الدور المركزي للبرامج الضارة

الدور المركزي للبرامج الضارة

تطورت تقنيات الهجوم في الآونة الاخير كما اصبحت البرامج الضارة تلعب دورا رئيسيا في دورة حياة الهجوم حيث طور المهاجمون طرقا جديدة لتقديم البرامج الضارة مثل التنزيلات من محرك الاقراص , وإخفاء اتصالات البرامج الضارة (مع التشفير) ، وتجنب الاكتشاف التقليدي القائم على التوقيع وغيرها من الطرق الحديثة التي يستخدمها المهاجمون

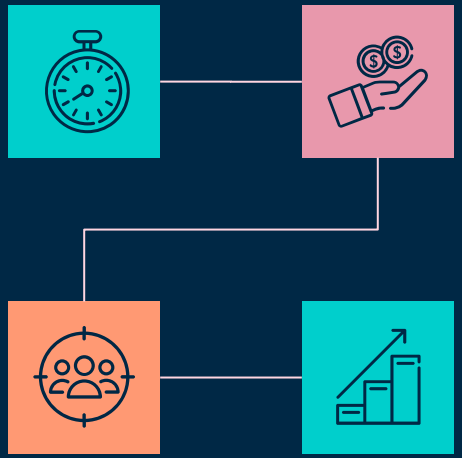
الدور المركزي للبرامج الضارة

البرامج الضارة الحديثة تشبه إلى حد ما حبة البازلاء في لعبة الصدف. يقوم محتال بإغراء الضحية لمحاولة تتبع البازلاء ، في حين أنه في الواقع تمرين في خفة اليد

لذا تعتمد دورة حياة التهديد الحديثة على خفة اليد - كيفية الإصابة والاستمرار والتواصل دون أن يتم اكتشافها

الدور المركزي للبرامج الضارة

كما إن نظرتنا التقليدية للبرامج الضارة وعادات الأمان القديمة تجعلنا نفكر في البرامج الضارة فقط, ولكن لفهم التهديدات الحديثة والتحكم فيها ومكافحتها بنجاح ، نحتاج إلى التركيز ليس فقط على البازلاء (البرامج الضارة) ولكن على جميع الأجزاء المتحركة أيضًا



APTs وأمن الأجهزة المحمولة

APTs وأمن الأجهزة المحمولة

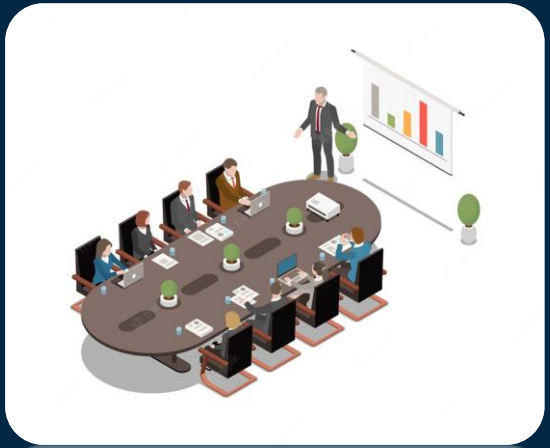
مع الاستخدام المتزايد للأجهزة المحمولة في المؤسسة ، اصبح المهاجمون يستخدمون الأجهزة المحمولة بشكل متزايد كجزء من هجماتهم .
الأمر المثير للاهتمام هو أن مجموعة الخدمات التي يوفرها الجهاز المحمول تجعل الجهاز مفيدًا جدًا لأجزاء متعددة من دورة حياة الهجوم.

على سبيل المثال ، يمكن للمهاجم استخدام جهازه المحمول للاستطلاع. ، والوصول إلى شبكات متعددة ، والقدرة على إعادة برمجة وظائفه الأساسية ، يمكن أن يكون الجهاز المحمول أداة فعالة للغاية للمراقبة

APTs وأمن الأجهزة المحمولة

يمكن استخدام البرامج الضارة للأجهزة المحمولة لإصابة الجهاز المحمول نفسه ،علي سبيل المثال الهجوم الاخير الذي نُفذت ضد الحاضرين في مؤتمر سياسي حيث تم ارسل قطعة من برامج Android الضارة متخفية كأداة لإجراءات المؤتمر. بمجرد التثبيت ، ذهب البرنامج الضار بعد قائمة جهات اتصال الجهاز لاكتساب معرفة أكبر بشبكة الحاضر.

الجهاز المحمول المُخترق قادر أيضًا على تنفيذ المزيد من الهجمات بمجرد أن يثبت وجوده داخل الشبكة المستهدفة ، يسمح للبرامج الضارة بالعمل بشكل جانبي ضد الأجهزة الأخرى وجمع المعلومات الاستخباراتية على الشبكة المستهدفة



وأمن الأجهزة المحمولةAPTs

ليس الجهاز المحمول فقط هو القناة للهجوم الجانبي ، ولكن في بعض الأحيان يكون الجهاز نفسه هو الهدف أيضًا. في يناير 2014 ، اكتشفت Kaspersky Labs هجوم APT واسع النطاق يسمى Red Octobe حيث حدث هجوم البرمجيات الخبيثة على أجهزة كمبيوتر سطح المكتب الخاصة بالموظف ولكن تم نقله بشكل جانبي لسرقة البيانات من الأجهزة المحمولة في المؤسسة ، وبالتالي توفير معلومات حول جهات اتصال المستخدمين

البرامج الضارة للأجهزة المحمولة في العالم الحقيقي : Dplug

البرامج الضارة للأجهزة المحمولة
في العالم الحقيقي : Dplug

في عام 2013 ، اكتشف باحثو Palo Alto Networks نوعًا جديدًا من البرامج الضارة للجوال (Android Package File (APK تسمى Dplug.

تشكل هذه البرامج الضارة بمثابة تطبيق أداة نظام لتنظيف الذاكرة .
يستخدم Dplug الرسائل القصيرة لاختطاف المعرفات الفريدة للجهاز والاشتراك في الخدمات المميزة وإخفاء هذا السلوك عن المستخدم عن طريق حظر إشعارات الخدمة المتميزة.

تحدث جميع سلوكيات الهجوم في الخلفية .لن يشعر المستخدم بأي شيء يتعلق بالاشتراك في الخدمة حتى استلام الفاتورة الشهرية

Do you have any questions?

THANKS