الخليج

اقتصاد, تقنية وسيارات

22 يوليو 2022 16:03 مساء

لونا».. عصابة فدية تستهدف أنظمة التشغيل ببرمجية واحدة»

كشف باحثو "كاسبرسكي" عن عصابة رقمية تختصّ بشنّ هجمات ببرمجيات الفدية.

إحدى لغات Rust تستخدم برمجية فدية مكتوبة بلغة Luna ووجد الباحثون أن العصابة، التي أُطلق عليها اسم وغيرها. Hiveو BlackCat البرمجة التي سبق استخدامها من قبل عصابات مثل

وتسمح لغة البرمجة بنقل البرمجيات الخبيثة بسهولة من نظام تشغيل إلى آخر. وأوردت كاسبرسكي هذا الاكتشاف التابع للشركة. Securelist وغيره في تقرير حول أدوات الجريمة الرقمية، يمكن الاطلاع عليه في موقع

تتيح إمكاناتها عبر الأنظمة الأساسية للمجموعة، استهداف أنظمة تشغيل Rust برامج ضارة مكتوبة بلغة Luna وتنشر .ESXiومنصات متنوعة، بينها «ويندوز» و«لينكس» و

نشرت إعلاناً على شبكة الويب المظلمة رصدته كاسبرسكي، يفيد بأنها تعمل فقط مع «حلفاء» ناطقين Luna وكانت باللغة الروسية. وعلاوة على ذلك، تحتوي برمجية الفدية المشفرة على بعض الأخطاء الكتابية، ما يدعو إلى استنتاج أن نظراً لكونها مكتشفة Luna العصابة قد تكون ناطقة بالروسية. وليس هناك معلومات كثيرة متاحة عن ضحايا عصابة حديثاً، لكن كاسبرسكي أكّدت حرصها على تتبع نشاطها.

التوجّه الحديث المتمثل باهتمام عصابات الفدية بالبرمجيات العاملة على عدة أنظمة تشغيل؛ إذ اعتمد Luna وتؤكّد

في تنفيذ برمجياتها Rustو Golang عدد من هذه العصابات الرقمية كثيراً في العام الماضي على لغات برمجة مثل الخبيثة.

المستقلتين Rustو Go التي استخدمت كلاً من لغتي البرمجة Hiveو BlackCat وتضمّ أبرز الأمثلة العصابتين وغير المرتبطتين بالطبيعة التقنية لأنظمة التشغيل، ما يمكّن الجهات التخريبية من نقل برمجيات الفدية المكتوبة باستخدامهما من نظام إلى آخر بحرّية؛ لذا يمكن أن تستهدف الهجمات أنظمة تشغيل متعدّدة في الوقت نفسه.

التي توظّف إصداراً Black Basta يقدّم تحقيق آخر أجرته كاسبرسكي حديثاً نظرة أعمق على نشاط عصابة الفدية منذ Black Basta التي ظهرت لأول مرة في فبراير/ شباط 2022. وهاجمت C++ جديداً من برمجية فدية مكتوبة بلغة ذلك الحين أكثر من 40 جهة معظمها في الولايات المتحدة وأوروبا وآسيا.

إضافة إلى نظامي ESXi تستهدفان كذلك أنظمة Black Bastaو Luna وأظهرت تحقيقات كاسبرسكي أن كلاً من نظام تشغيل ومراقبة ESXi التشغيل «ويندوز» و«لينكس»، وهو توجه آخر لبرمجيات الفدية برز في عام 2022. ويُعد للأجهزة الافتراضية يمكن استخدامه باستقلالية على أي نظام تشغيل. ويسهل على الجهات التخريبية تشفير بيانات الضحايا بعد أن انتقلت العديد من المؤسسات إلى الأجهزة الافتراضية القائمة على هذا النظام.

وقال يورنت فان ديرفيل خبير الأمن لدى كاسبرسكي: إن التوجّهات التي حدّدتها الشركة في وقت سابق من هذا العام «تزداد وضوحاً»، لافتاً إلى أن المزيد من العصابات الرقمية بدأت تستخدم لغات برمجية متعدّدة الأنظمة لكتابة برمجيات الفدية الخاصة بها. وأضاف: «هذا التوجه يمكّن العصابات من توظيف برمجياتها الخبيثة في مجموعة متنوعة تثير القلق. ونتوقع ESXi من أنظمة التشغيل؛ لذا نرى بأن الهجمات المتزايدة على الأجهزة الافتراضية العاملة بالنظام .«في هذا السياق ظهور المزيد من عائلات برمجيات الفدية