الخليج

اقتصاد, تقنية وسيارات

28 أبريل 2022 00:59 صباحا

نشاط ملحوظ في مشهد التهديدات المتقدمة المستمرة خلال الربع الأول

kaspersky

«دبي: «الخليج

في الربع الأول من العام (APT) أظهر أحدث تقرير من كاسبرسكي يتناول توجهات التهديدات المتقدمة المستمرة 2022، أن الجهات القائمة وراء هذه التهديدات كانت نشطة خلال الأشهر الثلاثة الأولى من العام. وأحدثت الحملات التخريبية التي نفذتها الجهات المعروفة والجديدة تغييرات كبيرة في مشهد التهديدات المتقدمة المستمرة. واستهدفت الجهات التخريبية في الغالب شركات وجهات حكومية، بعد أن أجرت تحديثات على أطقم الأدوات الخبيثة التي تستخدمها ونوّعت أساليبها لرفع مستوى هجماتها.

وواصل باحثو كاسبرسكي، خلال الأشهر الثلاثة الأولى من العام 2022، الكشف عن أدوات وتقنيات وحملات جديدة أطلقتها عصابات التهديدات المتقدمة المستمرة واستخدمتها في الهجمات الرقمية التي شنّتها في جميع أنحاء العالم. واستُخلص تقرير توجهات التهديدات المتقدمة المستمرة من أبحاث كاسبرسكي ومعلومات التهديدات التي تحصل عليها الشركة، علاوة على أبرز التطورات والحوادث الرقمية التي يرى الباحثون أن على الجميع إدراكها.

وطوال الربع الأول من العام الجاري، انشغلت الجهات التخريبية بإطلاق حملات جديدة وشنّ عدد من الهجمات المرتبطة بالأحداث الجيوسياسية الحساسة. وشملت أهم النتائج التي عرضها التقرير:

الأزمات الجيوسياسية محرك رئيس للتهديدات المتقدمة المستمرة

شهد مشهد التهديدات المتقدمة المستمرة العديد من الهجمات المرتبطة بالأزمة الأوكرانية. وأُبلغ عن هجمات وهجمات أخرى جديدة تستهدف جهات أوكرانية خلال شهري فبراير ومارس. DoubleZeroو HermeticRansom وUNC1151و APT Gamaredon وحدث ارتفاع كبير في مكونات البنية التحتية الجديدة التي وظفتها عصابات جرى تطويرهما WhisperGate واستطاع باحثو كاسبرسكي تحديد عيّنتين من النموذج التجريبي .(Ghostwriter) في ديسمبر 2021 وتحتويان على سلاسل اختبار ومراجعات سابقة لملاحظة الفدية الواردة في عينات من مايكروسوفت. وخلص الخبراء بثقة عالية إلى أن هذه العينات مثلت حالات تكرار سابقة لأداة المسح التي وردت تقارير عن استخدامها في أوكرانيا.

التي تنشط منذ منتصف العام 2021 في Konni كذلك حدّد باحثو كاسبرسكي ثلاث حملات مرتبطة بجهة التهديد نفسها خلال مختلف الحملات، Konni RAT استهداف الكيانات الدبلوماسية الروسية. واستخدم المهاجمون غرسة لكن نواقل الهجوم كانت مختلفة في كل حملة، وتنوّعت بين مستندات تحتوي على وحدات ماكرو، وأداة تثبيت متستّرة في هيئة أحد تطبيقات المستخدمة في جائحة كورونا، وأداة تنزيل متخفية في حافظة شاشة للعام الجديد.

عودة الهجمات منخفضة المستوى

في العام الماضي، توقع باحثو كاسبرسكي أن تحظى الغرسات الخبيثة منخفضة المستوى بمزيد من التطوير في العام ليؤكّد بوضوح هذا التوجه. فقد كانت هذه الغرسة Moonbounce 2022. وجاء اكتشاف كاسبرسكي للغرسة الخبيثة التي تستهدف البرمجيات Bootkit الحالة الثالثة المعروفة والمستخدمة في الواقع لمجموعة أدوات البرمجيات الثابتة وهي (UEFI) الثابتة. وأُخفيت هذه المجموعة البرمجية الخبيثة في الواجهة الموحدة والموسّعة للبرمجيات الثابتة مكون التخزين الواقع خارج القرص الصلب. SPI جزء أساسي من أجهزة الحاسوب، وتحديدًا في الذاكرة الفلاشية ونسب خبراء كاسبرسكي هذه الحملة إلى عصابة التهديدات المتقدمة المستمرة المعروفة APT41.

جهات التهديد تلاحق العملات الرقمية

في هذا الربع، لاحظت كاسبرسكي أيضًا أن جهات التهديد تواصل السعي وراء العملات الرقمية. وبخلاف غالبية وعصابات أخرى، تحقيق Lazarus عصابات التهديدات المتقدمة المستمرة التي تحظى برعاية حكومية، فقد جعلت مفخّخ (DeFi) في حملات لها تطبيق تمويل لامركزي Lazarus المكاسب المالية أحد أهدافها الرئيسة. ووزّعت بتروجان خطر سعيًا وراء زيادة الأرباح، إذ تُواصل العصابة استغلال التطبيقات الرسمية المستخدمة في إدارة محافظ العملات الرقمية وذلك بتوزيع برمجيات خبيثة تتيح التحكّم في أنظمة الضحايا.

التحديثات وإساءة استخدام الخدمات عبر الإنترنت

تواصل جهات التهديدات المتقدمة المستمرة البحث عن طرق جديدة لزيادة كفاءة هجماتها. وفي هذا السياق تستمر أقدَم برمجية خبيثة تقدّمها هذه Janicab بتحديث أدواتها. وتُعدّ DeathStalker عصابة المرتزقة التي يطلق عليها اسم

الوظائف نفسها مثل عائلات Janicab العصابة، وذلك في العام 2013، وهي مثال بارز على هذا التوجه. وتُظهر البرمجيات الخبيثة المماثلة، ولكن بدلًا من تنزيل العديد من الأدوات لاحقًا خلال عملية الاختراق، مثلما اعتادت تتضمن العينات الجديدة في داخلها معظم الأدوات مخفية Powersingو EVILNUM العصابة أن تفعل في عمليات YouTube أكبر الخدمات عبر الإنترنت في العالم، مثل DeathStalker ضمن أداة الإسقاط. كذلك تستخدم .لتنفيذ عمليات قيادة وسيطرة خفية وفعالة DDRs وغيرها، مثل أدوات WordPressو +Googleو

ويلخص تقرير توجهات التهديدات المتقدمة المستمرة للربع الأول من العام 2022 نتائج تقارير المعلومات الخاصة بالتهديدات والواردة من المشتركين في خدمات كاسبرسكي فقط، وتتضمن أيضًا بيانات مؤشرات الاختراق وقواعد .للمساعدة في البحث الجنائي واصطياد البرمجيات الخبيثة YARA