مؤسسة النقد العربي السعودي

Saudi Arabian Monetary Agency

الرسائل الاقتحامية و آثارها على القطاع المصرفي السعودي

صقر العرابي الحارثي
مسئول امن المعلومات

الرسائل الاقتحامية و آثارها على القطاع المصرفي السعودي

- أنواع الرسائل الاقتحامية (Spam)
- الاستدراج (Phishing)
- حجم المشكلة
- إستراتيجيات الحد من أضرارها

الرسائل الاقتحامية كوسيلة للغش التجاري (Fraud)

- تستخدم الرسائل الاقتحامية (Spam) كوسيلة لنقل أدوات الهجمات.
- تستخدم الرسائل الاقتحامية كوسيلة لإيجاد الأهداف الممكن خداعها للقيام بعمليات مصرفية.
- و تشمل:
  - الخدع العاطفية - المهرجانات – الكوارث الطبيعية.
  - الحصول على نسبة من إجراء عمليات مصرفية.
  - إعطاء مكافأة للرد على بريد إلكتروني .
  - خدعة "أنت الفائز" لقرعة لم تشترك بها.

أنواع الرسائل الاقتحامية و تأثيرها على القطاع المصرفي

للرسائل الاقتحامية أهداف و نواتج عديدة النقاط التالية تبين المحاور الرئيسية التي تتعلق بالقطاع المصرفي:

- توصيل برامج التجسس حصان الطراودة (Trojans).
- العثور على وسائل لنقل الأموال (Money Mules).
- عروض تجارية زائفة (Fraud).
- الاستدراج (Phishing).

توصيل أحصنة الطراودة (Trojan)

- **تكوين الرسائل الاقتحامية**

تثبيت خوادم (SMTP) لإرسال الرسائل الاقتحامية (Spam).

- **تسجيل ضربات لوحة المفاتيح.**
- **التسجيل عن طريق أحصنة الطراودة.**

تقوم أحصنة الطراودة بتسجيل ضربات لوحة المفاتيح لمواقع المصارف و من ثم إرسال تلك البيانات الى المهاجم عن طريق البريد الإلكتروني.

- جمع عناوين البريد الإلكتروني (Directory Harvesting)

و يحصل فيها اكتشاف عناوين البريد الإلكتروني من قبل المهاجمين.

توصيل الأموال عن طريق "Money Mules"

- بريد إلكتروني يقدم للمستلم عرض وظيفي جذاب.
- تكون العروض مقدمة من قبل شركات وهمية للإشتراك في عمليات تحويل نقدية و يحصل فيها المشترك على ١٥ – ٢٠ % من المبالغ المحولة.
- يطلب مقدم الوظيفة معلومات عن الحساب الشخصي للموظف.
- يستلم الـ "Money Mules" الأموال في حساباتهم الخاصة ليقوموا بتحويلها الى حسابات تكون غالبا في إفريقيا أو روسيا أو أمريكا الجنوبية.
- الغرض من استخدام الـ "Money Mules" هو:
  - تحويل الأموال من حساب مسروق.
  - غسيل الأموال.

عروض تجارية زائفة (Fraud)

- الاحتيال النيجيري ٤١٩ (419 Nigerian Fraud)
  - ويعتبر من أقدم عمليات الاحتيال المالية بدأ في الثمانينات عن طريق الرسائل البريدية ثم عن طريق الفاكسات و اليوم عن طريق البريد الإلكتروني.
  - يطلب من مستقبل الرسالة الاشتراك في تحصيل مبلغ مالي ضخم بحجة أن المبلغ مجمد في أحد الدول الإفريقية و سيكون له نصيب منها.
  - ثم يطلب منه القيام بدفع رسوم (أو هدايا) لتحرير الأموال.
  - الى اليوم، هناك العديد من الأشخاص الذين يقعون كضحايا لاحتيالات كهذه.
- طلبات التصدير الضخمة (Large Export Orders)
  - و هي عبارة عن بريد إلكتروني يحتوي على عرض تجاري في مجال التصدير.
  - تظهر هذه العملية للمستلم انها عرض تجاري ضخم.
  - يطلب من المستلم القيام بدفع الرسوم الجمركية بحجة الشحن.

الاستدراج (Phishing)

الاستدراج هو عملية احتيالية لمحاولة سرقة معلومات العميل السرية (الرقم السري واسم المستخدم) عن طريق تزوير صفحات البنوك في الانترنت لاستخدامها:

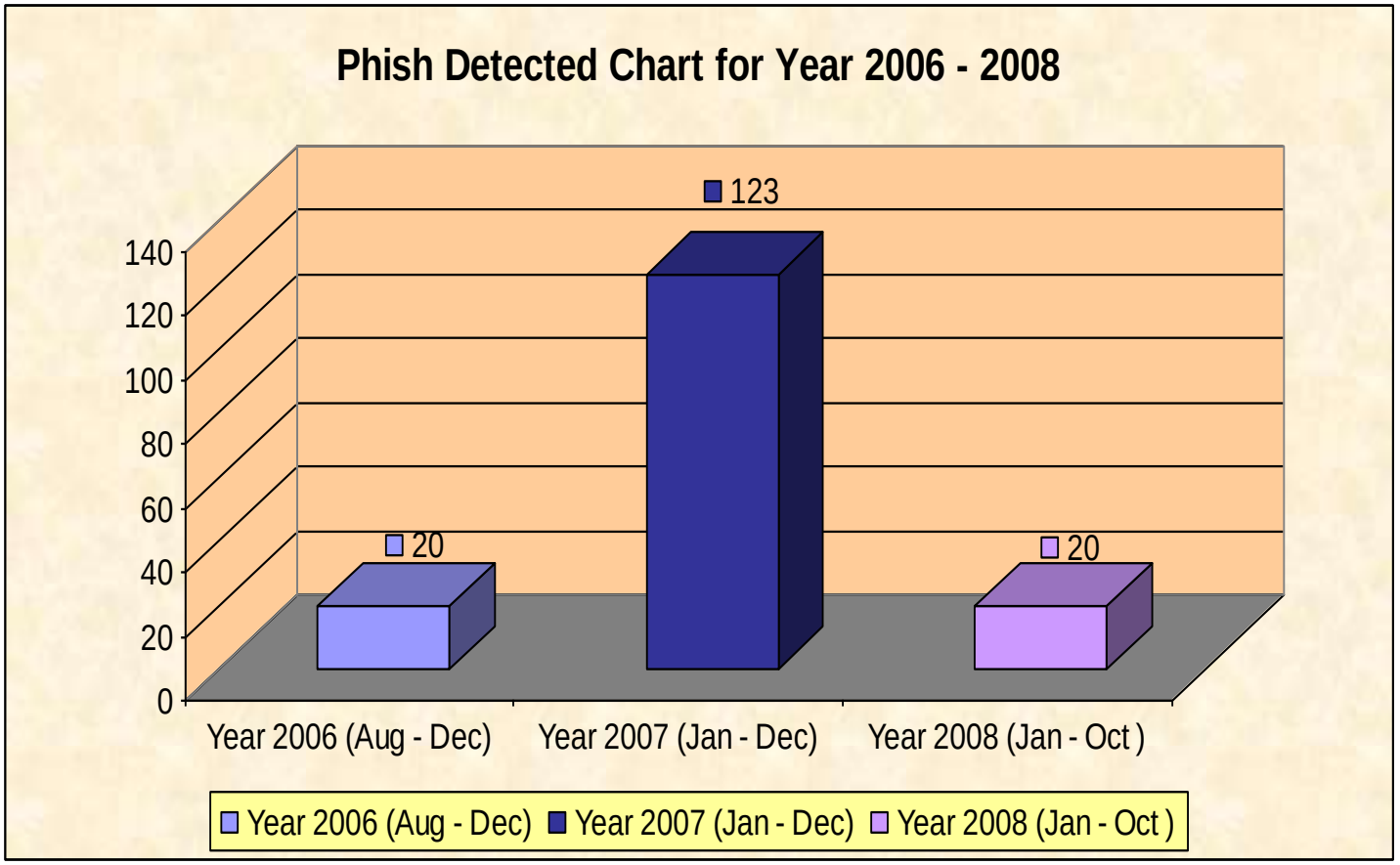
- للتحويل النقدي الغير شرعي
- للمشتر وات عبر الإنترنت

حجم المشكلة

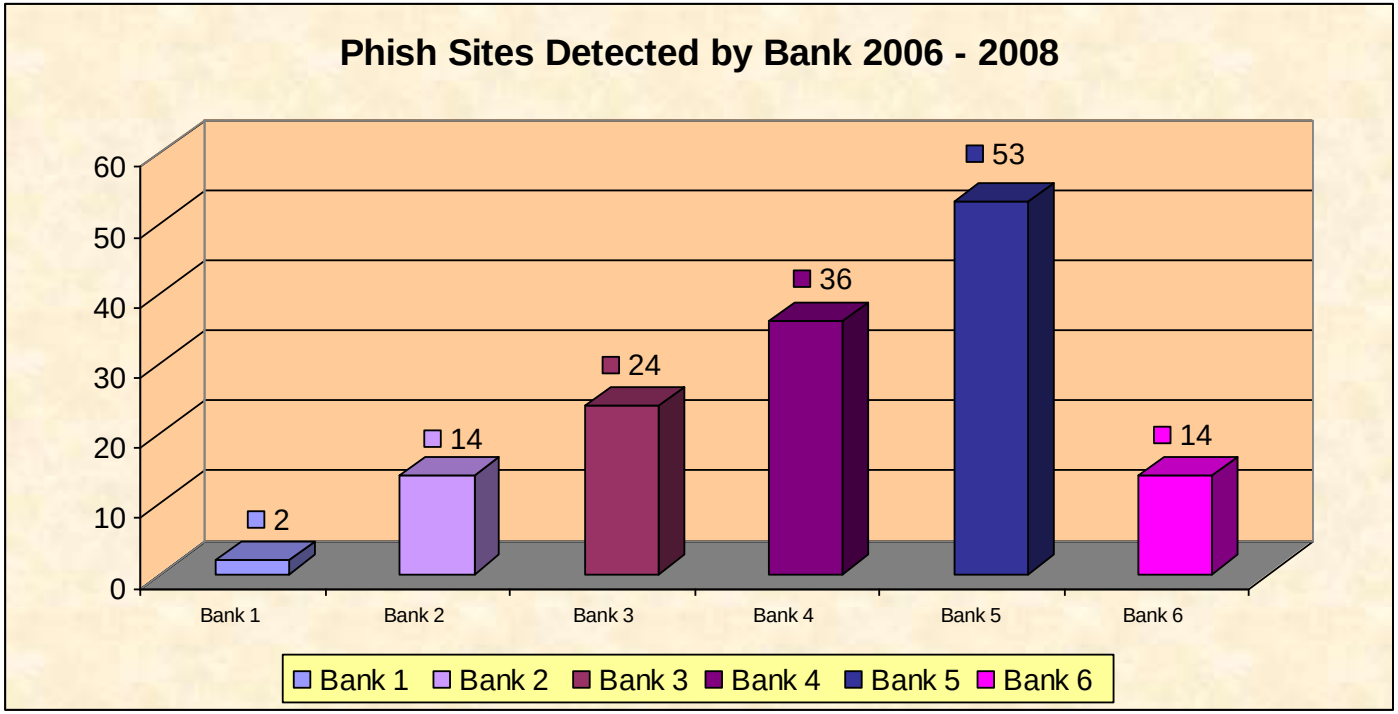
مقارنة لهجمات الاستدراج في البنوك الامريكية تبعا لإحصائيات شركة (Mark Monitor)

Month	2006	2007
January	1,482	11,878
February	1,933	7,044
March	3,062	11,771
April	2,983	15,488
May	2,215	16,648
June	2,611	18,035
July	2,326	15,359
August	2,582	25,016
September	4,411	16,699
October	3,632	14,162
November	2,470	12,474
December	7,851	11,510
Total	**37,828**	**176,084**

عدد هجمات الاستدراج التي استهدفت المصارف المحلية



توزيع هجمات الإستدراج للمصارف المحلية



محذوف

محذوف

محذوف

محذوف

إستراتيجيات الحد من الأضرار

- جهود لجنة مدراء أمن المعلومات في مؤسسة النقد العربي السعودي والبنوك SMC.
- الجهود التوعويه Awareness لتجنب الوقوع كضحايا لمثل هذه الهجمات.
- إيقاف الرسائل الاقتحامية Spam بالوسائل التقنية.
- مكافحة الاستدراج Phishing بحيث تجعل من نفسك هدفا صعبا للمستدرجين

لجنة مدراء امن المعلومات

SAMA & Banks Security Managers Committee (SMC)

- تبادل الخبرات في مجال أمن المعلومات بين البنوك و المؤسسة .
- تبادل المعلومات عن مخاطر التقنية الشائعة و تحذيرات أمن المعلومات ونقاط الضعف في أنظمة أمن المعلومات.
- ضمان التوافق مع توجهات المؤسسة الخاصة بأمن المعلومات.
- زيادة التوعية بأمن المعلومات في البنوك (لموظفيها وعملائها).
- تنظيم وضمان التدريب الأمني الملائم وتقديمه لمسئولي أمن المعلومات في مؤسسة النقد وجميع البنوك.

لجنة مدراء أمن المعلومات
المبادرات

- دراسة تعاونية على مراكز تشغيل أمن المعلومات SOC.
- المؤتمر الأول لأمن المعلومات القطاع المصرفي السعودي .
- تطوير إجراءات إدارة حوادث أمن المعلومات.
- إقامة دورات و وُرش عمل في أمن المعلومات.
- الحملة الوطنية للتوعية بأمن المعلومات والتي تستهدف كافة عملاء البنوك.

التوعية (Awareness)

- قامت المؤسسة بالطلب من جميع المصارف المحلية بالقيام بوضع برنامج لتوعية الموظفين و العملاء.
- قامت المصارف بوضع برامج للتوعية، و تحسن هذه البرامج بشكل مستمر.
- تقوم لجنة مدراء أمن المعلومات في المؤسسة والبنوك (SMC) بدراسة برنامج للتوعية على المستوى الوطني.

إيقاف الرسائل الاقتحامية في المصارف بالوسائل التقنية

- لحماية موظفي المصارف، قامت جميع المصارف بـ:
  - تثبيت حلول منع الرسائل الاقتحامية.
  - تثبيت حلول شاملة لمكافحة الفيروسات و أحصنة الطراودة.
  - تثبيت الجدران النارية و حلول كشف التسلل (IDS) للتقليل من أحصنة الطراودة التي تنشر الرسائل الاقتحامية.

مكافحة الاستدراج (Phishing)

- **الجهود و التنسيق المحلي لاكتشاف هجمات الاستدراج للحد منها بالتنسيق مع هيئة الاتصالات و تقنية المعلومات ومع أحدي شركات امن المعلومات:**
  - تم تثبيت "Honey Pots" لكشف مواقع الإستدراج.
  - تك الطلب من موفري خدمات الإنترنت (ISP) بضرورة التعاون مع هذه الجهودً لتحليل مجموعات من الرسائل الاقتحامية و إستخراج مواقع الاستدراج.
  - نشرات الاستدراج المحلية: يتم إخبار موفري خدمات الإنترنت المحليين فور اكتشاف مواقع استدراج لإغلاق هذه المواقع لحماية المستخدمين على المستوى الوطني.
  - ترويج فكرة "نشرات الاستدراج المحلية" على مستوى دول مجلس التعاون الخليجي.

مكافحة الاستدراج (Phishing)

- قامت جميع المصارف في المملكة التي تقدم خدمات مصرفية على الإنترنت بتطبيق إستراتيجية لمكافحة الاستدراج :
  - نظام الإنذار المبكر:
    - مراقبة يومية للمواقع الشبيهة.
    - الوصول لأكبر قاعدة بيانات لمالكي المواقع (Who Is Database)
    - مراقبة ٢٤*٧ للمواقع المشبوهة.
  - التواصل مع شركات مكافحة الاستدراج العالمية و التي تقوم بتحليل الرسائل الاقتحامية من (Hotmail) و (Yahoo) لاكتشاف مواقع الاستدراج.
  - نشرات الاستدراج: موفري برامج مستكشف الإنترنت يقومون بإغلاق مواقع الاستدراج على مستوى المستكشف (على مستوى المستخدمين).

الخلاصة

- الرسائل الاقتحامية تلعب دور رئيسي في عمليات الإحتيال.

- من الضروري معالجة هذه المسألة على المستوى الوطني وذلك بتنسيق الجهود مع كل من:
  - هيئة الاتصالات و تقنية المعلومات
  - مركز المعلومات الوطني
  - موفري خدمات المعلومات و الإنترنت (DSPs and ISPs)
  - مؤسسة النقد العربي السعودي (المصارف و شركات الاستثمار)
  - الدول المجاورة (دول مجلس التعاون).

التوعية

Awareness

مؤسسة النقد العربي السعودي

Saudi Arabian Monetary Agency

شكراً لكم