كاسبرسكي: الثغرات غير المكتشفة تسببت في أكثر من 5 ملايين هجمة خلال الربع الثاني من 2017

الاثنين 21 أغسطس 2017 05:08 م

أصبحت حزم الثغرات الأمنية غير المكتشفة والتي لاتزال قيد الاختبار، بمثابة العامل الأبرز لتغيير قواعد مشهد التهديدات الإلكترونية والتي تم رصدها في الربع الثاني من عام 2017.

وفي غضون 3 أشهر فقط، تمكنت منتجات كاسبرسكي لاب من منع أكثر من خمسة ملايين هجمة كان السبب الكامن وراءها استغلال ثغرات أمنية في ملفات مؤرشفة كان قد تم تسريبها عبر الإنترنت. وقد بلغت هذه الهجمات ذروتها بنهاية الربع، مما يشير، وفقًا للشركة، إلى وجود حجم لا يستهان به من هذه التهديدات الإلكترونية.

وقد توصل تقرير كاسبرسكي لاب بشأن هجمات البرمجيات الخبيثة للربع الثاني من عام 2017 إلى أن الثغرات هي نوع من البرمجيات الخبيثة التي تستغل الأخطاء البرمجية في برنامج ما لتصيب الأجهزة بمزيد من الأكواد الخبيثة الإضافية، مثل أحصنة طروادة المصرفية أو هجمات الفدية الخبيثة أو ملفات التجسس الإلكتروني.

ووفقًا لتقرير الشركة الروسية الرائدة في مجال أمن المعلومات، تأتي الهجمات التي تُشن عن طريق استغلال الثغرات الأمنية من بين الهجمات الأشد تأثيرًا لأنها لا تتطلب عمومًا أي تواصل أو تفاعل مع المستخدم ويمكنها توصيل أكوادها الخطيرة من دون إثارة أي شكوك لدى المستخدم. وبالتالي فإن هذه الأدوات تستخدم على نطاق واسع، سواء من قبل مجرمي الإنترنت الذين يسعون إلى سرقة الأموال من المستخدمين والشركات الخاصة، وفي هجمات موجهة متطورة تستهدف الاستيلاء على معلومات حيوية وحساسة.

وقد شهد الربع الثاني من عام 2017 موجة كبيرة من الثغرات الأمنية غير المعروفة بسبب تسريب عدد من الثغرات البرمجية عبر الإنترنت. وقد استتبع ذلك تغييرًا كبيرًا في مشهد التهديدات الإلكترونية. وتمثلت البداية الأساسية في إصدار Shadow Brokers لأرشيف Lost In Translation، الذي تضمن عددًا كبيرًا من الثغرات غير المكتشفة لإصدارات مختلفة من برنامج ويندوز.

وبالرغم من حقيقة أن معظم هذه الثغرات الأمنية لم تكن من نوع ثغرات يوم الصفر وتم تصحيحها عن طريق تحديث مايكروسوفت الأمني قبل شهر من ذلك التسرّب، إلا أن هذا الإصدار قد أدى إلى عواقب كارثية. يتزايد متوسط عدد الهجمات اليومية بشكل مستمر: تم اكتشاف 82% من جميع الهجمات في آخر 30 يوما من الربع.

كما توصل التقرير إلى أن الأضرار الناجمة عن البرمجيات الخبيثة التي استخدمت الثغرات الأمنية غير المكتشفة من الأرشيف المسرّب، بالإضافة إلى عدد من المستخدمين المصابين لا تعد ولا تحصى – وكان من الأمثلة الأكثر وضوحًا عليها، هجمات ExPetr و "وانا كراي". ومن ضمن الأمثلة الأخرى، ثغرة CVE-2017-0199 المكتشفة في مايكروسوفت أوفيس مطلع شهر نيسان/أبريل. ومع أنه قد تم تصحيحها في الشهر نفسه، إلا أن عدد المستخدمين الذين تم استهدافهم قد وصل ذروته مسجلًا 1.5 مليون مستخدمًا. وبشكل عام، شكلت الهجمات المستهدفة لهؤلاء المستخدمين عن طريق استغلال الثغرة الأمنية CVE-2017-0199 نسبة 71% من إجمالي عدد تلك الهجمات.

وأشار الكسندر ليسكين، الخبير الأمني في كاسبرسكي لاب، قائلًا: "يعد مشهد التهديدات في الربع الثاني بمثابة إنذار آخر يوضح حقيقة مفادها أن عدم توخي الحذر يعتبر من أكثر المخاطر تأثيرًا على الإنترنت. ومع أن الموردين يقومون بتصحيح الثغرات الأمنية على أساس منتظم، إلا أن العديد من المستخدمين لا يولون اهتماما لهذا، الأمر الذي سيؤدي إلى شن هجمات واسعة النطاق بمجرد تسرب تلك الثغرات الأمنية إلى مجتمع مجرمي الإنترنت".

وتشمل إحصاءات تهديدات الإنترنت الأخرى الواردة في تقرير الربع الثاني 2017 ما يلي:

- في الربع الثاني، اكتشفت حلول كاسبرسكي لاب ومنعت عدد 342,566,061 من هجمات البرمجيات الخبيثة من مصادر عبر الإنترنت تقع في 191 دولة حول العالم، وهو أقل من الرقم المسجل في الفترة السابقة والذي بلغ 479,528,279 هجمة خبيثة من مصادر إنترنت موجودة في 190 دولة حول العالم.
- تم اكتشاف محاولات لإصابة عدد 224,675 جهاز حاسب مختلف بهجمات البرمجية الخبيثة التي تستهدف سرقة الأموال عن طريق اختراق الحسابات المصرفية عبر الإنترنت، مقارنة بعدد 288,000 جهاز حاسب في الربع الأول.
- تم حجب هجمات الفدية لتشفير البيانات على 246,675 جهاز حاسب مختلفًا، مقارنة بعدد 240,799 جهاز حاسب في الربع الأول.
- تمكنت برامج كاسبرسكي لاب لمكافحة الفيروسات من اكتشاف ما مجموعه 185,801,835 برمجية خبيثة مختلفة وعنصرًا محتملًا غير مرغوب فيه في الربع الثاني، مقارنة مع ما مجموعه 174,989,656 من البرمجيات الخبيثة المختلفة وعنصرًا محتملًا غير مرغوب فيه في الربع الأول.
- وفي المتوسط، تعرضت نسبة 26.17% من أجهزة الحاسب المتصلة بالإنترنت في العالم لمرة واحدة على الأقل إلى هجوم على الإنترنت باستخدام عناصر بمستوى برمجية خبيثة.

وللحد من مخاطر الإصابة، تنصح كاسبرسكي لاب المستخدمين بالمواظبة على تحديث البرنامج المثبت على جهاز الحاسب الخاص بكم بشكل مستمر، وتفعيل خاصية التحديث التلقائي في حال كانت متوفرة. كما توصي بالقيام باختيار بائع برمجيات يتبع نهجًا مسؤولًا تجاه حل مشكلات الثغرات الأمنية وتصحيحها. وتأكدوا كذلك فيما إذا كان بائع البرمجيات يوفر برنامج اكتشاف الثغرات خاصًا به.

وتوصي الشركة باستخدام حلول أمنية قوية والتأكد من أنها تبقي جميع البرامج في حالة تحديث دائم، وبالقيام بإجراء فحص دوري للنظام للتحقق من خلوه من أي إصابات محتملة.