمدون غالبًا على الهندسة الاجتماعية لخداع المستخدمين لتثبيت برمجيات ضارة على أنظمتهم بأنفسهم، حتى لو كانت أجهزة الحاسوب تستخدم برامج حديثة.

ونشر موقع ZDNet قائمة بسلالات البرمجيات الضارة المعروفة التي استُخدمت على مدار العامين الماضيين لتثبيت برامج الفدية الضارة. وتعاون الموقع مع باحثين أمنيين من شركات، مثل: Advanced Intelligence، و Binary Defence، و Sophos.

وتشمل قائمة البرامج الخبيثة كلًا من: Emotet، و Trickbot، و BazarLoader، و QakBot، و SDBBot، و Dridex، و Buer، و Per Sophos، و Phorpiex، و CobaltStrike.

وينصح موقع ZDNet مسؤولي النظام في الشركات؛ بمجرد اكتشاف أي من سلالات البرمجيات الضارة هذه، بالتفرغ للتصدي لها، وإيقاف تشغيل الأنظمة، وتدقيق البرامج الخبيثة، وإزالتها كأولوية قصوى.