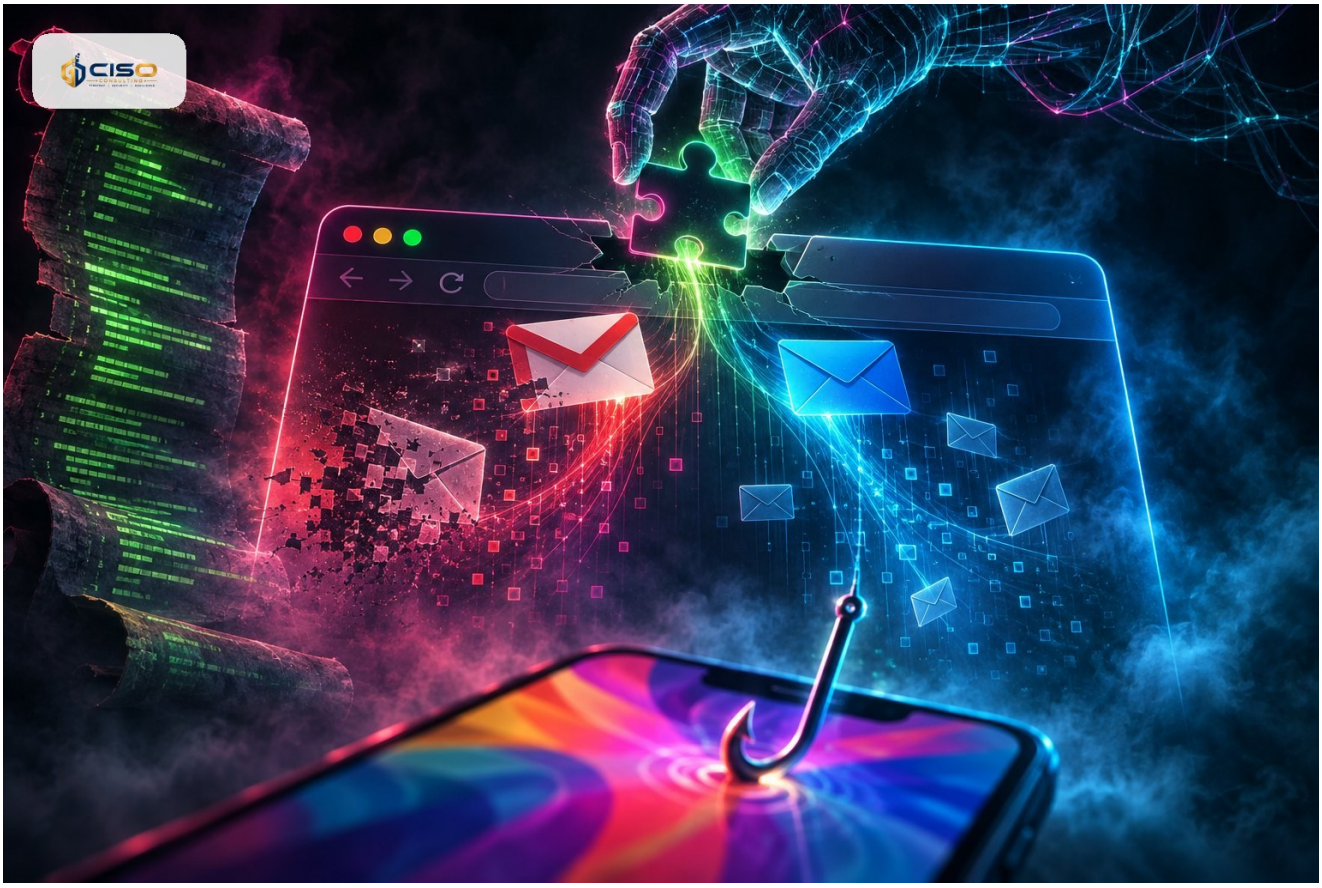
برمجية SYS010 تستغل سياسات إدارة المتصفحات للتجسس على Gmail وOutlook



رصدت Bitdefender نسخة جديدة من SYS01 باسم SYS010 تنتشر عبر إعلانات Meta لتطبيقات خلفيات مزيفة، وتفرض تثبيت إضافات متصفح عبر سياسات الإدارة لسرقة الجلسات وقراءة بريد Gmail وOutlook أو حذفه.

- تروّج إعلانات Meta الخبيثة لتطبيقات مزيفة تنتحل Wallpaper Engine وLively Wallpapers على Windows، وتعمل الخلفيات فعلًا بينما تُثبَّت البرمجية الخبيثة في الخلفية.
- تسجّل البرمجية متصفح Chrome في وحدة إدارة Google يتحكم بها المهاجم، وتستخدم سياسة ExtensionSettings في Firefox، ويمكنها تسجيل أجهزة Edge في خادم MDM يتحكم به المهاجم.
- تكرر نافذة UAC كل ثلاث ثوانٍ حتى 99 مرة إلى أن يوافق المستخدم.
- تسرق الإضافات ملفات تعريف الارتباط الخاصة بالجلسات فتتجاوز كلمات المرور والتحقق الثنائي،

وتستطيع إضافة Chrome قراءة رسائل Gmail وOutlook وحذفها نهائياً.

- تشير Bitdefender إلى أن أعداد الطلبات حسب الدولة لا تعني إصابات مؤكدة.

وصفت Bitdefender Labs حملة تتابعها باسم SYS010، يُرجَّح أنها نسخة جديدة من برمجية سرقة المعلومات SYS01 التي رُصدت في إعلانات فيسبوك الخبيثة منذ عام 2022 على الأقل. وقد حدد الباحثون إعلاناً خبيثاً في 16 أكتوبر ووجدوا أن الحملة ما زالت مستمرة مع إنشاء مئات الإعلانات.

كيف يتم الهجوم

تنتحل الإعلانات تطبيقي Wallpaper Engine وLively Wallpapers وتوجّه مستخدمي Windows إلى مواقع تنزيل خبيثة، بعضها بنطاقات تبدو رسمية. ويوفّر التطبيق المثبّت الخلفيات المتحركة الموعودة، مما يخفي النشاط الخبيث.

ثم يعدّل سكربت سياسات إدارة المتصفحات لفرض تثبيت إضافات في Chrome وEdge وFirefox. وتتطلب هذه التغييرات صلاحيات المسؤول، فتعرض البرمجية نافذة UAC كل ثلاث ثوانٍ حتى 99 مرة إلى أن يوافق المستخدم. وبعد التثبيت لا يستطيع المستخدم تعطيل الإضافات أو إزالتها.

ما الذي يتعرض للخطر

تتنكر الإضافات في هيئة أدوات مستندات وتُوزَّع خارج متجر Chrome الإلكتروني. وهي تسرق ملفات تعريف الارتباط الخاصة بالجلسات، فيصل المشغّل إلى الحسابات المسجّلة دون كلمات مرور أو تحقق ثنائي. كما تجمع بيانات صفحات فيسبوك والحسابات الإعلانية وحسابات الأعمال، ومنها الإنفاق وبيانات الدفع. وتستطيع إضافة Chrome قراءة أحدث رسائل Gmail وOutlook وحذف رسائل مختارة نهائياً، وقد يتيح ذلك اعتراض رموز الدخول وإزالة تنبيهات الأمان.

وتؤكد Bitdefender أن أعداد الطلبات حسب الدولة ليست إصابات مؤكدة. أما على الشركات، فقد يعني سرقة الحسابات الإعلانية رسوماً إعلانية غير مصرّح بها، وفقدان الوصول إلى حسابات التواصل الاجتماعي، وانكشاف محادثات العملاء.

ما يجب فعله الآن

1. افحصوا أجهزة Windows المُدارة وغير المُدارة بحثاً عن تسجيل غير متوقع في إدارة المتصفحات، مثل رسالة «managed by your organization» لم تضبطها إدارة التقنية.
2. راجعوا سياسات Chrome وEdge وFirefox بحثاً عن إضافات مفروضة التثبيت لم تعتمدوها، خصوصاً إضافات أدوات المستندات المثبّتة من خارج المتاجر الرسمية.
3. قيّدوا تثبيت البرامج القادمة من إعلانات وسائل التواصل، ودرّبوا الموظفين على رفض نوافذ UAC غير المبررة.
4. راجعوا من يملك صلاحية الوصول إلى حسابات Meta للأعمال والإعلانات في المنشأة، وأزيلوا الصلاحيات غير اللازمة، وتحققوا من الإعلانات غير المألوفة أو تغيّر وسائل الدفع أو الإنفاق.
5. عند الاشتباه بإصابة، ألغوا الجلسات النشطة وأعيدوا تعيين بيانات الدخول للبريد وحسابات الأعمال من جهاز سليم، وراجعوا صناديق البريد بحثاً عن تنبيهات أمنية محذوفة.