باللغة العربية

SAC 028

التقرير الاستشاري لـ SSAC

حول الهجمات الخداعية التي تنتحل صفة المُسجل

ملاحظة حول الترجمات

كُتبت النسخة الأصلية لهذه الوثيقة باللغة الإنجليزية، وهي متاحة على http://www.icann.org/committees/security/sac028.pdf. وأينما وجد اختلاف في المعنى أو ما يوهم أنه اختلاف في المعنى بين هذه الوثيقة والنص الأصلي، فسيكون النص الأصلي هو السائد.

تقرير استشاري صادر عن
اللجنة الاستشارية للأمان والاستقرار (SSAC)
التابعة لـ ICANN
مايو 2008

مقدمة

يصف هذا التقرير الاستشاري أحد أشكال الهجمات الخداعية التي تستهدف مسجّلو نطاقات اسم النطاق. حيث ينتحل المعتدي صفة مُسجل اسم نطاق ويقوم بإرسال مراسلات متوقعة أو مرتقبة إلى عميل المُسجل (مسجّل النطاق) تتعلق بنواحٍ ذات صلة باسم النطاق. وتتضمن أمثلة المراسلات المتوقعة إخطاراً بانتهاء فترة تعليق تسجيل اسم نطاق أو بريد إلكتروني للترقية أو إخطار لإخبار مسجّل النطاق بحدوث مشكلة في إدارة الحساب أو -بشكل عام- أية مراسلات تتطلب الانتباه الفوري للعميل أو تُشجّعه. ومع ذلك، فإن هذه المراسلات تكون مزيفة. حيث يقوم المخادع بإنشاء موقع ويب يكون مشابهاً بشكل مخادع للموقع الخاص بالمُسجل لحث العميل على الدخول إلى حساب إدارة النطاق الخاص به ثم يقوم بدون قصد بكشف بيانات اعتماد حسابه للمخادع. ويقوم المخادع باستخدام بيانات المستخدم التي تم جمعها للدخول إلى سندات اسم نطاق العميل وتغيير معلومات DNS الخاصة باسم/بأسماء النطاق الموجود/الموجودة في هذا الحساب واستخدام النطاقات للتحريض على ارتكاب المزيد من الهجمات.

وفي هذا التقرير الاستشاري، تصف SSAC أشكالاً عامة لهذا النوع من الهجوم. ونراعي أنواع وتنسيقات المعلومات المضمنة في رسائل البريد الإلكتروني القانونية التي يستخدمها المُسجلون المختلفون عند تبادل الرسائل مع العملاء. كما نناقش كيفية تلاعب المخادعين بأنواع وتنسيقات هذه المعلومات لإنشاء مراسلات مزيفة تم وضعها ليتم تحريض عميل المُسجل من خلال أسلوب *الهندسة الاجتماعية*[1] على زيارة موقع ويب خاص بالمُسجل المزيف. ويقوم المعتدي بتصميم موقع الويب المزيف لخداع العميل حتى يقوم بكشف الأسماء وبيانات الاعتماد الخاصة بحساب إدارة النطاق. ونناقش بعض الممارسات الموصى بها حالياً لتخفيض الهجمات الخداعية التي يتم توظيفها بواسطة أهداف الخداع العامة مثل المؤسسات المالية والشركات الكبيرة أو منعها. ونوصي ببعض الإجراءات التي يستطيع المُسجلون اتخاذها حتى تكون مراسلاتهم مع مسجّلي النطاق أقل "قابلية للخداع" كما نحدد طرقًا لمسجّلي النطاق لاكتشاف هذا الشكل من أشكال الخداع وتجنب الوقوع ضحية له.

[1] للحصول على مزيد من المعلومات حول الهندسة الاجتماعية، انظر *سبب عمل الخداع*، http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf

خلفية: تحليل الهجوم

يقوم المخادعون باستغلال العديد من أشكال مراسلات البريد الإلكتروني التي تقوم الشركات الجارية أو المالية بإرسالها إلى العملاء[2]. كما يستخدم المُسجلون أيضًا البريد الإلكتروني في العديد من أنواع المراسلات المتعلقة بتسجيل اسم النطاق، بما في ذلك:

- إخطارات تجديد اسم النطاق
- تأكيدات طلب اسم النطاق
- تأكيدات طلب التسجيل
- تأكيدات تعديل معلومات النطاق
- رسائل تذكير دقة بيانات WHOIS
- إخطارات انتهاء فترة صلاحية اسم النطاق أو إلغائه
- رسائل الترقية والإعلان عن خدمات وميزات (جديدة)

ويقوم المخادعون باستغلال حقيقة اعتماد المُسجلين على مراسلات البريد الإلكتروني. ومن خلال انتحال (خداع) صفة المُسجل في هجوم خداعي، يكون المخادع قادرًا على إغراء عميل المُسجل لزيارة نسخة مزيفة من صفحة تسجيل الدخول الخاصة بعميل المُسجل، حيث قد يقوم العميل بدون قصد بكشف بيانات اعتماد الحساب للمعتدي. وتوفر بيانات الاعتماد هذه دخولاً غير مُصرح به للمخادع إلى حساب إدارة اسم النطاق. ويحتوي الحساب على عدد من الأصول ذات القيمة بالنسبة للمعتدي:

- عمليات تسجيل نطاق العميل والتي يمكن تعديلها لأهداف ضارة (انظر خريطة التهديد)
- استخدام (بشكل محتمل) بطاقات الائتمان أو أشكال الدفع الأخرى في ملف مُرسل إلى المُسجل والتي يمكن استخدامها لشراء نطاقات إضافية وبالتالي، يمكن استخدامها لأهداف ضارة.

ويقوم المخادعون بجمع المعلومات من العديد من المصادر لارتكاب هجوم انتحال صفة المُسجل. ويقومون بنسخ الصفحات والصور والشعارات والملفات الضرورية لإنشاء نسخة يمكن تصديقها -وإن كانت مزيفة- لصفحة تسجيل الدخول الخاصة بالمُسجل من موقع الويب "الموثوق" الخاص بالمُسجل. وتتم استضافتها على خادم ويب يتم تشغيله بواسطة المخادع ويتم استخدامه لإنشاء صفحة مزيفة من صفحة تسجيل الدخول الخاصة بالمُسجل. كما يستخدم المخادع المعلومات التي يتم التقاطها من المراسلات العادية للمُسجل مع العملاء لـ "تخصيص" الرسالة التي يقوم بتضمينها في البريد الإلكتروني المخادع. ويمكن الحصول على المراسلات ببساطة من خلال كونك مسجّل نطاق للمُسجل المستهدَف. ويستخدم المخادع معلومات WHOIS لإضفاء مزيد من التخصيص على الرسائل المخادعة، والأمر الأكثر أهمية هو أن المخادع قادر على استخدام معلومات WHOIS لإنشاء قائمة بالمستلمين الذين هم مسجّلو نطاق للمُسجل المستهدَف.

استغلال المعلومات التي يتم جمعها من مراسلات المُسجل

في المراسلات العادية، قد يقوم بعض المُسجلين بتضمين معلومات مشتقة من تسجيل اسم النطاق. وقد تتضمن هذه المعلومات معلومات تسجيل دخول (هوية) العميل وحساب العميل وأرقام التعاملات التجارية أو إيصال الاستلام. ويقوم بعض المُسجلين بتضمين معلومات جهة الاتصال ومكتب الدعم الخاصة بالعملاء، بما في ذلك أرقام الهاتف وعناوين البريد الإلكتروني وعناوين URL (الروابط التشعبية). ويقوم بعض المُسجلين الذين يستخدمون رسائل البريد الإلكتروني التي تعتمد على صيغة HTML بتضمين شعارات الشركة وإعلانات اللافتات ورسوم "التصنيف".

ويستطيع المعتدون استغلال حقيقة أن هؤلاء المُسجلون يقومون بتضمين هذه المعلومات عند قيامهم بإنشاء رسائل البريد الإلكتروني المخادعة التي تستهدف عملاء هؤلاء المُسجلين. فعلى سبيل المثال، يستطيع المخادع

[2] يمكن العثور على أمثلة تقارير الخداع وعمليات الاحتيال على أرشيف الخداع الخاص بمجموعة عمل مكافحة الخداع (http://www.apwg.org/phishing_archive/phishing_archive.html) وMillersMiles.co.uk (http://www.millersmiles.co.uk/archives.php).

تضمين حساب العميل وأرقام التعاملات التجارية *لتخصيص* الرسالة، كما هو مثبت في مضمون رسالة المثال التالي الخاصة بالنص الصريح لرسالة البريد الإلكتروني الافتراضية:

نشكرك على طلبك
الأربعاء، 19 أكتوبر، 2005 الساعة 5:18:34 صباحًا

عزيزي العميل،

نشكرك على تقديم طلب شراء من <registrar>. وفيما يلي تفاصيل تعاملك الأخير معنا. والرجاء حفظ هذه المعلومات للرجوع إليها في المستقبل.

رقم العميل: 123456789
اسم تسجيل الدخول: mumbledyfoodle
رقم الإيصال:3340-298884
القيمة الإجمالية للطلب: 19.99$
خدمة العملاء:1234-555-800

يجب عليك تسجيل الدخول إلى حسابك لإكمال هذا التعامل التجاري. والرجاء زيارة رابط التأكيد التالي على الموقع http://www.<registrar>.tld/login

في هذا الهجوم الافتراضي، يكون عنوان http://www.registrar.tld/login URL حقيقة عبارة عن رابط تشعبي موجود في رسالة البريد الإلكتروني حيث سيقوم بتحويل الضحية أو توجيهها إلى مضيف مختلف، على سبيل المثال، قد تبدو علامة HTML المضمنة في البريد الإلكتروني حول http://www.registrar.tld/login على الشكل

<a
href="http://stealyourdomainthisway.tld">http://www.registrar.tld/login

وسيؤدي النقر فوق هذا الرابط إلى زيارة المتصفح للموقع stealyourdomainthisway.tld. وليست هناك ضرورة على الإطلاق لتضمين معلومات العميل للقيام بالهجوم الخداعي كما أنه ليست هناك ضرورة أيضًا لدقة المعلومات بالكامل. ومع ذلك، فإن تضمين حتى رقم حساب أو تعامل تجاري خطأ سيؤدي إلى تحسين الخداع. و*تبدو* الرسالة قانونية، وعلى الرغم من احتفاظ بعض العملاء بتفاصيل التعاملات التجارية وقد يتعرفوا على أرقام العملاء غير أن البعض الآخر لا يفعل ذلك وقد يوافق بعض العملاء من المجموعة الثانية على أي رقم (أو أية هوية) دون أدنى شك. وبدلاً من ذلك، قد تثير المعلومات غير الدقيقة استجابة مسجّل النطاق والذي قد يتجاهل الرسالة بطريقة أخرى. وعلى فرض وجود مسجّل نطاق زائف يدعى جون سميث، حيث يقدر اسم النطاق smith.tld بشدة. ويتلقى رسالة تذكير دقة WHOIS تحتوي على معلومات جهة الاتصال لفرد آخر مختلف له نفس اللقب، كما هو موضح في رسالة تذكير دقة WHOIS الافتراضية الواردة أدناه:

من: whoisreminders@whoisupdate.com
تاريخ الإرسال: الأربعاء، 12 ديسمبر 2007 الساعة 11:57 صباحًا
إلى: جون سميث
الموضوع: رسالة تذكير بيانات WHOIS

عزيزي العميل المبجل،

وفقًا للقرار رقم 03.41 الخاص بسياسة تذكير بيانات Whois (WDRP) التابعة لشركة الإنترنت للأرقام والأسماء المُخصصة، نُذكرك بالمحافظة على تحديث بيانات جهة الاتصال المحلية لـ WHOIS المرتبطة بتسجيل اسم النطاق الخاص بك. وتتضمن سجلاتنا المعلومات التالية منذ 15 نوفمبر 2007:

اسم النطاق: tld.smith
تاريخ التسجيل: 9 أغسطس 2006
تاريخ الانتهاء: 9 أغسطس 2008
تفاصيل جهة اتصال مسجّل النطاق
الاسم :بيتر سميث
العنوان: 11 شارع سميث
العنوان: (فارغ)
المدينة: سميثفيل
الولاية/المقاطعة: بنسلفانيا
الرمز البريدي:
الدولة: الولايات المتحدة
تفاصيل جهة اتصال الإدارة
الاسم :بيتر سميث
عنوان البريد الإلكتروني: psmith@iamtherealsmith.tld
العنوان: 11 شارع سميث
العنوان:
المدينة: سميثفيل
الولاية/المقاطعة: بنسلفانيا
الرمز البريدي:
الدولة: الولايات المتحدة
رقم الهاتف:7305825074307
اسم المُسجل: <المُسجل>
تفاصيل خادم الاسم

في حالة وجود خطأ في أي من المعلومات الواردة أعلاه، يجب عليك تصحيحها بواسطة زيارة الموقع http://correctmywhoisinfo.tld/login[3]. والرجاء تذكر أنه وفقًا لبنود اتفاقية التسجيل الخاصة بك، قد يكون البند الخاص بمعلومات WHOIS الخطأ أساسًا لإلغاء تسجيل اسم النطاق الخاص بك.

فيتفاعل جون بسرعة لتصحيح المشكلة خوفًا من الاستيلاء على اسم النطاق. وفي عجلة منه، يقوم بالنقر فوق الرابط المضمن وزيارة موقع الويب المخادع ويقوم بكشف بيانات اعتماده للمخادع.

[3] في هذا المثال،تحتوي علامة HTML المضمنة في البريد الإلكتروني الخداعي على عنوان بروتوكول الإنترنت (IP) بدلاً من اسم النطاق، مثل <a “href=http://206.197.43.103/login/”> http://correctmywhoisinfo.tld/login .

استغلال المعلومات التي تم جمعها من خدمات WHOIS

فيما يلي الترتيب الزمني للأحداث التي تحدث في هجوم انتحال صفة المُسجل التمثيلي:

1. يقوم المخادع بإعداد منفذ مزيف لعميل المُسجل (موقع تسجيل الدخول).
2. يقوم المخادع بإنشاء مراسلات بريد إلكتروني تبدو وكأنها من المُسجل.
3. يقوم المخادع بإرسال هذا البريد الإلكتروني إلى عناوين البريد الإلكتروني الخاصة بجهة اتصال اسم النطاق (يقوم بشكل اختياري باستهداف مسجّل النطاق هذا على وجه الخصوص أو يقوم باستهدافه كجزء من الهجوم الخداعي الشامل ضد قائمة من عملاء المُسجل المستهدَف).
4. يقع بعض عملاء المُسجل ضحية للخداع، حيث يقومون بزيارة منفذ عميل المُسجل المزيف وكشف بيانات اعتماد تسجيل الدخول.
5. يقوم المخادع بجمع بيانات اعتماد حساب مسجّل النطاق ليتم استخدامها استخدامًا سيئًا بعد ذلك.

بعد مطالعة هذا الترتيب الزمني للأحداث، يتضح أن المخادعين يحتاجون إلى الربط بين العميل واسم النطاق والمُسجل الراعي لاسم النطاق لمحاولة القيام بهجوم انتحال صفة المُسجل. وتوفر خدمات WHOIS معلومات تسجيل اسم النطاق، بما في ذلك اسم مسجّل النطاق والمعلومات البريدية وعناوين البريد الإلكتروني لجهات الاتصال الإدارية والتقنية للنطاق والمُسجل الراعي. وفيما يلي شرح تمثيلي لنتيجة تفصيلية لاستفسار WHOIS:

هوية النطاق: D2347548-LROR
اسم النطاق: ICANN.ORG
تاريخ الإنشاء: 14 سبتمبر 1998 الساعة 04:00:00 بالتوقيت العالمي (UTC)
تاريخ آخر تحديث: 16 نوفمبر 2007 الساعة 20:24:23 بالتوقيت العالمي (UTC)
تاريخ الانتهاء: 7 ديسمبر 2011 الساعة 17:04:26 بالتوقيت العالمي (UTC)
المُسجل الراعي: شركة .Register.com Inc (R71-LROR)
الحالة: ممنوع الحذف
الحالة: ممنوع التجديد
الحالة: ممنوع النقل
لحالة: ممنوع التحديث
هوية مسجّل النطاق: C4128112-RCOM
اسم مسجّل النطاق: (ICANN) شركة الإنترنت للأرقام والسماء المُخصصة
منظمة مسجّل النطاق: شركة الإنترنت للأرقام والأسماء المُخصصة
عنوان الشارع الرئيس لمسجّل النطاق: 4676 طريق أدميرالتي, جناح رقم 330
مدينة مسجّل النطاق: مارينا ديل راي
ولاية/مقاطعة مسجّل النطاق: كاليفورنيا
الرمز البريدي لمسجّل النطاق: 90292
دولة مسّجل النطاق: الولايات المتحدة
رقم هاتف مسجّل النطاق: +1.3108239358
رقم فاكس مسجّل النطاق: +1.3108238649
عنوان البريد الإلكتروني لمسجّل النطاق: icann@icann.org
هوية المدير: C4128112-RCOM
اسم المدير: (ICANN) شركة الإنترنت للأرقام والأسماء المُخصصة
منظمة المدير: شركة الإنترنت للأرقام والأسماء المُخصصة (ICANN)
عنوان الشارع الرئيسي للمدير: 4676 طريق أدميرالتي, جناح رقم 330
مدينة المدير: مارينا ديل راي
ولاية/مقاطعة المدير: كاليفورنيا
الرمز البريدي للمدير: 90292
دولة المدير: الولايات المتحدة
رقم هاتف المدير: +1.3108239358
رقم فاكس المدير: +1.3108238649
عنوان البريد الإلكتروني للمدير: icann@icann.org
هوية التقنية: C1-RCOM
اسم التقنية: مُسجل نطاق

منظمة التقنية: Register.Com
عنوان الشارع الرئيسي للتقنية: 575 الجادة الثامنة
عنوان الشارع الفرعي للتقنية: الطابق الحادي عشر
مدينة التقنية: نيويورك
ولاية/مقاطعة التقنية: نيويورك
دولة التقنية: الولايات المتحدة
رقم هاتف التقنية: 1.9027492701+
رقم فاكس التقنية: 1.9027495429+
عنوان البريد الإلكتروني للتقنية: domain-registrar@register.com
خادم الاسم: NS.ICANN.ORG
خادم الاسم: A.IANA-SERVERS.NET
خادم الاسم: C.IANA-SERVERS.NET
خادم الاسم: B.IANA-SERVERS.ORG

وفي العديد من الحالات، يقوم المُسجل أو طرف ثالث يقدم خدمة WHOIS بتقديم معلومات إضافية حول النطاق، بما في ذلك:

- حالة الأمان (ما إذا كان يمكن الوصول إلى الموقع من خلال SSL أو HTTP)
- تاريخ إنشاء سجل النطاق وتاريخ آخر تعديل لهذا السجل (في بعض الحالات، يمكن الحصول على سجل جزئي أو كامل للنطاق)
- تاريخ انتهاء سجل النطاق
- حالة مزود الامتداد (رمز حالة EPP[4] الذي وضعه مزود الامتداد على الاسم: ممنوع نقل العميل وفترة الاسترداد، إلخ.)
- بيانات الخادم، مثل نوع خادم الويب (مثل، Apache وMicrosoft IIS) وحالة موقع الويب (مثل، نشط) وعنوان بروتوكول الإنترنت (IP) وحالة القائمة السوداء.
- معلومات DNS (الأسماء وعناوين بروتوكول الإنترنت (IP) الخاصة بخوادم الاسم)
- بحث مسجّل النطاق (مثل، النطاقات الأخرى التي تم تسجيلها بواسطة مسجّل النطاق هذا)
- الكلمات الرئيسية الوصفية التي يستخدمها مسّجل نطاق اسم النطاق لتنقية عمليات البحث
- الإعلان

ويستطيع المعتدون استخدام المعلومات التي تم التقاطها من استجابات WHOIS لخداع مسجّلو النطاق بشكل شامل أو بشكل اختياري بناءً على المراسلات المتوقعة، مثل انتهاء فترة تعليق اسم النطاق. حيث تقوم معلومات معينة من WHOIS بتحديد جهات اتصال البريد الإلكتروني الخاصة باسم النطاق وبالتالي فإن الهدف هو مستلمو البريد الإلكتروني بالإضافة إلى المُسجل الراعي الذي سيقوم المخادع بانتحال صفته (مرسل البريد الإلكتروني). وقد يتم استخدام معلومات أخرى لتحسين موثوقية مضمون الرسالة، على سبيل المثال يمكن استخدام تواريخ إنشاء سجل النطاق وآخر تعديل وتواريخ الانتهاء لإنشاء إخطار تجديد مزيف، كما يمكن استخدام حالة الأمان لإنشاء إخطار مزيف يتعلق بالقلق من إحدى شهادات SSL، إلخ.

[4] بروتوكول التوزيع المرن (EPP)، انظر RFC 3731. http:// www.rfc-archive.org/getrfc.php?rfc=3731

خريطة التهديد

قد يكون الاستيلاء على اسم النطاق عبر هذا النوع من الهجمات الخداعية هو أحد أهدافها ولكنه ليس الهدف الرئيسي بشكل عام. فبمجرد وصول المعتدي إلى حساب مسجّل النطاق، يمكنه تعديل سجلات DNS عبر المُسجل وبالتالي، تشير هذه السجلات إلى خوادم اسم يتحكم بها. ويعد هذا هدفًا شائعًا للأنشطة الإجرامية والضارة التي تقوم باستغلال خدمة الاسم في هجمات التمويه السريع[5]، وخاصة مع مؤشرات الاسم التي تشير إلى النظم التي يتحكم بها، ويستطيع المعتدي بعد ذلك التلاعب بقيم مدة الاستمرار (TTL) وتغيير سجلات DNS الخاصة ببيانات منطقة النطاق على خوادم الاسم التي يقوم بتشغيلها على هذه العناوين.

ويستطيع المعتدي القيام بما يتجاوز استغلال DNS في هجمات التمويه السريع. فعلى سبيل المثال، يستطيع المعتدي إضافة السجلات التالية أو تعديلها في بيانات منطقة النطاق التي يتحكم بها:

- **MX**، للإشارة إلى مضيفي البريد الذين يتحكم بهم واستخدامهم لإرسال بريد مزعج. ويُفضَّل استخدام النطاق الخاص بمسجّل النطاق على النطاق الذي يستطيع المعتدي تسجيله بشكل مباشر نظرًا لأنه في حالات عدة، تعتبر نظم البريد الأخرى أن نطاق مسجّل النطاق "موثوق" أي أنه لا يوجد لديه أي سجل بإنشاء بريد مزعج أو لا يُعرف عنه القيام بترحيل البريد المزعج ولا يتم وضعه في القائمة السوداء أو منعه بطريقة أخرى من إرسال البريد الإلكتروني.

- **A** أو **AAAA**، للإشارة إلى النظم التي تستضيف مواقع الويب المخادعة التي يتحكم بها أيضًا (قد يكون الويب هو الأكثر شيوعا، ولكن يمكن تعديل عناوين بروتوكول الإنترنت (IP) الخاصة بـ FTP وخدمات استضافة المحتوى الأخرى بهذه الطريقة أيضًا). ويستطيع المعتدي بعد ذلك استضافة أي محتوى يختاره على الموقع الخيالي، على سبيل المثال، قد يقوم المعتدي باختيار تشويه موقع الويب وإرباك مسجّل النطاق.

  وقد يقوم المخادعون أيضًا باستبدال معلومات خطأ على الموقع لتعطيل عمل مسجّل النطاق. وتتضمن أمثلة هذا الشكل من الهجوم، إعلانات التخفيضات الكبيرة على أسعار المنتجات وعمليات استرداد المنتج، إلخ. كما يستطيع المعتدي أيضًا تضمين روابط تشعبية تبدو غير ضارة تقوم بتوجيه المستلمين إلى مواقع تستضيف محتوى ضار قابل للتحميل أو محتوى ضار بديل للتطبيقات أو البرامج القابلة للتنفيذ المطلوب تنزيلها.

- **A** أو **AAAA**، للإشارة إلى النظم التي تستضيف مواقع ويب مخادعة داخلية أو مواقع عملاء يتحكم بها المعتدي أيضًا. ويستطيع المعتدي استهداف الشركة التي توفر الوصول عبر الويب إلى معلومات حساسة عبر صفحة توثيق. ويتوقع المعتدي –من خلال إشارة سجلات DNS إلى صفحة توثيق خيالية لشركة إنترانت يتحكم بها- خداع الموظفين غير المرتابين للكشف عن أسماء المستخدمين وكلمات المرور حيث سيقوم ببيعها أو استخدامها في "نشر" الهجمات التالية ضد هذه الشركة. وستكون المؤسسات المالية أهدافًا مختارة لهذه الهجمات، حيث سيقوم العملاء بكشف معلومات الحساب التي قد تتسبب في تعاملات تجارية احتيالية وسرقة صناديق الأموال. ومع ذلك، فإن الشركات التجارية والمنظمات التي توفر الوصول إلى معلومات حساسة أو معلومات ملكية أو شخصية محمية بواسطة قيود الخصوصية معرضة أيضًا لهذه الهجمات.

وهذه القائمة ليست شاملة ولكنها مجر نماذج تمثيلية لأنواع سجلات DNS التي يحاول المخادعون إضافتها أو تغييرها حاليًا.

---

[5] انظر، SAC022، هجمات التمويه السريع و*DNS*،
http://www.icann.org/committees/security/sac025.pdf

إضافة سجلات DNS أو تغييرها

من الواضح أن المخادعين يُفضلون إضافة سجلات DNS بدلاً من استبدالها حيث قد تطول فترة عدم إدراك مسجّل النطاق للهجمات في حالة استمرار حل بعض الأسماء الموجودة في النطاق الخاص به أو جميعها كما هو متوقع. وإضافةً إلى ذلك، يأمل المعتدي -من خلال الاستخدام السيئ لاسم نطاق مملوك لمسجّل نطاق في وضع جيد- في فرض موقف شك عند إثارة إدعاءات الاستخدام السيئ من جانب مستجيبي مكافحة الخداع والقائمين على حماية الماركات. وقد يتردد المُسجلون أو يرفضوا اتخاذ إي إجراء ضد عميل موثوق ويصروا على صدور أمر محكمة، إلخ. وهو الأمر الذي قد يؤدي إلى تأخير جهود تعليق الأنشطة غير القانونية التي يتم إجراؤها بالارتباط باسم النطاق هذا.

وقد يستخدم المعتدي أيضًا أدوات إدارة النطاق التي يُقدمها المُسجل لتمكين إعادة توجيه النطاق أو تغيره لتشير سجلات DNS إلى موقع (رابط) آخر. وفي حالة استخدام العميل المخدوع المُسجل لاستضافة ويب أو بريد إلكتروني، يستطيع المعتدي تحميل محتوى وتعديله على موقع الويب الخاص بالعميل أو إنشاء حسابات بريد إلكترونية (لإرسال بريد مزعج) أو الدخول إلى حسابات البريد الإلكتروني الحالية الموجودة في هذا النطاق أو تعديلها أو توجيهها.

الطريقة التي يستطيع المُسجلون من خلالها خفض تهديدات الخداع

قام المخادعون بتوسيع وصولهم ليتعدى المؤسسات التجارية والمالية إلى مزودي خدمة تسجيل النطاق. ويجب أن يعترف المُسجلون والبائعون أنهم يصبحون أهدافًا للخداع عند استجابتهم. وتوصي SSAC بضرورة التزام المُسجلين (والبائعين) الحذر واتباع أفضل ممارسات مكافحة الخداع عند إنشاء مراسلات لإرسالها إلى العملاء. ويوصى بشدة بالممارسات التالية:

1. تضمين المعلومات الضرورية فقط لنقل الرسالة المرغوبة في مراسلات العملاء. عدم تضمين أرقام الحساب والهويات و(بشكل عام) معلومات التسجيل الخاصة بالعميل. حيث توفر هذه المعلومات فرصًا للمخادعين لتخصيص البريد الإلكتروني.

2. تجنُّب استخدام مراجع الروابط التشعبية في المراسلات مع العملاء. حيث يقوم المخادعون عادةً بإخفاء الروابط لإعادة توجيه المستخدمين من صفحة قانونية إلى أخرى مزيفة.

3. تحذير العملاء من النقر فوق الروابط التشعبية المضمنة في أية مراسلات على هيئة نص أو صورة. تضمين عبارات في نصوص رسالة المراسلات التي تقوم بإرسالها، مثل "للحماية من الخداع، الرجاء كتابة عنوان الويب في شريط عنوان متصفح الويب الخاص بك" أو "لا تثق في الروابط الموجودة في البريد الإلكتروني. وقم دائمًا بكتابة عنوان الويب في شريط عنوان المتصفح الخاص بك". وسيقدر العديد من العملاء التعبير عن الاهتمام بأمنهم وخصوصيتهم، وحتى مع الانزعاج من الاضطرار إلى كتابة العنوان بدلاً من النقر فوقه.

4. رفع الوعي باستهداف الهجمات الخداعية للمُسجلين. وتقديم صفحة الأسئلة الشائعة (أو توسيع الصفحة الموجودة) لجذب الانتباه إلى خداع انتحال صفة المُسجل وجذب الانتباه إلى التهديدات التي تفرضها هذه الهجمات الخداعية والمعايير التي تقوم باتخاذها لتفادي الخداع والمعايير التي يستطيع العملاء الخاصون بك اتخاذها لاكتشاف هذه الهجمات وتجنب الوقوع ضحية لها. وشرح نوع المعلومات التي ستقوم بتضمينها في مراسلات البريد الإلكتروني وبشكل خاص، تحديد أنواع المعلومات التي *لن تقوم أبدًا* بتضمينها في المراسلات وبالتالي يتوفر للعملاء أساسًا لتقييم ما إذا كانت المراسلات التي يتلقونها قانونية أو موضع شبهة.

5. توفير وسائل للعملاء لتقديم تقارير عن الهجمات الخداعية المشبوهة إما بشكل مباشر أو بالتعاون مع منظمة تُشجع تقديم تقارير عن عمليات الاحتيال المشتبه فيها ورسائل البريد الإلكتروني المحتالة والمحافظة على مستودع رسائل البريد الإلكتروني المخادعة[6].

6. التفكير في تنفيذ نموذج بريد إلكتروني لا يمكن إنكار أصله لمراسلات العملاء، مثل التوقيع الرقمي.

[6] صفحة تقرير الخداع الخاصة بمجموعة عمل مكافحة الخداع على الموقع http://www.antiphishing.org/report_phishing.html.

الطريقة التي يستطيع مسجّلو النطاق من خلالها تجنُّب الوقوع ضحية لانتحال صفة المُسجل

تقع على مسجّلي النطاق مسؤولية حماية استثماراتهم في أسماء النطاق. وهذه المسؤولية ليست أقل أهمية -في سياقات التواجد والتشغيل والتجارة على الإنترنت- عن مسؤولية حماية الفرد من السرقة والاستخدام السيئ. وتقوم منظمات سلامة العميل والمؤسسات المالية وشركات بطاقات الائتمان بتنبيه العملاء بالخداع وعمليات الاحتيال التي تتم عبر الإنترنت وتوضح كيفية اكتشاف الهجمات الخداعية وتجنبها. ويمكن تطبيق الكثير من هذه النصائح لتجنب الهجمات الخداعية من خلال انتحال صفة المُسجل. ونعيد هنا ذكر بعض النصائح الأكثر صلة:

1. لا تقم بالنقر فوق الروابط التشعبية المضمنة في رسائل البريد الإلكتروني التي تتسلمها. وبدلاً من ذلك، قم بكتابة عنوان صفحة الويب يدويًا في شريط عنوان متصفح الويب الخاص بك.

2. استخدام عميل بريد إلكتروني يوفر ميزات مكافحة البريد المزعج والخداع أو قم بتثبيت برنامج إضافي أو برنامج مساعد جيد لتكملة هذه الميزات لعميل بريدك الإلكتروني.

3. استخدم عميل بريد إلكتروني يتمتع بالقدرة على كشف مرجع الرابط التشعبي المرتبط بالنص أو الرسائل المعروضة المضمنة في عنوان البريد الإلكتروني أو معرفة كيفية عرض النص "المصدر" أو العادي (ASCII) لرسالة البريد الإلكتروني وقراءته. وتعرف على كيفية قراءة علامات الرابط التشعبي، مثل HREF حتى يمكنك اكتشاف أساليب الخداع التي تعرض رابط مثل، www.example.com ولكنه يقوم في الحقيقة بتوجيهك إلى نطاق خاص بالمعتدين بسرعة، مثل

   <A HREF="http://iwillscamu.tld">www.example.com

   أو عنوان بروتوكول الإنترنت (IP)، مثل

   <A HREF="http://192.168.2.3">www.example.com.

4. قم بالشك في مراسلات البريد الإلكتروني التي تستدعي ضرورة استجابة مُلحة عندما تكون الوسائل المتاحة للاستجابة من خلال زيارة موقع ويب فقط. وتقوم العديد من الشركات التجارية حسنة السمعة عبر الإنترنت –بما في ذلك المُسجلون- بتضمين وسائل أخرى للاتصال بدعم العميل مثل الهاتف أو عنوان البريد الإلكتروني أو الفاكس. وفي حالة الشك، قم بالرد على المُسجل الخاص بك باستخدام وسائل بديلة للاتصال، وخاصة الوسائل التي تجدها مباشرة من خلال زيارة موقع المُسجل الخاص بك.

5. قم بقراءة نص رسالة البريد الإلكتروني بعناية حيث تشير قواعد الإعراب والترقيم السيئة دائمًا إلى أن البريد الإلكتروني مزيف.

6. لا تثق في البريد الإلكتروني ببساطة بسبب أنه مُخصَّص.

7. لا تقم بكشف معلومات شخصية أو معلومات الحساب في أي شكل من أشكال الإرسال عبر الويب حتى تتأكد من شرعية الصفحة.

8. قم بالتأكد من أمان أي شكل من أشكال الإرسال عبر الويب أو صفحة تسجيل الدخول باستخدام SSL. ومع ذلك، لا تثق في الرابط التشعبي ببساطة بسبب ظهوره كصفحة آمنة. وتحقق من موثوقية الشهادة الرقمية المرتبطة بصفحات SSL[7].

9. قم باختيار مُسجل –إذا أردت شراء خدمات اسم نطاق باستخدام بطاقة الائتمان- يطلب من عملائه تقديم رمز التحقق من قيمة البطاقة (CVV) وقت إجراء التعامل التجاري. حيث يعد رمز التحقق من قيمة البطاقة (CVV) معيار أمان لبطاقة الائتمان وتستخدمه الشركات للتحقق من امتلاكك للبطاقة عند إجراء عملية شراء.

10. قم بتقديم تقرير عن رسائل البريد الإلكتروني الخادعة إلى المُسجل أو منظمات مكافحة الخداع الخاصة بك، مثل مجموعة عمل مكافحة الخداع (APWG) أو شبكة تقارير الخداع[8] أو PhishTank[9] أو فريق استجابة طوارئ الكمبيوتر (CERT)[10] المحلي الخاص بك.

للحصول على مزيد من المعلومات حول كيفية تجنب الوقوع ضحية للمخادعين، اقرأ صفحات نصائح العملاء التي توفرها مجموعة عمل مكافحة الخداع[11] وPhishTank ومشروع SpamHaus[12].

النتائج

أصبحت أسماء النطاق سلعًا عالية القيمة بشكل عام، كما أن أسماء النطاق ذات سجل تواجد حسن السمعة وعمليات تشغيل جديرة بالثقة بمثابة أهداف مختارة للمعتدين. كما أن انتحال صفة المُسجل للحصول على بيانات اعتماد العميل وبالتالي الوصول إلى عمليات تسجيل اسم النطاق هو تهديد خداعي خطير. وتُشجع SSAC المُسجلون والبائعون على الاعتراف بأنهم أهداف لعمليات الخداع عند الاستجابة لهذا التهديد وعلى اتخاذ إجراءات لمنع وقوع تلاعب.

كما تدرك SSAC أن عمليات الخداع تنمو بالاعتماد على التضليل والهندسة الاجتماعية. وسيحاول المخادعون تدمير الإجراءات التي يقوم المُسجلون بتنفيذها. وفي النهاية، يتحمل العميل مسؤولية تجنب الوقوع ضحية لعمليات الخداع والاحتيال. وهكذا، وعلى الرغم من توفر العديد من إجراءات تفادي الخداع للمُسجلين، غير أن رفع وعي العميل ونصيحة العملاء بالتزام الحذر عند الاستجابة لمراسلات المُسجل هي الأكثر أهمية.

---

[7] انظر SSL.com، Q10068 – الأسئلة الشائعة: كيف يمكنني أن أعرف إن كانت صفحة الويب آمنة؟ http://info.ssl.com/Article.aspx?id=10068.

[8] شبكة تقارير الخداع، http://www.phishreport.net/

[9] PhishTank: انضم إلى معركة مكافحة الخداع، http://www.phishtank.org

[10] قم بتضمين عناوين البريد الإلكتروني أو صفحات الويب هنا.

[11] نصيحة العميل: كيفية تجنب عمليات الخداع، http://www.antiphishing.org/consumer_recs.html

[12] فهرس صفحات الأسئلة الشائعة (FAQ) الخاصة بمشروع SpamHaus، http://www.spamhaus.org/faq/index.lasso