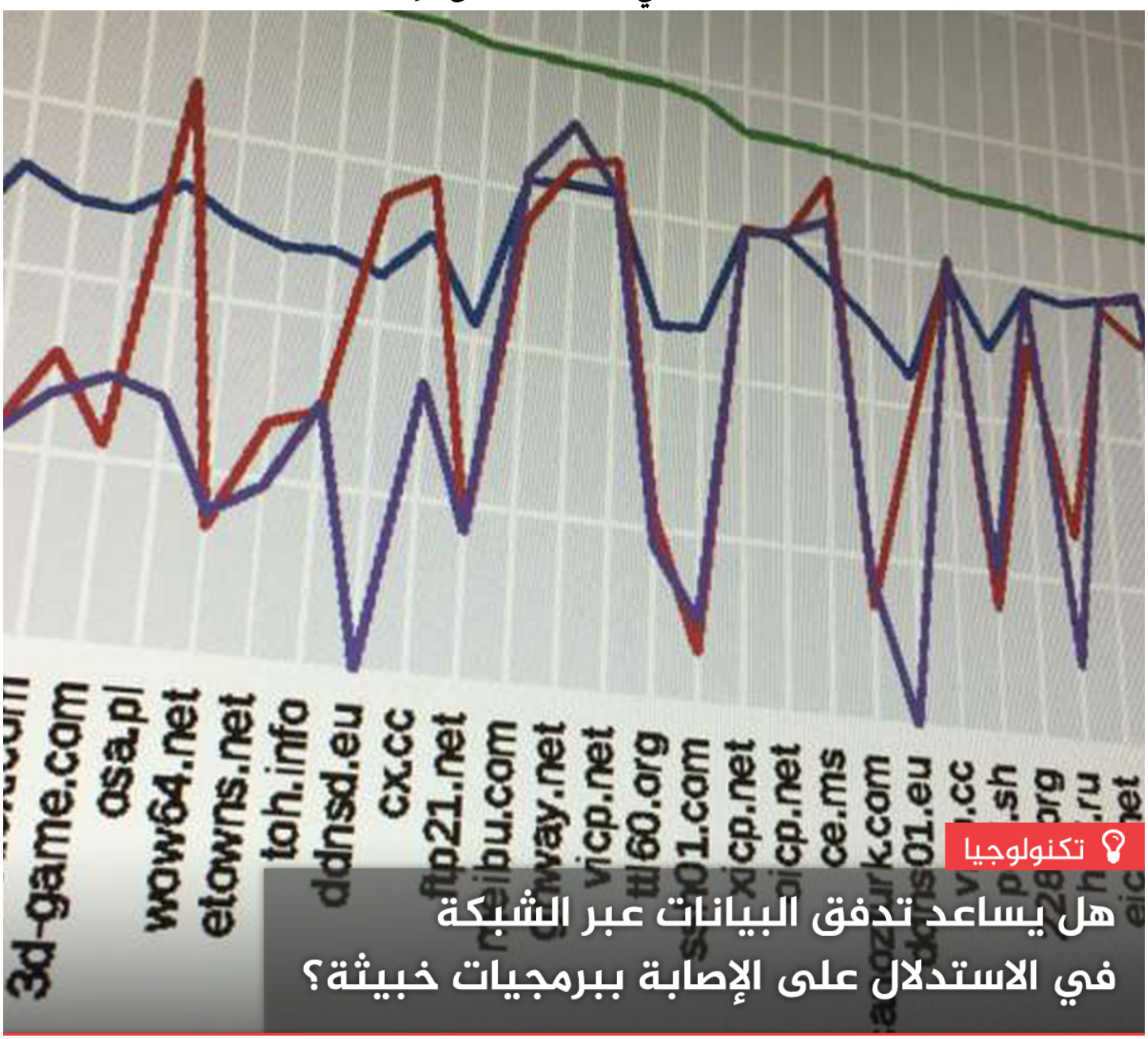
هل يساعد تدفق البيانات عبر الشبكة في الاستدلال على الإصابة ببرمجيات خبيثة؟



قائمة بأكثر النطاقات التي استعلَمَت عنها عيناتُ البرمجيات الخبيثة، ودرسها باحثو أمن الانترنت في معهد جورجيا التقني.

حقوق الصورة: Georgia Tech

ذكرت دراسة حديثة أن باستطاعة مسؤولي أمن الأنظمة اكتشافُ إصابة الشبكة بالبرمجيات الخبيثة خلال فترة كافية (أسابيع أو أشهر حتى)، قبل أن يصبح بمقدورهم التقاط عينة من هجوم البرمجيات الخبيثة، وذلك عن طريق فحص وتحليل تدفق البيانات إلى نطاقات مشبوهة خلال الشبكة. وقد أفضت نتائج الدراسة إلى الحاجة لإيجاد استراتيجيات مستقلة للكشف عن هذه البرمجيات الخبيثة الجديدة، حيث تساعد هذه الاستراتيجياتُ أنظمةَ حماية الشبكات في اكتشاف الخروقات الأمنية للشبكة في الوقت المناسب.

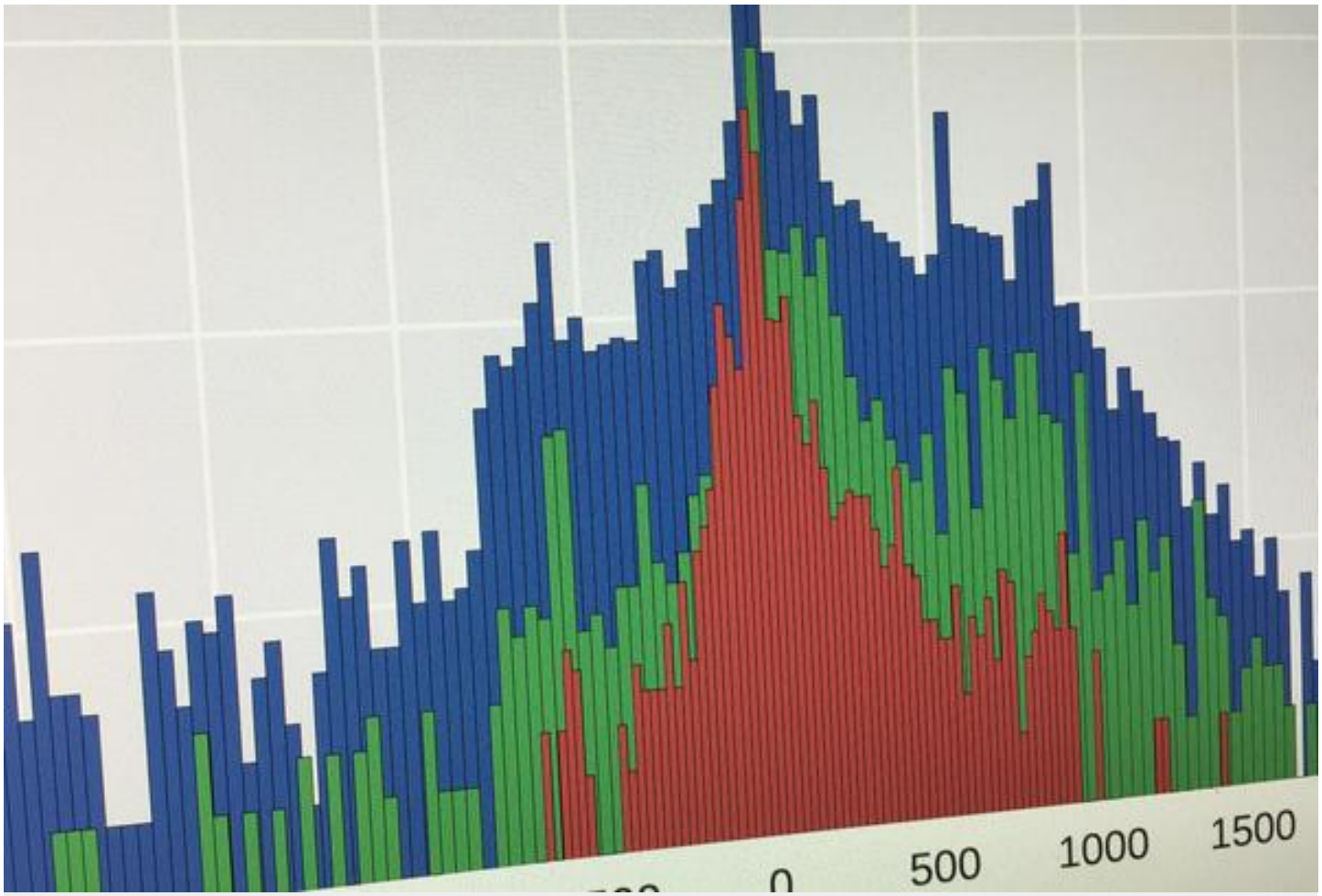
ويُستفاد في هذه الاستراتيجية من حاجة البرمجياتِ الخبيثة للاتصال بالأجهزة المتحكِّمة بها والتي تعطيها الأوامر ببدء الهجوم، مما يؤدي إلى حدوث تدفق للبيانات عبر الشبكة، الأمر الذي يمكن تحليله والتنبؤ بحدوثه. وذكر الباحثون في الدراسة أيضاً أنه كلما كانت التحذيرات بحدوث الهجمات في وقت مبكر، كلما زادت فرصة الاستجابة ومواجهة الهجمات وتقليل خطرها.

ويقول مانوس أنتوناكاكيس **Manos Antonakakis** وهو أستاذ مساعد في كلية الهندسة الكهربائية وهندسة الحاسوب في معهد جورجيا للتقنية **Georgia institute of Technology**: "أظهرت الدراسة أنه وفي اللحظة التي تُكتشف فيها هذه البرمجيات الخبيثة في الشبكة يكون الأوان قد فات، لأنه وعند اكتشافها، تكون قد انتشرت ونشطت في استخدام نطاقات الشبكة واتصالاتها منذ أسابيع أو أشهر على الأقل". ويتابع: "هذه النتائج تعني أننا بحاجة إلى تغيير مفاهيمنا الأساسية حول حماية الشبكات وأمنها."

تعتمد الطرق التقليدية في حماية الشبكات على اكتشاف البرمجيات الخبيثة في الشبكة، وبينما نستطيع من خلال عملية تحليل عينات البرمجيات الخبيثة التعرف على النطاقات المشبوهة وربط هذه الهجمات بمصادرها، يعطي الاعتمادُ على هذه العينات ـ لاتخاذ إجراءات حماية الشبكة ـ البرمجياتِ المشبوهة بالمقابل فرصةً لجمع المعلومات والتسبب بالأضرار. ويضيف أنتوناكاكيس: "ما نحتاجه فعلاً هو تقليل الزمن بين اكتشاف المشكلة والعثور على حلول مناسبة لها."

دُعم هذا البحث ـ والذي عُرض في الرابع والعشرين من أيار/مايو لعام 2017 في الندوة الثامنة والثلاثين لمنظمة **IEEE** الخاصة بالأمن والخصوصية في مدينة سان خوسيه **San Jose** في كاليفورنيا ـ من قبل وزارة التجارة الأمريكية **U.S. Department of Commerce**، ومؤسسة العلوم الوطنية **National Science Foundation**، ومختبر أبحاث السلاح الجوي **Air Force Research Laboratory**، ووكالة مشاريع الأبحاث المتطورة الدفاعية **Defense Advanced Research Projects Agency**. وقد جرى هذا البحث بالتعاون بين جامعة يوريكوم **EURECOM** في فرنسا ومعهد البرمجيات آي إم دي إي إيه **IMDEA** في إسبانيا والذي دُعم كذلك من الحكومة الإسبانية.

أجرى أنتوناكاكيس ومساعد بحوث الدراسات العليا تشاز ليفر **Chaz Lever** وزملاؤهما في هذه الدراسة تحليلاً لأكثر من خمسة مليارات حالة لحركة البيانات على الشبكة من المزود الرئيس للانترنت (**ISP**) في الولايات المتحدة على مدى خمس سنوات. كذلك درسوا حوالي 27 مليون طلب من عينات البرمجيات الخبيثة على خوادم نظام أسماء النطاقات **domain name server** والذي يُطلق عليه اختصاراً **DNS** (خوادم **DNS** تحول العنوان الحرفي إلى عنوان رقمي**IP** لتسهيل الوصول إليه)، وفحصوا الوقت الذي يحدث فيه إعادة تسجيل النطاقات المنتهية والتي تقدم مواقع لإطلاق هجمات البرمجيات الخبيثة من خلالها.



رسم بياني يوضح فارق الزمن بين اكتشاف إشارات البرمجيات الخبيثة في حركة المرور على الشبكة لمزود الانترنت الرئيسي وبين تسجيلها في القوائم السوداء. حقوق الصورة: Georgia Tech

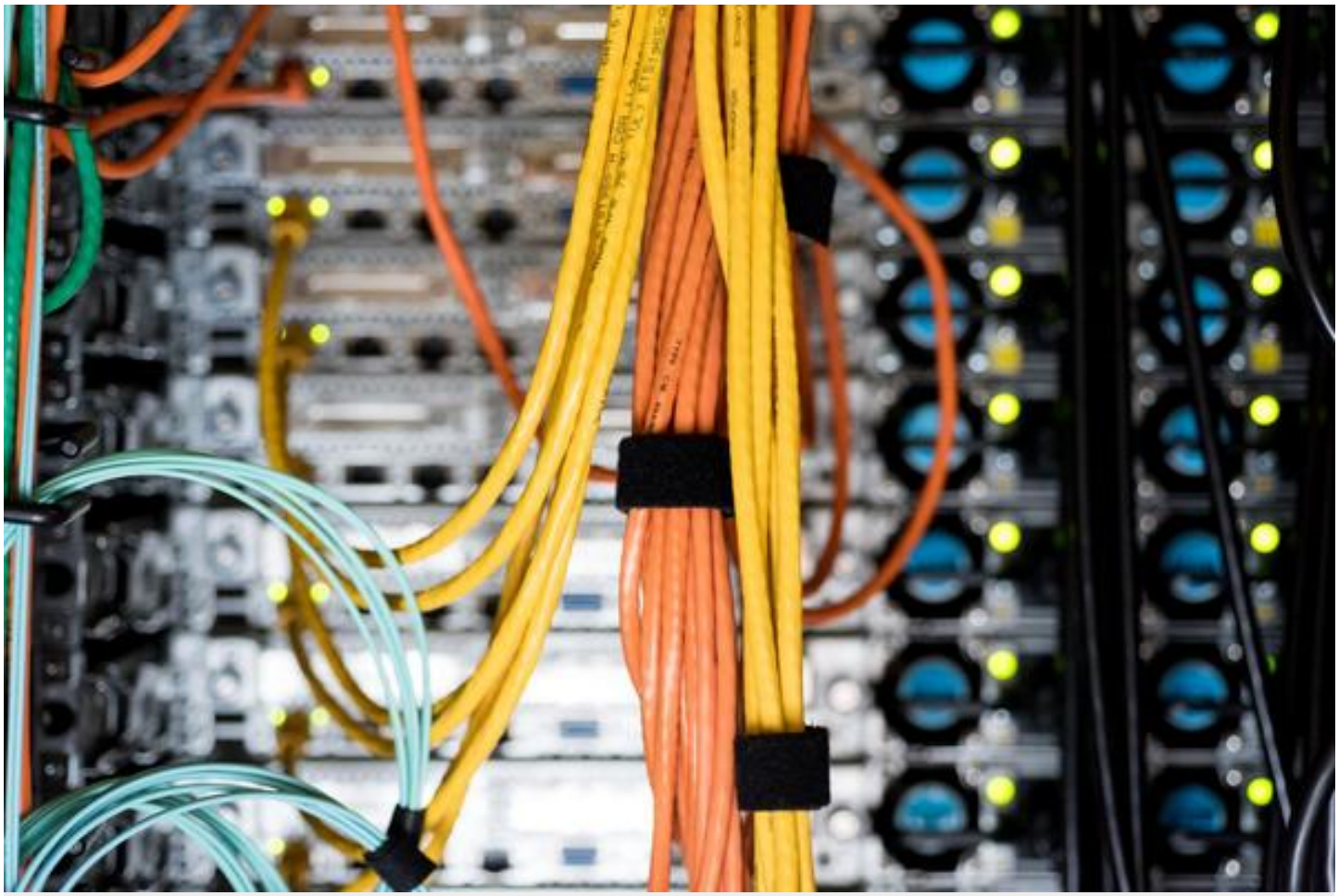
يقول تشاز ليفر، المؤلف الأول للدراسة وطالب في قسم الهندسة الكهربائية وهندسة الحاسوب في معهد جورجيا للتقنية: "من الممكن أن يعطي التركيزُ على حركة البيانات في بعض الشبكات –والتي تكون معرضةً أكثر من غيرها لسوء الاستخدام– إشارةً جيدةً توحي بقرب حدوث عبث ما وسوء استخدام في الشبكات. وإذا ما لوحظ وجودُ كثرةٍ في الطلبات على خادم **DNS** –والتي تشير إلى النقاط الفعّالة لسوء الاستخدام في منطقة معينة– فلا بد من الاهتمام بهذا الأمر الدال على وجود هجمات خبيثة محتملة."

ووجد الباحثون أيضاً أن الطلبات على خوادم **DNS** الديناميكية ترتبط كذلك بأنشطة سيئة وغير مرغوبة، لأنها غالباً ما ترتبط بخدمات تُستخدم من قبل أشخاص سيئين يقدمون خدمة تسجيل نطاقات مجانية وإضافتها بشكل سريع، ويأمل الباحثون أن يعطي تسجيل أسماء النطاقات منتهية الصلاحية تحذيراً باحتمال وجود هجمات وشيكة. إلا أن ليفر وجد أن الهجمات غالباً ما كانت تأتي من نطاقات أُعيد تسجيلها بعد أشهر من انتهاء صلاحيتها.

ويتطلب البحث تطوير نظام فلترة (في بيانات مزوّد خدمة الانترنت) يعمل على الفصل بين حركة مرور البيانات الطبيعية في الشبكة وتلك المشبوهة. كذلك أجرى الباحثون ما يعتقدون أنه أكبر مجهود –حتى اليوم– لتصنيف البرمجيات الخبيثة، حيث يجري التمييز بينها وبين البرمجيات غير المرغوبة **PUPs**. ولدراسة أوجه التشابه، فقد صُنفت هذه البرمجيات الخبيثة إلى عوائل محددة **families**.

وتمكّن الباحثون من خلال دراسة حركة المرور المتعلقة بالبرمجيات الخبيثة ـالتي لوحظت من قِبل مزود خدمة الانترنت قبل اكتشاف البرمجيات الخبيثةـ من تحديد إشارات هذه البرمجيات قبل أسابيع أو أشهر من ظهور البرمجيات، ويشبّه أنتوناكاكيس إشارات الشبكة بالحمّى أو الشعور بالوهن العام، والذي يسبق إصابة الإنسان بالعدوى الفيروسية المسببة للمرض.

ويقول أنتوناكاكيس: "يدرك الإنسان إصابته بالمرض فور شعوره بالحمى، وبدون معرفته سبب المرض"، ويتابع قائلاً: "إن أول ما يفعله أصحاب البرمجيات الخبيثة هو إعدادها للتواجد في شبكة الانترنت، ويعتبر هذا الأمرُ أولَ علامة للإصابة بهذه البرمجيات. لذا علينا أن نلحظ تواجد هذه الأعراض في الشبكة من البداية، لأننا لو انتظرنا رؤية عينة من هذه البرمجيات، فهذا يعني في غالب الأمر سماحنا لها بالتطور بشكل كبير في الشبكة."



وجد باحثون من معهد جورجيا للتقنية أن باستطاعة مسؤولي أمن الأنظمة اكتشاف إصابة الشبكة بالبرمجيات الخبيثة قبل فترة كافية (أسابيع أو حتى أشهر) قبل أن يكونوا قادرين على التقاط عينة من هجوم البرمجيات الخبيثة، وذلك عن طريق فحص وتحليل تدفق البيانات في الشبكات إلى نطاقات مشبوهة.Credit: Fitrah Hamid, Georgia Tech

وتمكن الباحثون من العثور على أكثر من 300 ألف نطاق للبرمجيات الخبيثة، والتي كانت نشطة لأسبوعين على الأقل قبل أن يجري تعريف وتحليل العينات الخبيثة المقابلة لها.

يقول أنتوناكاكيس: "وبشكل مشابه لدراسة الحالة الصحيّة للإنسان، حيث نحتاج لمعرفة الحالة الطبيعية لأنشطة الجسم كي نتمكن من رصد التغيرات التي تشير إلى إصابته بعدوى معينة". لذا، يجب على مسؤولي الشبكات أن يكونوا على علم بالأنشطة اليومية للشبكة

وبالحركة العادية لمرور البيانات حتى يتمكنوا من تحديد أي أنشطة غير معتادة يمكن أن تشير إلى احتمالية حدوث هجمات. وبالرغم من قدرة البرمجيات على إخفاء الكثير من آثار هجماتها على الشبكات، إلا أنها تبقى بحاجة إلى الاتصال بالأشخاص الذين أرسلوها.

ويتابع أنتوناكاكيس قائلاً: "عندما تكون قادراً على تحديد حركة مرور الشبكة ـبغض النظر عن كيفية دخول البرمجية الخبيثةـ فباستطاعتك ملاحظة إجراءات التواصل خلالها، وعلى مسؤولي الشبكات أن يُقللوا ـقدر المستطاعـ من وجود الأنشطة غير المعروفة في شبكتهم، وأن يُصنّفوا حالات تناقل البيانات والاتصالات المناسبة فيها، وذلك حتى يتمكنوا من معرفة وملاحظة أي حالة أو نشاط غير معتاد في الشبكة فور حدوثه."

ويأمل كل من أنتوناكاكيس وليفر أن تؤدّي هذه الدراسة إلى تطور استراتيجيات جديدة في حماية شبكات الحاسوب.

ويقول أنتوناكاكيس: "إن حركة مرور البيانات هي النقطة الحرجة في الشبكات، وهي كذلك المكان الذي يجب أن نخوض المعركة فيه". ويتابع: "تُقدم هذه الدراسة رؤيةً أوّليةً لما يجب أن يكون عليه شكل وتصميم آليات حماية الشبكات في الجيل القادم منها، فكلما كانت الهجمات أعقد وأكثر شراسة، كلما كان علينا أن نكون أذكى ونكتشفها بوقت أبكر."

- التاريخ: 2017-07-18
- التصنيف: تكنولوجيا

#الانترنت #البرمجيات الخبيثة #حماية شبكات الحاسوب

المصادر

- phys.org

المساهمون

- ترجمة
  - حمدان زياد
- مُراجعة
  - دانا أسعد
- تحرير
  - مريانا حيدر
  - حسن شوفان
- تصميم
  - أسامة أبو حجر
- نشر
  - مي الشاهد