كاسبرسكي لاب: منصات "Botnets" الخبيثة تعود مجدداً

الخميس 14 سبتمبر 2017 08:09 م

اكتشف فريق أبحاث مكافحة البرمجيات الخبيثة في كاسبرسكي لاب اثنتين من شبكات "botnets" مثبت عليهما أجهزة كمبيوتر مصابة ببرمجيات خبيثة تقوم خلسة بتثبيت أدوات إنتاج العملة المشفرة، والتي هي عبارة عن برنامج نظامية تستخدم لإنتاج عملات افتراضية قائمة على تكنولوجيا "Blockchain".

وتمكن الباحثون في إحدى الحالات من التوصل إلى تقديرات خلصت إلى أن ما يقارب 4,000 من تلك الأدوات المثبتة على الشبكة بمقدورها أن تدر على أصحابها دخلاً يصل حتى 30 ألف دولار أمريكي شهرياً، وفي حالة أخرى توصل الباحثون بأن مجرمي الإنترنت يحققون أموالاً طائلة بأكثر من 200 ألف دولار أمريكي ناتجة عن 5,000 جهاز حاسب مصاب مثبت على شبكات "botnet".

وتشير طبيعة تكوين بنية العملة الرقمية "Bitcoin" وغيرها من العملات المشفرة إلى أنه بالإضافة إلى قيام المستخدم بشراء العملة الرقمية، فإن بإمكانه أيضاً إنشاء وحدة عملة جديدة (أو القطع نقدية) من خلال الاستفادة من القدرة الحوسبية للأجهزة المثبت عليها برامج متخصصة في "إنتاج" العملات.

وفي الوقت ذاته، وفقاً لمفهوم العملات المشفرة، فإنه كلما يتم إنتاج المزيد من القطع النقدية، كلما يتطلب الأمر مزيداً من الوقت والقدرة الحاسوبية لإنشاء عملة جديدة، فقبل عدة سنوات، كانت البرمجيات الخبيثة تقوم خلسة بتثبيت أدوات إنتاج العملة الرقمية "Bitcoin"، والتي تستخدم أجهزة كمبيوتر الضحية لإنتاج العملات المستخدمة لمجرمي الإنترنت.

وكانت هذه ظاهرة شائعة في مشهد التهديدات الإلكترونية، إلا أن العدد المتزايد للعملات الرقمية "Bitcoin" التي كان يتم إنتاجها، جعل إمكانية إصدار عملات جديدة أمراً أكثر صعوبة، بل أن هذه العملية كانت في بعض الأحيان عديمة الجدوى، فالمكاسب المالية المحتملة التي يمكن أن يحصل عليها المجرم نظير جهوده المبذولة لإنتاج العملة الرقمية "Bitcoin" لا تغطي الاستثمار الذي يحتاجه لإنشاء ونشر البرمجية الخبيثة أو نفقات دعم البنية التحتية المطلوب.

ومع ذلك، فإن سعر العملة الرقمية "Bitcoin"، أول عملة مشفرة وأكثرها شهرة، قد ارتفع في السنوات الأخيرة من عدة مئات إلى آلاف الدولارات لكل عملة رقمية، الأمر الذي تسبب في إحداث ظاهرة "حمى العملة المشفرة" حول العالم. وفي أعقاب ذلك، سارعت المئات من المجموعات والشركات الناشئة المتحمسة إلى طرح بدائل عن العملة الرقمية الخاصة بها، والتي اكتسب الكثير منها أيضا قيمة سوقية كبيرة خلال فترة زمنية قصيرة نسبياً.

وقد جذبت التغييرات في أسواق العملات المشفرة في نهاية المطاف انتباه مجرمي الإنترنت الذين ينتهزون مثل هذة الفرص للإحتيال، حيث يقومون بتثبيت برنامج إنتاج العملات المشفرة خلسة على الآلاف من أجهزة الكمبيوتر.

واستنادا إلى نتائج دراسة أجراها خبراء كاسبرسكي لاب مؤخراً، يقوم المجرمون الذين يقفون وراء شبكات "botnets" المكتشفة حديثا بدس ونشر برامج إنتاج العملات الرقمية بمساعدة برامج عرض الإعلانات "adware" التي يقوم الضحايا بتثبيتها طوعاً.

وبعد تثبيت برنامج عرض الإعلانات "adware" على جهاز حاسوب الضحايا، يقوم بتنزيل مكون خبيث وهو أداة تثبيت برنامج إنتاج العملة الرقمية، حيث يعمل هذا الأخير على تثبيت برنامج إنتاج العملة ويقوم أيضاً بتنفيذ بعض الإجراءات للتأكد من فاعلية أداء أداة تثبيت برنامج إنتاج العملة وإمكانية استمرارها لأطول فترة ممكنة.

وتشمل هذه الأنشطة ما يلي:

• محاولة تعطيل برنامج الحماية الأمنية.

• تتبع جميع التطبيقات النشطة وتعليق أنشطتها في حال بدء تشغيل برامج مراقبة أنشطة النظام أو سلامة سير العمليات.

• التأكد من وجود نسخة احتياطية من برنامج إنتاج العملة الرقمية بشكل دائم على محرك الأقراص واسترجاعها في حال إزالتها.

وبعد أن يتم إنتاج القطع النقدية الأولى، يتم نقلها إلى محافظ تابعة للمجرمين الغير مكترثين لما سيعانيه الضحايا من أضرار تتمثل في بطء أداء أجهزة الكمبيوتر الخاصة بهم على نحو غير مألوف وارتفاع تكاليف فواتير الكهرباء.

واستنادا إلى ملاحظات كاسيرسكي لاب، يميل المجرمون إلى إنتاج اثنتين من العملات المشفرة وهي: "Zcash" و"Monero"، ومن المحتمل أن يتم اختيار هذه العملات الخاصة لأنها توفر وسيلة موثوقة لأساليب إخفاء مصدر المعاملات وهوية أصحاب المحفظة.

وقد رصدت كاسبرسكي لاب أول مؤشرات تدل على عودة البرمجيات الخبيثة المختصة في إنتاج العملات الرقمية مطلع شهر ديسمبر 2016، عندما أبلغ أحد الباحثين في الشركة بأن ما لا يقل عن 1,000 جهاز كمبيوتر مصاب ببرمجية خبيثة عرفت آنذاك بإسم "Zcash"، وهي عملة رقمية تم طرحها بنهاية أكتوبر 2016.

وفي ذلك الوقت، ونتيجة لسعر "Zcash" الذي كان ينمو بشكل متسارع، تمكنت شبكة "botnet" من أن تحقق لأصحابها دخلاً أسبوعياً يصل حتى 6,000 دولار أمريكي، وفيما بعد، صدرت تنبؤات باحتمال ظهور منصات إنتاج عملات رقمية جديدة، والتي أكدت نتائج البحوث الأخيرة صحتها.

وقال يفجيني لوباتين محلل برمجيات خبيثة في كاسبرسكي لاب "تكمن المشكلة الرئيسية بالنسبة لبرمجيات إنتاج العملات الرقمية في في صعوبة اتباع وسائل موثوقة للكشف عن أنشطتها، وذلك لأن برامج إنتاج العملات الرقمية المستخدمة من قبل هذه البرمجيات الخبيثة نظامية كلياً، بحيث أنه من الممكن في الأحوال العادية تثبيتها من قبل أي مستخدم اعتيادي".

وأضاف لوباتين "ثمة شيء آخر مثير للقلق لاحظناه أثناء مراقبة شبكتي "botnets" المذكورتين، وهو أن برمجيات إنتاج العملات الرقمية ذاتها تكتسب قيمة متزايدة في السوق السوداء، لقد رأينا هناك مجرمين يطرحون للبيع ما يعرف باسم "Miner Builders"، وهو برنامج يتيح لأي شخص، على استعداد لدفع قيمة هذا الإصدار الكامل، إنشاء منصة لإنتاج العملات "botnet" خاصة به، وهذا يعني أن شبكات "botnets" التي اكتشفناها مؤخرا هي بالتأكيد ليست الأخيرة".

وارتفع عدد المستخدمين الذين تعرضوا لهجمات منتجي العملات الرقمية المشفرة بشكل كبير في السنوات الأخيرة، وعلى سبيل المثال فقد تمكنت منتجات كاسبرسكي لاب في عام 2013 من توفير الحماية لنحو 205,000 من المستخدمين على مستوى العالم عندما تم استهدافهم بهذا النوع من التهديدات، وفي عام 2014 ارتفع العدد إلى 701,000، ووصل عدد المستخدمين الذين تمت مهاجمتهم في الأشهر الثمانية الأولى من عام 2017 إلى 1.65 مليون.

ولحماية أجهزة الكمبيوتر الخاصة بكم من استهلاك قدر أكبر من الطاقة التي تعود بمنافع كبيرة على مجرمي الإنترنت، يوصي باحثو كاسبرسكي لاب باتباع الإجراءات التالية:

- الامتناع عن تثبيت برامج مشبوهة من مصادر غير موثوق بها على جهاز الكمبيوتر الخاص بكم.
- قد يتم تعطيل خاصية الكشف عن برنامج عرض الإعلانات "adware" بشكل افتراضي في الحل الأمني المثبت لديكم، لذا تأكدوا من تفعيلها باستمرار.
- استخدموا حل "Internet Security" المثبت حتى تتمكنوا من حماية بيئتكم الرقمية من جميع التهديدات المحتملة بما في ذلك البرمجيات الخبيثة لإنتاج العملات الرقمية.
- في حال كنتم تقومون بتشغيل سيرفر، تأكدوا من أنه محاط بالحماية الكافية عن طريق اختيار الحل الامني المناسب، إذ إن السيرفرات تشكل أهدافاً مربحة للمجرمين بفضل أدائها الحوسبي المتميز بالمقارنة مع أجهزة الكمبيوتر متوسطة الأداء.

وقد تمكنت منتجات كاسبرسكي لاب من أن تكتشف وتمنع بنجاح البرمجية الخبيثة المسؤولة عن نشر برنامج إنتاج العملات الرقمية باستخدام الأداتين التاليتين:

- RiskTool.Win32.BitCoinMiner.hxao
- PDM:Trojan.Win32.Generic