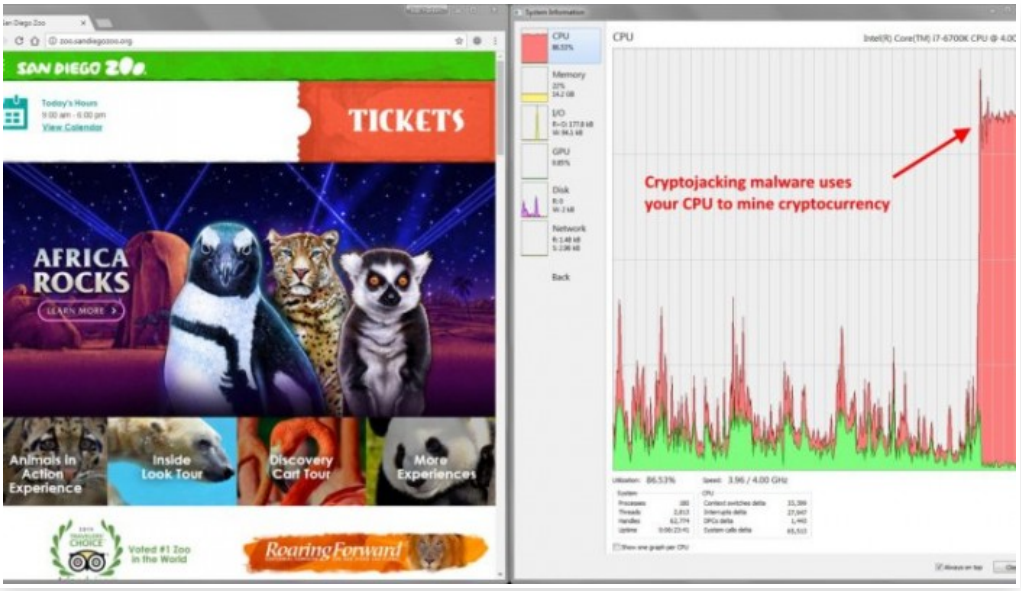
ما يقرب من 400 موقع دروبال مصابة ببرامج خبيثة لتعدين العملات الرقمية



الثلاثاء 8 مايو 2018 08:05 م

يبدو أن برمجيات التعدين الخبيثة لن تتوقف عن العمل حيث تم توظيفها على نحو متزايد بداية من العام الماضي 2017، وذلك بسبب الارتفاع الشديد في أسعار العملات الرقمية، حيث يقوم القراصنة بسرقة قوة الحوسبة للمستخدمين من أجل إخفاء عمليات توليد للعملات الرقمية.

وقد اكتشف الباحث الأمني تروي مورش بموقع Bad Packets Report أن عددًا من مواقع الويب والتي تستخدم إصدارًا قديمًا من نظام إدارة المحتوى دروبال Drupal يتعرضون للاعتداء من قِبل القراصنة للقيام بعمليات التعدين الخفية.
في حين أن الأهداف الرئيسية لهذا الهجوم – الذي أصاب نحو 400 موقع – هي كيانات حكومية ومؤسسات تعليمية مقرها الولايات المتحدة، والعديد من مواقع شركات التكنولوجيا أصيبت أيضًا بهذه البرامج الخبيثة.

حيث تشمل قائمة المواقع المتأثرة التي قام بتجميعها الباحث الأمني تروي مورش: المجلس القومي الأمريكي لعلاقات العمل (NLRB)، وشركة التكنولوجيا الصينية لينوفو، والشركة التايوانية دي – لينك D-Link المتخصصة في صناعة معدات الشبكات والاتصالات، وجامعة كاليفورنيا بلوس أنجلوس (UCLA)، كما تأثرت المواقع الإلكترونية الحكومية في كل من الولايات المتحدة والمكسيك وتركيا وبيرو وجنوب أفريقيا وإيطاليا. في حين أنه لا توجد علاقة بين هذه المواقع، إلا أنهم يشتركون في قاسم مشترك – وهو استخدام إصدار قديم من نظام إدارة المحتوى دروبال.

وقد اكتشف مورش أن جميع رموز جافا سكريبت المصابة تشير إلى نفس اسم النطاق وهو (vuuwd.com) ونفس أداة التعدين وهي Coinhive المستخدمة في تعدين عملة مونيرو، مما يعني أن فردًا أو كيانًا واحدًا كان وراء كل هذه الهجمات.

وقد توصل بحث مورش السابق إلى أن هناك حملات تعدين بإستخدام برمجيات خبيثة قد أصابت ما يقرب من 50 ألف موقع على شبكة الإنترنت، وكثير منها يتم دون معرفة القائمين على إدارة هذه المواقع.

والحقيقة المثيرة للاهتمام حول كل هذه الهجمات هي خدمة التعدين التي اختارها القراصنة – حيث هناك تفضيل واضح لأداة التعدين Coinhive، والتي أصبحت مسؤولة عن أكثر من 80 في المئة من جميع المواقع المصابة.

ويعتبر موقع Coinhive من أكثر متصفحات التعدين شهرةً وشعبيةً، فهو يقدم لأصحاب الموقع أجزاءً من نصوص الجافا سكريبت الخاصة بأجهزة مستخدمي الموقع من أجل تعدين العملة الرقمية.

يذكر أن موقع Coinhive قد حصل على بعض الشرعية بعد طرحه لميزة تتطلب موافقة المستخدم قبل استخدام الكمبيوتر الخاص به في التعدين. وبعد دمج هذه الميزة مع Coinhive استعانت بها منظمة الأمم المتحدة للطفولة "اليونيسف" لتمويل أعمالها الخيرية للأطفال في بنغلاديش.

ومع ذلك فقد اكتشف الباحثون أن الإصدار الذي يحتوي على خيار طلب موافقة المستخدم عادةً لا يكون شائعًا في الاستخدام مع مواقع الويب، وأنهم يختاروا دمج Coinhive مع موقعهم على الويب بطريقة لا تخبر المستخدمين، وذلك لتحقيق إيرادات بديلة لإيرادات الإعلانات.

ووفقاً لأحدث التقارير فإن CoinHive مسؤول عن أكثر من 80 في المئة من جميع المواقع المصابة.

لذلك فقد حان الوقت لأن يتوقف موقع Coinhive عن تقديم خدماته التي تسمح بالتعدين دون معرفة المستخدم، ويحتفظ فقط بالإصدارالذي يحتوي على خيار طلب موافقة المستخدم "Opt-in" والذي يخبر المستخدم ويطلب موافقته أولا

لا توجد طريقة للمستخدمين لمعرفة ما إذا كان يتم استخدام جهاز الكمبيوتر الخاص به لتعدين العملات الرقمية من خلال Coinhive ما لم يلاحظوا بطء أجهزتهم بسبب الضغط الشديد على وحدة المعالجة المركزية دون سبب واضح، وينبغي على المستخدمين في الوقت الحالي الاستعانة بالإضافات الخاصة بالمتصفحات التي تساعد على منع البرمجيات الخبيثة malwareg adware من العمل مثل AdBlock Plus أو Adguard، للمساعدة في حجب البرمجيات النصية الخاصة بعمليات التعدين