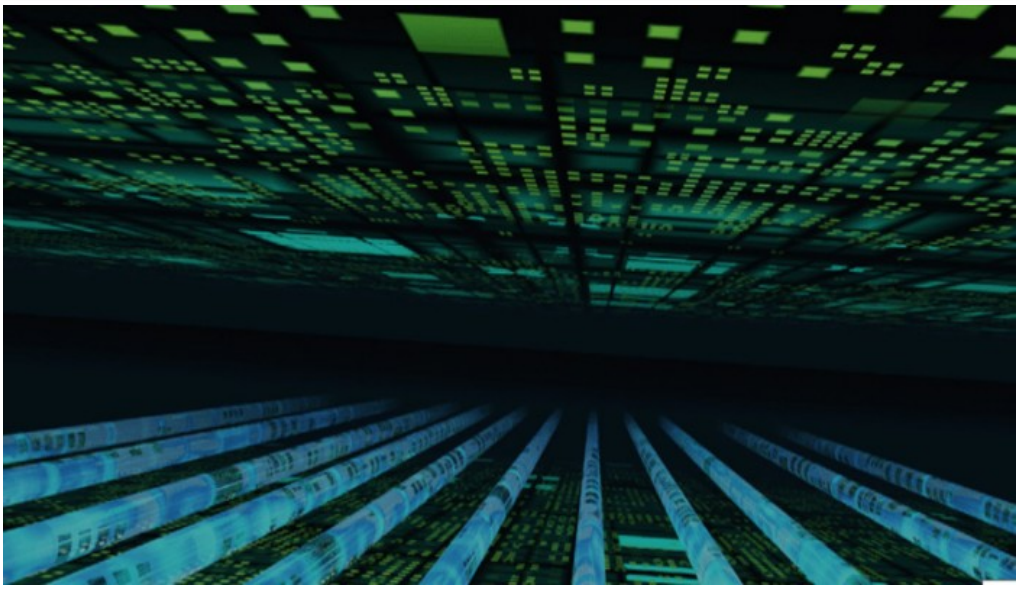
سيكيوروركس تكشف تفاصيل جديدة عن برمجيات الفدية سام سام



الاثنين 19 فبراير 2018 01:02 م

كشفت اليوم سيكيوروركس Secureworks، الشركة العالمية المتخصصة في توفير الحماية للشركات في العالم الرقمي المتصل بالإنترنت، عن تفاصيل جديدة حول برمجيات الفدية "سام سام"، وهي عبارة عن حملات إلكترونية خبيثة للاستغلال المالي باستخدام برمجية الفدية الخبيثة ظهرت أواخر العام 2015، والتي تعرف أيضاً باسم "ساماس"، و"سام سام كريبت".

وربط باحثو وحدة مكافحة التهديدات نشاط هذه الحملات بمجموعة القرصنة الإلكترونية "جولد لويل"، التي تقوم بعملية مسح لاستغلال الثغرات الأمنية المعروفة في أنظمة الإنترنت بهدف الحصول على موطئ قدم أولي على شبكة الضحية.

ويقوم مطلقو التهديدات بنشر برمجية الفدية سام سام، وطلب دفعة مالية لفك التشفير عن ملفات الشبكة المستهدفة، وتشير الأدوات والسلوكيات المرتبطة بهجمات سام سام منذ العام 2015 إلى أن جولد لويل هي إما مجموعة تهديد محددة أو عبارة عن مجموعة من الجهات الإجرامية الإلكترونية الفاعلة المرتبطة ببعضها ارتباطاً وثيقاً.

وإن تطبيق التحديثات الأمنية في الوقت المناسب، والمراقبة الدورية للسلوكيات الشاذة على الأنظمة المرتبطة بالإنترنت تشكل وسيلة دفاعية فعالة ضد هذه التهديدات، كما يتوجب على الشركات إنشاء واختبار خطط استجابة واضحة لحوادث الإصابة ببرمجيات الفدية، واستخدام حلول النسخ الاحتياطي التي تمتاز بالمرونة تجاه محاولات الاختراق والتهديد المختلفة.

وقام الباحثون لدى وحدة مكافحة التهديدات لدى شركة سيكيوروركس بتقسيم المعلومات الخاصة بالتهديد الإلكتروني إلى قسمين: قسم استراتيجي، وقسم تكتيكي.

ويمكن للتنفيذيين استخدام التقييم الاستراتيجي للتهديد المتواصل لتحديد كيفية الحد من المخاطر التي يمكن أن تتعرض لها الأصول والبيانات الحساسة لدى مؤسساتهم، كما يمكن للمدافعين عن شبكات الحواسيب استخدام المعلومات التكتيكية التي تم جمعها من الأبحاث وتحقيقات الاستجابة للحوادث للحد من الوقت والجهد المرتبط بعملية الاستجابة لأنشطة المجموعة الإجرامية.

نقاط رئيسية
يشير تحليل وحدة مكافحة التهديدات الخاصة ببرمجية الفدية الخبيثة سام سام إلى أنه عادة ما يتم نشر هذه البرمجية بعد أن تتمكن الجهات المهاجمة من استغلال الثغرات الأمنية المعروفة على الأنظمة الخارجية للتمكن من الوصول إلى شبكة الضحية.
تتسم عمليات الفدية هذه بالانتهازية، وقد أثرت كثيراً على هيئات ومؤسسات من مختلف القطاعات والصناعات حول العالم.
يشير قرار مجموعات التهديد بنشر برمجية الفدية عقب اختراق أولي للشبكة إلى تركيز هذه المجموعات على عمليات الاستغلال الفردية عوضاً عن نشر برمجيات الفدية عشوائياً عبر حملات للتصيد والاحتيال الواسعة عبر الشبكة.
تعود هذه الحملات الخبيثة بالربح المادي الكبير على المهاجمين، على سبيل المثال، حققت هجمة واحدة قامت بها مجموعة القرصنة الإلكترونية "جولد لويل" بين أواخر العام 2017 وبداية العام 2018 ربح مادي لا يقل عن 350 ألف دولار أمريكي.
الاستقصاء الاستراتيجي للتهديدات
إن تحليل أهداف وأصول وكفاءة مجموعات القرصنة الإلكترونية يمكن أن يحدد ماهية الشركات التي يمكن أن تكون عرضة لهجمات هذه المجموعات، ويمكن لهذه المعلومات أن تساعد الشركات على اتخاذ قرارات دفاعية استراتيجية فيما يتعلق بهذه التهديدات.

الإمكانيات
تجمع مجموعة القرصنة الإلكترونية "جولد لويل" بين أدوات ومنتجات الملكية مع تقنيات الاستغلال والاستهداف المتاحة أمام العامة، وإن تطوير مجموعة "جولد لويل" لأداة فدية برمجية خاصة يشير إلى أنهم يتمتعون بمعرفة كبيرة بعمليات التشفير وبيئات ويندوز الشبكية.

وتظهر هذه المجموعة قدرة على الاستفادة من النفاذ إلى الأنظمة المرتبطة بالإنترنت وتصعيد الامتيازات ضمن الشبكات المخترقة، وتتطلب أعمال مجموعة القرصنة الإلكترونية خبرات عملية وتفاعلية على لوحة المفاتيح لتأسيس علاقة مباشرة بين مجموعة التهديد والضحية

وعادة ما يعرض مطلقي التهديد على الضحايا خيارات لاختبار فك التشفير قبل عملية الدفع بهدف بناء الثقة بين الطرفين

ويشير زيادة نشاط مجموعة القرصنة الإلكترونية "جولد لويل" بين العام 2015 والعام 2018 إلى أن المجموعة تستفيد مالياً من حملات برمجيات الفدية الخبيثة عقب عمليات الاستهداف الانتهازية للشبكات وقامت المجموعة بتعديل أسلوب عملها قليلاً للاستفادة من الأدوات المتاحة للجمهور، وطورت تدريجياً أدوات الملكية بهدف مواصلة النجاح في عمليات الاستهداف

ودائمًا ما يبحث أصحاب التهديدات عن الأنظمة الغير محمية والمعرضة للخطر، لذا، تشجع وحدة مكافحة التهديدات العملاء على منح الأولوية للضوابط الأمنية للأنظمة والخدمات المرتبطة بشبكة الإنترنت

وتعتبر عمليات تحديث البرمجيات والقيام باختبارات دورية للكشف عن الخروقات، ومراقبة السلوكيات الشاذة، والحد من النفاذ إلى الشبكة من أفضل الممارسات المتبعة للحد من مخاطر الإصابة بالهجمات الإلكترونية الخبيثة، ويجب على الشركات تقييم مدى قدرتها على الصمود أمام هجمات الفدية والذي يتضمن إيجاد واختبار خطط استجابة للحوادث، وتوليد وحماية النسخ الاحتياطية للبيانات الحساسة