تقرير FortiGuard: أكثر من 4,400 نطاق خبيث تستهدف متسوقي موسم الأعياد



رصدت FortiGuard Labs أكثر من 24,000 نطاق جديد بطابع التسوق خلال 90 يومًا، منها أكثر من 4,400 خبيث، إلى جانب تداول بيانات دخول متاجر مسروقة وثغرات تجارة إلكترونية.

- رُصد أكثر من 24,000 نطاق جديد مرتبط بالتسوق خلال 90 يومًا، صُنّف منها أكثر من 4,400 نطاق على أنه خبيث.
- شكّلت مصطلحات التوصيل والشحن 34.88% من النطاقات، وهي أكثر المواضيع شيوعًا.
- جُمع نحو 1.72 مليون سجل من البرمجيات الخبيثة سارقة المعلومات مرتبط بسبع منصات تجارة إلكترونية من سوق روسي بين أغسطس وأكتوبر 2026.
- تعلن المنتديات السرية عن أدوات تصيّد يُزعم تجاوزها للمصادقة متعددة العوامل، وخدمات احتيال الاسترداد، ووصول إلى مواقع Magento وPrestaShop وWordPress وOpenCart.
- وجدت أبحاث Doppel أن نحو صفحة من كل أربع صفحات مزيفة لـ Black Friday استُضيفت على

> منصات مشروعة مثل Google Sites وBlogger وGitHub Pages.

يصف تقرير FortiGuard Labs حول تهديدات موسم الأعياد 2026 منظومة إجرامية تستعد لموسم التسوق عبر متاجر وهمية، وانتحال هوية تجار التجزئة، واحتيال الدفع، والاستيلاء على الحسابات.

أبرز ما توصل إليه الباحثون

خلال 90 يومًا رصد الباحثون أكثر من 24,000 نطاق مسجّل حديثًا يحمل كلمات مرتبطة بالتسوق الموسمي، صُنّف منها أكثر من 4,400 نطاق على أنه خبيث. وكانت مصطلحات الطرود والتوصيل والشحن الأكثر حضورًا بنسبة 34.88%، مع رصد نطاقات تشير إلى DHL وUPS وFedEx وUSPS. وقد تطلب هذه المواقع بيانات الدفع بحجة تعذّر التسليم أو رسوم جمركية.

وأشارت أبحاث Doppel المنفصلة إلى أن أغلب صفحات Black Friday المزيفة المؤكدة تستخدم عناوين لا تشبه العلامة المنتحلة، وأن نحو صفحة من كل أربع صفحات مشابهة استُضيفت على منصات مشروعة مثل Google Sites وBlogger وGitHub Pages.

بيانات مسروقة وخدمات سرية

بين أغسطس وأكتوبر 2026 جمع الباحثون نحو 1.72 مليون سجل من البرمجيات سارقة المعلومات مرتبطة بسبع منصات تجارة إلكترونية، منها نحو 1.49 مليون لمنصة Amazon. وقد تتيح ملفات تعريف الارتباط المسروقة اختطاف الجلسات بحسب صلاحيتها وضوابط المنصة.

كما تعلن المنتديات عن خدمات تصيّد بالاشتراك، وأدوات فحص البطاقات، وأدوات تصيّد يُزعم تجاوزها للمصادقة متعددة العوامل، وخدمات استرداد مبالغ احتيالية، وانتحال هوية المتصل، ورسائل SMS والبريد الجماعي، ووصولاً إلى أنظمة التجار. وتشير إعلانات ثغرات مزعومة في Magento وPrestaShop وWordPress وOpenCart إلى مخاطر تعديل صفحات الدفع وحقن شيفرات سرقة بيانات البطاقات واستخراج قواعد بيانات العملاء. ويستكشف المجرمون أيضًا الذكاء الاصطناعي لتخصيص الرسائل وإنتاج شهادات وإعلانات مزيفة.

الصلة بالمملكة

لا يتناول التقرير المملكة العربية السعودية، لكن الأساليب المذكورة تنطبق على أي متجر أو بنك أو جهة مصدرة للبطاقات يتسوق عملاؤها عبر الإنترنت خلال الحملات الموسمية.

ما يجب فعله الآن

1. راقبوا النطاقات المسجلة حديثًا والصفحات الاجتماعية التي تقلّد علامتكم أو شركاء التوصيل، وقدّموا طلبات إزالة سريعة.
2. نبّهوا العملاء والموظفين إلى التحقق من رسائل التوصيل والاسترداد والخصومات عبر التطبيقات الرسمية لا الروابط.
3. حدّثوا منصات التجارة الإلكترونية مثل Magento وPrestaShop وWordPress وOpenCart، وراقبوا صفحات الدفع بحثًا عن أي تغيير غير مصرح به في الشيفرات.

4. عزّزوا الحماية من الاستيلاء على الحسابات: مصادقة متعددة العوامل مقاومة للتصيّد، وانتهاء الجلسات، وكشف الشذوذ في الدخول واستخدام بيانات الدفع المخزنة.
5. راجعوا إجراءات الاسترداد والإرجاع ودعم العملاء تحسبًا لهجمات الهندسة الاجتماعية، بما فيها انتحال هوية المتصل.
6. افحصوا مصادر التسريبات الخاصة بالبرمجيات سارقة المعلومات بحثًا عن بيانات الموظفين والعملاء، وأعيدوا تعيين كلمات المرور عند العثور عليها.