كاسبرسكي تكتشف ثغرة أمنية خطيرة في أحد أكثر برامج إدارة الخوادم استخداما حول العالم

الأربعاء 16 أغسطس 2017 07:08 م

اكتشف خبراء كاسبرسكي لاب ثغرة أمنية على شكل هجمات الباب الخلفي زرعت في برمجية لإدارة الخوادم تُستخدم من قبل مئات الشركات الكبيرة حول العالم.

وأوضحت الشركة الروسية أنه بعد تفعيل ثغرة الباب الخلفي، سرعان ما تسمح للمهاجمين بتنزيل المزيد من البرمجيات الخبيثة أو سرقة البيانات. وقد أخطرت كاسبرسكي لاب شركة توريد البرنامج المتأثر: NetSarang والتي قامت على الفور بإزالة الكود الخبيث وطرح إصدار محدّث للعملاء.

وأضافت الشركة الرائدة في مجال أمن المعلومات أن ShadowPad هي واحدة من أكبر الهجمات المعروفة والتي تتسلل عن طريق شبكات سلسلة التوريد. وفي حال أنه لم يتم اكتشافها وتصحيحها بسرعة، فمن المحتمل أن تستهدف مئات الشركات في جميع أنحاء العالم.

وذكرت كاسبرسكي لاب أنه في شهر تموز/يوليو الماضي، تم التواصل مع فريق الأبحاث والتحليلات العالمي في كاسبرسكي لاب من قبل أحد شركائه وهي مؤسسة مالية. وقد أبدى خبراء الأمن في المؤسسة المعنية قلقهم بشأن طلبات مشبوهة واردة من خادم أسماء النطاقات، وأظهرت تحقيقات أخرى أن مصدر هذه الطلبات يعود إلى برنامج إدارة الخادم الذي أنتجته شركة نظامية واستخدمه مئات العملاء في قطاعات عديدة، من ضمنها قطاع الخدمات المالية والتعليم والاتصالات والتصنيع والطاقة والنقل. ومن أكثر النتائج إثارة للقلق، وفقًا للشركة، أن المورد لم يقصد من وراء بيع هذا البرنامج تقديم أي من هذه الطلبات.

وكشفت تحاليل إضافية أجرتها كاسبرسكي لاب أن الطلبات المشبوهة كانت في الواقع نتيجة لنشاط نمط برمجي خبيث مندسّ داخل إصدار محدّث لإحدى البرامج النظامية. وبعد تثبيت الإصدار المحدّث للبرنامج المصاب، تبدأ البرمجية الخبيثة نشاطها بإرسال طلبات خادم أسماء النطاقات إلى نطاقات محددة (خادم خادم التحكم والسيطرة الخاص بها) بشكل متكرر، بمعدل مرة واحدة كل ثماني ساعات.

ويتضمن الطلب عادة معلومات أساسية عن نظام الضحية (اسم المستخدم، اسم النطاق، اسم المضيف) . وفي حال ارتأى المهاجمون أن هذا النظام مثير للاهتمام، يقوم خادم التحكم بالرد وتفعيل منصة الباب الخلفي المكتملة الأركان والتي تتغلغل ذاتيًا وبصمت داخل حاسب الضحية. بعد ذلك، وبعد تلقي أوامر من المهاجمين، تصبح منصة الباب الخلفي قادرة على تحميل وتنفيذ المزيد من الأكواد الخبيثة.

وفي أعقاب هذا الاكتشاف، قام باحثو كاسبرسكي لاب على الفور بالتواصل مع NetSarang. واستجابت الشركة المعنية بسرعة لطلب كاسبرسكي لاب وطرحت إصدارًا محدّثًا من البرنامج خال من الكود الخبيث.

وفقا لأبحاث كاسبرسكي لاب، تم تفعيل هذا النمط البرمجي الخبيث، حتى الآن، في هونج كونج، وهناك احتمال بأن يكون موجودًا ولكن في حالة خمول على العديد من الأنظمة الأخرى حول العالم، وخاصة في حال لم يقم المستخدمون بتثبيت النسخة المحدثة من البرنامج المتأثر.

وأثناء تحليل أدوات التقنيات والإجراءات المستخدمة من قبل المهاجمين، توصل باحثو كاسبرسكي لاب إلى استنتاج مفاده أنه توجد أوجه تشابه تشير إلى متغيرات البرمجيات الخبيثة PlugX المستخدمة من قبل Winnti APT، وهي مجموعة ناطقة باللغة الصينية المعروفة. غير أن هذه المعلومات لا تكفي لتأسيس علاقة وثيقة مع هذه الجهات الفاعلة.

وقال إيجور سومينكوف، الخبير الأمني في فريق الأبحاث والتحليلات العالمي لدى كاسبرسكي لاب: "تعد ShadowPad مثالًا على مدى الخطورة الناجمة عن النجاح في شن هجمات واسعة النطاق من خلال التسلل عن طريق شبكات سلسلة التوريد وما يمكن أن تحدثه من تداعيات. وبالنظر إلى ما تتيحه للمهاجمين من مزايا الوصول السهل وجمع البيانات، فمن المرجح أن يتم إعادة إنتاج أو استنساخ برمجية ShadowPad مرارا وتكرارا مع بعض من مكونات البرمجيات الأخرى المستخدمة على نطاق واسع".

وأضاف سومينكوف: "ولحسن الحظ، لمسنا من شركة NetSarang تجاوبًا سريعًا لملاحظاتنا، حيث بادرت الشركة على الفور بطرح إصدار محدّث ونظيف للبرنامج، مما ساهم على الأرجح في منع مئات الهجمات المستهدفة لسرقة بيانات عملائها. ومع ذلك، تظهر هذه الحالة أنه من الضروري أن يكون لدى الشركات الكبيرة حلولًا أمنية متقدمة قادرة على رصد نشاط الشبكة والكشف عن الحالات المشبوهة والمريبة. وهذا هو السبيل الوحيد الذي يتيح لعملائنا اكتشاف الهجمات الخبيثة حتى في حال كان المهاجمون على قدر عال من التطور بحيث يلجؤون للتخفي داخل البرامج النظامية".

وتنصح كاسبرسكي لاب المستخدمين بالقيام وبشكل فوري بتثبيت الإصدار المحدّث لبرنامج NetSarang، الذي تمت إزالة النمط الخبيث المكتشف حديثًا منه، والتأكد من خلو أنظمتهم من أي مؤشرات على طلبات مشبوهة صادرة عن خادم أسماء النطاقات DNS إلى نطاقات غير مألوفة. وتتوفر قائمة بأسماء خادمات نطاقات التحكم المستخدمة من قبل هذا النمط البرمجي الخبيث في مدونة Securelist، والتي تتضمن أيضًا المزيد من المعلومات التقنية بشأن ثغرة الباب الخلفي.