"سوفوس" : المهاجمون السيبرانيون يستغلون ملفات تعريف الارتباط لاختراق الشبكات وانتحال شخصية المستخدمين القانونيين

غالاغر: شهدنا ازدياد الهجمات التي حوّلت الأمر إلى وسيلة للالتفاف على أنظمة التحقق المتعدد من الهوية

أعلنت "سوفوس" الشركة العالمية الرائدة لحلول الجيل الجديد للأمن السيبراني، عن إطلاق تقريرها Sophos X-Ops بعنوان "سرقة ملفات تعريف الارتباط: الطريقة الجديدة لتجاوز المحيط الخارجي"، والذي أظهر بأن المجرمين السيبرانيين رفعوا من وتيرة استهداف الثغرات عبر سرقة ملفات تعريف الارتباط لاستخدامها في اجتياز إمكانات التحقق المتعدد والوصول إلى الموارد المؤسسية.

وفي بعض الحالات، تعتبر سرقة ملفات تعريف الارتباط بحد ذاتها هجمة عالية التركيز، يحصل فيها المهاجمون على البيانات من نظام ما في الشبكة ويستخدمون ملفات قانونية لتكون واجهة تخفي أنشطتهم الخبيثة.

وبعد أن يتمكن المهاجم من الدخول إلى الموارد السحابية وموارد الويب التابعة للمؤسسة باستخدام ملفات تعريف الارتباط، يصبح بوسعه استخدامها لمزيد من الهجمات كاختراق البريد الإلكتروني وهجمات الهندسة الاجتماعية للتغلغل في النظام بشكل أكبر وحتى تغيير البيانات والسيطرة على رموز المصادر.

في هذا السياق قال شون غالاغر، كبير باحثي التهديدات لدى سوفوس: "شهدنا على مدى العام الماضي ازدياد الهجمات التي حوّلت سرقة ملفات تعريف الارتباط إلى وسيلة للالتفاف على أنظمة التحقق المتعدد من الهوية. فقد انتقل المهاجمون إلى نسخ محسّنة وحديثة من برمجيات سرقة المعلومات، مثل Raccoon Stealer وغيرها لتبسيط أمر الحصول على ملفات تعريف الارتباط الخاصة بالتحقق من الهوية. وفي حال حصول المهاجم على تلك الملفات، سيصبح بإمكانه التحرك بحريّة في الشبكة وانتحال شخصية المستخدمين القانونيين."

يذكر أن ملفات تعريف الارتباط للجلسات – أو تلك الخاصة بالتحقق من الهوية – هي نوع محدد من ملفات تعريف الارتباط التي يتم تخزينها في متصفح الويب عندما يقوم المستخدمين بتسجيل دخوله إلى موارد الويب. وفي حال حصول المهاجمين على تلك الملفات، فإن بوسعهم تنفيذ هجمة لتمرير تلك الملفات


شون غالاغر كبير باحثي التهديدات لدى سوفوس

وبالتالي التمكن من دخول الويب من جديد عبر خداع المتصفح واعتقاده بأنه تحقق من هوية المستخدم بالفعل، وبالتالي لا حاجة لتكرار التحقق.

ويضمن ذلك للمهاجم القدرة على اجتياز طبقة تحقق أخرى، فيما تتفاقم المشكلة نظرًا لأن العديد من تطبيقات الويب القانونية تستخدم ملفات تعريف الارتباط ذات الصلاحية طويلة الأمد والتي نادرًا ما تنتهي صلاحيتها أو لا تنتهي أبدًا – أما ملفات تعريف الارتباط الأخرى فتصبح غير سارية في حال تسجيل المستخدم خروجه من الخدمة.

واشار الي انه نظرًا لوجود قطاع يوفر البرمجيات كخدمة، فقد أصبح من السهل على المهاجمين المبتدئين أن يمارسوا سرقة كلمات المرور، فكل ما عليهم على سبيل المثال هو شراء نسخة من برمجيات سرقة المعلومات مثل Raccoon Stealer لجمع البيانات ككلمات المرور او ملفات تعريف الارتباط بكميات كبيرة ومن ثم بيعها في أسواق إجرامية منها Genesis. و حينها يمكن لمجرمين آخرين مثل مهاجمي برمجيات طلب الفدية شراء تلك البيانات وتصفيتها للاستفادة من أي شيء يمكنهم تحويله إلى هجمة مفيدة لهم.

حيث تجدر الإشارة إلى أن اثنتين من الهجمات الأخيرة التي حققت فيها سوفوس شهدتا اتخاذ مقاربة أكثر تركيزًا، حيث أمضى المهاجمون في واحدة من الهجمات عدة أشهر داخل الشبكة المستهدفة للحصول على ملفات تعريف الارتباط من متصفح مايكروسوفت إيدج.

وذكر انه تم الاختراق الأولي باستخدام برمجيات اختراق جاهزة، ثم استعمل المهاجم مزيجًا من أنشطة Cobalt Strike و M – terpreter لإساءة استخدام أدوات قانونية والحصول على حقوق الوصول إلى التطبيقات ، وفي حالة أخرى، استعمل المهاجم احد مكونات Microsoft V – sual Studio لإيصال برمجيات خبيثة تمكنت من سرقة ملفات تعريف الارتباط لأسبوع كامل.

أضاف غالاغر: "شهدنا سرقة ملفات تعريف الارتباط بكميات كبيرة في السابق ولكن المهاجمين الآن يعملون بشكل دقيق ومركّز لسرقتها، ونظرًا لانتقال قدر كبير من الأعمال إلى الويب، فإن هناك عددًا غير محدود من الأنشطة الخبيثة التي يستطيع المهاجمون القيام بها في الشبكات عند سرقة ملفات تعريف الارتباط. فبوسعهم التلاعب بالبنية التحتية السحابية واختراق البريد الإلكتروني وإقناع الموظفين بتنزيل البرمجيات الخبيثة أو حتى إعادة كتابة الأكواد للمنتجات – لا حدود للأفكار التي يمكن أن يطبقوها."

عبر حلول الأمن السيبراني الرائدة

"تريند مايكرو" تمكّن الشركات الصغيرة والمتوسطة في الكويت لبلوغ طموحاتها الرقمية

أعلنت شركة "تريند مايكرو إنكوربوريتيد"، إحدى الشركات العالمية الرائدة في حلول الأمن السيبراني، عن إطلاق مبادرة استراتيجية لتعزيز إمكانيات الشركات الصغيرة والمتوسطة في مجال الأمن الإلكتروني والمعلوماتي في الكويت، وذلك عبر مجموعة خدمات «Worry-Free» التي تقدمها الشركة، وهي عبارة عن حزمة من الحلول الأمنية المطورة خصيصًا لتلبية متطلبات الشركات الصغيرة والمتوسطة. وتهدف الشركة عبر إتاحة هذه الحلول إلى دعم ودفع عجلة التحول الرقمي للشركات الصغيرة والمتوسطة في الدولة عبر حلول مخصصة لتوفير حماية شاملة لأعمالها من المخاطر السيبرانية في خضم هذا العصر الرقمي المتطور.

وبمناسبة هذا الإعلان، صرّح أسعد عُرابي، المدير الاقليمي لتريند مايكرو في منطقة الخليج العربي، قائلًا: "أثبتت الكويت خلال السنوات القليلة الماضية مدى قدرتها على التكيّف مع التغيرات الكبيرة التي طرأت على العالم الرقمي. وبما أن الدولة تتبنى التكنولوجيا وتتجه نحو الرقمنة في كافة خدماتها، أصبح من الضروري أن تعمل الشركات الصغيرة والمتوسطة على تأمين نفسها لتتمكن من التطور بأمان، لأن هذه الشركات تعتبر ركيزة أساسية ضمن الاقتصاد الوطني وعنصر مهم لخلق فرص العمل، ولن يتم ذلك إلا عبر تبني اسراتيجيات الأمن السيبراني المتقدمة، ونحن في ترينـد مايكرو نملك إلتزاما راسخا بتسخير حلولنا الأمنية المتطورة لخدمة الشركات الصغيرة والمتوسطة والمجتمع الكويتي".

ووفقا لتقرير الأمن السيبراني السنوي الصادر عن شركة ترينـد مايكرو لعام 2021، نجحت الحلول الأمنية من ترينـد مايكرو في رصد وإيقاف أكثر من 14 مليون (14،911،051) تهديد عبر البريد الإلكتروني في الكويت، وإيقاف أكثر من3.5 مليون (3،528،979) هجمة باستخدام الروابط الضارة في جميع أنحاء الدولة. كما نجحت ترينـد مايكرو في رصد وإيقاف أكثر من1.7 مليون (1،780،214) هجمة عبر البرامج الضارة. ومع انتقال البلاد للعمل عن بُعد، تمكنت حلول ترينـد مايكرو «شبكة المنزل الذكي Smart Home Ne – work» من حماية الأجهزة المنزلية وإيقاف أكثر من 700 ألف (756،857) من التهديدات الواردة والصادرة في الشبكة. وتُشير إحصاءات التقرير إلى أنه في ظل تنامي مشهد التهديدات الرقمية يومًا بعد يوم، ستجد الشركات نفسها بحاجة إلى تطبيق حلول متعددة المستويات لتكون قادرة على حماية أعمالها في هذا العصر.


شركة "ترينـد" أطلقت مبادرة إستراتيجية لتعزيز إمكانات الشركات الصغيرة والمتوسطة

جدير بالذكر تقدم حزمة خدمات «Worry-Free Services» من شركة ترينـد مايكرو، وهي واحدة من حلول الأمن السيبراني المتطورة، حماية متكاملة من التهديدات عبر الأجهزة الطرفية المتصلة. بالإضافة إلى ذلك، توفر حماية فائقة ضد هجمات البريد الالكتروني وبرمجيات الفدية وفيروسات الابتزاز وغيرها من الهجمات المتقدمة عبر الجمع بين امكانيات التعلم الآلي عالي الدقة وخوارزميات الرصد العميق. وبإمكان حزمة خدمات «Worry-Free XDR» إجراء عمليات تحليل واسعة النطاق واتخاذ قرار الاستجابة الآلية بسرعة بسبب قدرتها المدعومة بالذكاء الاصطناعي على ربط البيانات التلقائي عبر مختلف الأجهزة الطرفية والحاسبات الخادمة وخدمات الويب السحابية وشبكات الانترنت والبريد الإلكتروني. وتتميز هذه الحزمة بأنها منصة موحدة تخفف أعباء العمل على موظفي تكنولوجيا المعلومات عبر تقديم حماية متعددة المستويات، الأمر الذي يجعلها المنصة المثالية للشركات على اختلاف أحجامها لحماية عملياتها.

"بلومبرغ" : تحالفا بيكتل وألستوم توصلا لحلول

السعودية تقترب من تسوية بمليارات الدولارات تسرّع مشروع مترو الرياض

تعتزم المملكة العربية السعودية تسوية نزاع مع شركات المقاولات والذي يحتمل أن تصل قيمته إلى عدة مليارات من الدولارات لحل نزاع بشأن مترو الرياض، ما يقرب المشروع خطوة نحو الاكتمال، وفقاً لما نقلته "بلومبرغ" عن مصادر، واطلعت عليه "العربية. نت".

وقالت المصادر، إن تحالفي بكتل غروب، وألستوم، من أصل 3 تحالفات، توصلا إلى اتفاق بشأن المدفوعات المتنازع عليها، فيما يقترب التحالف الثالث الذي يضم شركة Webuild SpA الإيطالية، من توقيع اتفاق قريباً.

كان المقاولون العاملون في المشروع يسعون للحصول على عدة مليارات من الدولارات في المجموع كمدفوعات من الحكومة، إذ طلبت شركة Bec – tel حوالي مليار دولار، حسبما أفادت بلومبرغ، ولكن شروط التسوية لم تكن واضحة.

ومع انتعاش أسعار النفط الخام هذا العام، تستعد السعودية لتسجيل أول فائض في الميزانية منذ سنوات.

ومنحت المملكة عقوداً تبلغ قيمتها حوالي 22 مليار دولار في عام 2013 لتطوير نظام المترو، الذي يشمل ما يقرب من 175 كيلومتراً من خطوط السكك الحديدية. وكان من المقرر الانتهاء من المشروع في عام 2019.

وتشمل الشركات الأخرى المشاركة في المشروع شركة Fomento de Construcciones Contratas SA الإسبانية وشركة WS Atkins Ltd.

ويعد استكمال مترو الرياض جزءاً مهماً من خطط ولي العهد الأمير محمد بن سلمان لمضاعفة حجم المدينة وتحويلها إلى مركز أعمال دولي، مع خفض الانبعاثات.

«إيكيا» تحتفل بالطعام الصحي والمستدام: الغذاء الجيد لحياة أفضل

لدى "ايكيا" رؤية تتمثل في أن تكون مصدر إلهام وتحفيز للجميع على إتباع أسلوب حياة يومية أفضل، وفق الشروط والمتطلبات التي تحافظ على البيئة والكوكب. تماشيا، وإلتزاما بهذه الرؤية، أخذت ايكيا على عاتقها أن يكون لها دورٌ مهمٌ في توفير حلول مُلهمة وجذابة يمكن أن تساعد أكبر عدد ممكن من الناس من العيش بصحة أفضل وبطريقة أكثر إستدامة.

أحد المجالات الرئيسية التي تُركز عليها ايكيا لتحقيق هذه الرؤية يرتبط بمبدأ إختيار الطعام الصحي والمُستدام.

يقول مدير ايكيا الكويت، السيد مرصاد العاجي، "تُعتبر ايكيا واحدة من أكبر مزودي المواد الغذائية في العالم. ومن هذا المنطلق اتخذنا خطوة كبيرة نحو الأمام باتجاه جعل الطعام الصحي والمُستدام متوفر للجميع وبأسعار معقولة ويلبي كافة الأذواق. ونحن نأمل في نكون مصدر إلهام للمزيد من الناس وتحفيزهم على تبني أسلوب حياة أكثر صحة وإستدامة، لذلك أضفنا إلى قائمة الطعام في جميع مطاعمنا خيارات جديدة كلها لذيذة وغنية بكل العناصر المغذية والصحية".

وفقاً لنتائج أبحاث علمية حديثة، هناك أكثر من 54٪ من الناس في جميع أنحاء العالم باتوا يولون أولوياتهم لتحقيق هدف العيش بطريقة جيدة وايجابية من الناحية الصحية ومن ناحية الحفاظ على البيئة في الوقت نفسه. وهناك كثير من الناس أصبحوا مقتنعين بأن التقليل من تناول اللحوم الحمراء والإكثار من تناول الفواكه والخضروات مفيد للصحة والبيئة.

وفي هذا الخصوص يضيف العاجي: "نحن في ايكيا قد بدأنا بالفعل خطوات بنّاءة في هذا الاتجاه. اليوم، الخيارات المتوفرة في قائمة الطعام لدينا غنية بالأطعمة النباتية والصحية ذات الطعم اللذيذ. ومؤخراً أضفنا كرات النبات H – VUDROLL ؛ وهي الخيار الأكثر إستدامة بالنسبة للعديد من محبي كرات اللحم، مع 4٪ فقط من البصمة المناخية التي تشكلها كرات اللحم التقليدية، وذلك من دون المساومة على المذاق أو الشكل أو العناصر المغذية".


«إيكيا» تحتفي بالغذاء الصحي والمستدام

وتابع العاجي: "هناك الكثير من الناس لا يزالون يعتقدون أن العائق الأكبر أمام إتباع أسلوب عيش بطريقة أكثر صحية ومُستدامة هو التكلفة الباهظة لمثل هكذا خيار. لكننا في ايكيا نؤمن بأن الخيارات الصحية والمُستدامة لا يمكن أن تكون ترفاً وحكراً على قلة من الناس، بل يجب أن تكون خياراً جذاباً للجميع، ومتوفرة بأسعار مقبولة تناسب الجميع". و"عندما بدأنا في إنتاج المزيد من المواد الغذائية النباتية، وتوفيرها بأسعار مقبولة للجميع، لم يكن هدفنا الأول الإستغناء عن اللحوم، بل كان الهدف الأساسي تقديم طعام لذيذ وصحي وأكثر إستدامة، يحبه الجميع ويلبي كافة الأذواق. ومن ما قاله مؤسس ايكيا، إنغفار كامبراد، ذات يوم: 'من الصعب العمل مع شخص على معدة فارغة'.. ففي نهاية اليوم، لن يرغب أي شخص بتناول أي شيئ غير لذيذ، حتى لو كانت كل شروط الإستدامة متوفرة فيه".

وختم العاجي، قائلاً: "أنا أدعو الجميع للإنضمام إلينا في ايكيا الأفينيوز لتذوق الأطعمة الجيدة والطعام الصحي والوصفات المختلفة المتأصلة في المطبخ السويدي. الطعام الجيد يستحق الاحتفال. الطعام الجيد يساعدنا دائماً في الحصول على حياة أفضل. ابدأ اليوم، اختر الطعام الصحي والمُستدام لكي تعيش حياة أفضل!!".