SAC 025
تقرير SSAC حول استضافة التمويه السريع وDNS

ملاحظة حول الترجمات

كُتبت النسخة الأصلية لهذه الوثيقة باللغة الإنجليزية، وهي متاحة على http://www.icann.org/committees/security/sac025.pdf. وأينما وجد اختلاف في المعنى أو ما يوهم أنه اختلاف في المعنى بين هذه الوثيقة والنص الأصلي، فسيكون النص الأصلي هو السائد.

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

مقدمة

"التمويه السريع" هو تقنية خداعية يستخدمها المجرمون الإلكترونيون ومجرمو الإنترنت، لتجنب تحديد هويتهم وإحباط جهود تنفيذ القانون ومكافحة الجريمة التي تهدف إلى تحديد مواقع الويب المستخدَمة للأغراض غير القانونية وإغلاقها. وتُدعِّم استضافة التمويه السريع تنوعًا كبيرًا من أنشطة الجرائم الإلكترونية (الخداع وسرقة الهوية وعمليات الاحتيال على الإنترنت)، وهي إحدى أخطر التهديدات التي تواجه أنشطة الإنترنت حاليًا. ويقوم "التمويه المزدوج" -أحد أنواع استضافة التمويه السريع- باستغلال خدمات تسجيل أسماء النطاق وتحليل الاسم.

يوضح هذا التقرير الاستشاري الجوانب الفنية لاستضافة التمويه السريع وشبكات خدمة التمويه السريع. حيث يوضح كيفية استغلال DNS، للتحريض على ارتكاب الأنشطة الإجرامية التي تستخدم استضافة التمويه السريع، مع تحديد آثار استضافة التمويه السريع، كما يدعو إلى توجيه انتباه خاص لطريقة إطالة هذه الهجمات لمدة الإستمرار الضارة أو الربحية للأنشطة غير القانونية، التي يتم تنفيذها باستخدام تقنيات التمويه السريع هذه. كما يصف الطرق الحالية والمحتملة لتخفيف استضافة التمويه السريع في مجالات مختلفة في الإنترنت. ويناقش التقرير الاستشاري مزايا طرق التخفيف هذه وعيوبها، ويحدد الطرق التي تنظر إليها SSAC على أنها عملية وملموسة. كما يوصي الهيئات المناسبة بدراسة السياسات التي تساعد على إتاحة طرق التخفيف العملية على المستوى العالمي لمسجّلي النطاق ومقدمي خدمة الإنترنت ومكاتب التسجيل وأصحاب السجل (أينما كان التطبيق مناسبًا).

خلفية

قام متخصصو الأمان ومجتمع مكافحة الجريمة الإلكترونية وهيئات تنفيذ القانون بدراسة استضافة التمويه السريع لبعض الوقت. وتعمل استضافة التمويه السريع على قمة شبكة كبيرة موزعة من الأنظمة المشبوهة التي يمكن نشرها على مستوى العالم بصورة جيدة. حيث تقوم شركات تنمو حديثًا وتعمل في الخفاء، بتأجير عشرات أو آلاف النظم المشبوهة لمخادعي الإنترنت كشبكات خدمة تمويه سريع[1]. ويستخدم مُشغلو شبكات هذه الخدمة قنوات اتصالات (مشفرة) في مخابئ تسلسلية وتقنيات البروكسي. ويقومون بإدارة هذه الشبكات مع بعض التحفظ من خلال الاستفسارات المعتادة عن حالة الأنظمة المشبوهة وعمليات الإضافة والحذف الأساسية للشبكات وفقًا لتواجد استجابة محددة أو عدم تواجدها. ويهتم مجتمع اسم النطاق اهتمامًا خاصًا بطريقة تشغيل هؤلاء المشغلين لتحديثات خدمة اسم النطاق آليًا لإخفاء أماكن مواقع الويب حيث يتم تنفيذ الأنشطة غير القانونية مثل: الاستيلاء على بروتوكول الإنترنت IP (الموسيقى ومقاطع الفيديو والألعاب) واستضافة مواقع بث صور الأطفال الإباحية واستضافة نظم الاحتيال ومبيعات المستحضرات الطبية غير القانونية والقيام سرقة الهوية والخداع.

يستخدم أحد نوعي استضافة التمويه السريع تحديثات سريعة لمعلومات DNS لإخفاء مكان استضافة مواقع الويب وخدمات الإنترنت الأخرى التي تستضيف أنشطة غير قانونية. وفي النوع الآخر الذي يسمى "التمويه المزدوج" يقوم مخادعو الإنترنت بإلحاق شبكة الخدمة التي تستضيف مواقع ويب بشبكة خدمة أخرى تستضيف خوادم DNS. تم وصف طريقة تشغيل شبكات الخدمة هذه بشكل مفصل متاح في الأقسام التالية لهذا التقرير.

المصطلحات

بدأت SSAC في تحديد بعض المصطلحات التي يربط مجتمع أمان الإنترنت بينها وبين استضافة التمويه السريع، وذلك بهدف وصف تقنية التمويه السريع المعقدة ومتعددة الجوانب هذه حسب المتاح حاليًا:

[1] تستخدم منظمات الأمان مجموعة مختلفة من المصطلحات عند وصف استضافة التمويه السريع في مطبوعاتها ومنشوراتها. في هذا التقرير الاستشاري، قمنا بتطبيق المصطلحات الواردة في التقرير الصادر عن Honeynets Project Report *بعنوان اعرف عدوك: شبكات خدمة التمويه السريع*، انظر http://www.honeynet.org/papers/ff/

botnet. botnet هي شبكة تتكون من أجهزة كمبيوتر مشبوهة تقوم بتشغيل برامج (ro)bots ومملوكة لأطراف أخرى. ويمكن التحكم فيها عن بعد –وذلك من خلال المهاجم الفعلي في البداية ثم من خلال الطرف الذي يقوم بالدفع إلى المهاجم مقابل استخدام **botnet** هذه– وذلك لأي عدد من الأنشطة غير المرخصة أو غير القانونية. ويرتبط هذا المهاجم عادةً بفريق إجرامي منظم. ويقوم بتثبيت "برنامج **bot**" على جهاز كمبيوتر دون إخطار أو ترخيص عبر تنزيل برامج تجسس أو فيروسات مرفقة برسالة بريد إلكتروني أو -الأكثر شيوعًا- عبر متصفح أو عبر استغلال أي من عمليات التشغيل الأخرى الخاصة بالعميل (مثل لافتة إعلانية مشبوهة). وبمجرد أن يكون **botnet** قادرًا على التنفيذ، يقوم بإنشاء قناة مساعدة لإعداد بنية تحتية للتحكم من خلال المهاجم. ويستخدم التصميم التقليدي لـ**botnet** نموذجًا مركزيًا، وتتصل كافة القنوات المساعدة بمركز قيادة وتحكم (**C&C**) خاص بالمهاجم. ومؤخرًا، قام مُشغلو **botnet** باستخدام نماذج نظير لنظير (**P2P**) في تشغيل القناة المساعدة لإعاقة اكتشاف القيادة والتحكم (**C&C**)، عبر تحليل الحركة.

مُشغل botnet. هو مصمم الهجوم الموزع ومنفذه، ويتم استخدامه لإنشاء **botnet** وصيانتها واستخدامها بهدف التربح المالي أو غيره (السياسي). وبمجرد تكوين **botnet**، يقوم مُشغل **botnet** بتأجير استخدام **botnet** المملوكة له لتسهيل عمل **مُشغل خدمة التمويه السريع**

التمويه السريع. تُستخدم هذه العبارة للتعبير عن القدرة على النقل السريع لمكان موقع ويب أو بريد إلكتروني أو DNS أو -بصفة عامة- أية خدمة إنترنت أو أية خدمة موزعة من جهاز كمبيوتر واحد أو أكثر متصل/متصلة بالإنترنت إلى مجموعة مختلفة من أجهزة الكمبيوتر لتأجيل الاكتشاف أو تجنبه.

برامج التمويه السريع. في هذا التقرير، *يشير* المصطلح *برنامج* إلى عميل برمجي تم تثبيته دون موافقة على عدد كبير من أجهزة الكمبيوتر عبر الإنترنت.

شبكة خدمة التمويه السريع. في هذا التقرير، تشير شبكة الخدمة إلى مجموعة فرعية من الbotnet التي يقوم مُشغل botnet بتخصيصها لمُشغل خدمة تمويه سريع محدد، والذي يقوم بدوره بتقديم برامج استضافة التمويه السريع أو خدمة الاسم إلى عملائه. لاحظ أنه يتم تشغيل شبكة الخدمة هذه في معظم الأحيان بواسطة "وسيط"، وليس العميل بنفسه.

تحليل استضافة التمويه السريع

يوضح الوصف التالي استضافة التمويه السريع. من الممكن ظهور أشكال وأنواع أخرى، وقد يقوم المهاجمون بتغيير استضافة التمويه السريع في المستقبل لتجنب طرق اكتشاف استضافة التمويه السريع –كما هو موصوف هنا- أو قد يقومون بإضافة طبقات إضافية للتسلسل أو إضافة تلخيص.

وعلى الرغم من توجيه انتباه منطقي للجوانب الفنية للتمويه السريع، توجد مجموعة من الأنشطة "التجارية" المرتبطة بذلك والتي ينبغي وصفها أيضًا. ولا ننسى الحالة التي يريد فيها المخادع القيام بهجوم خداعي.

تبدأ النواحي التجارية لاستضافة التمويه السريع بمصممي البرامج الضارة. حيث يقوم بعض مصممي البرامج الضارة بتطوير أدوات خداعية وحزم برامج يمكن تخصيصها لتوصيل رسائل البريد الإلكتروني المخادع إلى قائمة من المستلمين، واستضافة موقع الويب غير القانوني المرتبط بهذه الأنشطة، والذي يتم من خلاله إرسال رسائل البريد الإلكتروني المخادع إلى الضحايا. بينما يقوم آخرون بإنشاء عناوين بريد إلكتروني وبيع قوائم البريد المزعج. ولكن يستمر آخرون في تطوير برامج bot. ويُعد برنامج bot بمثابة عميل مرن يمكن التحكم به عن بعد، وتوجيهه لإجراء وظائف عشوائية نيابة عن برنامج **مركز قيادة وتحكم** (C&C) مناظر: وبمجرد أن يتم تثبيته في الخفاء على نظام مشبوه، يقوم برنامج bot بتسهيل عمليات التنزيل التالية وتنفيذ برنامج هجوم محدد إضافي عن بعد. ويستخدم مشغلو

botnet كثيرًا ديدان البريد الإلكتروني المتنقلة لإصابة آلاف الأنظمة والسيطرة عليها، على الرغم من أن عمليات السيطرة من جانب العميل -مثل عمليات الاستغلال المعتمدة على المتصفح- هي الأكثر شيوعًا حاليًا.

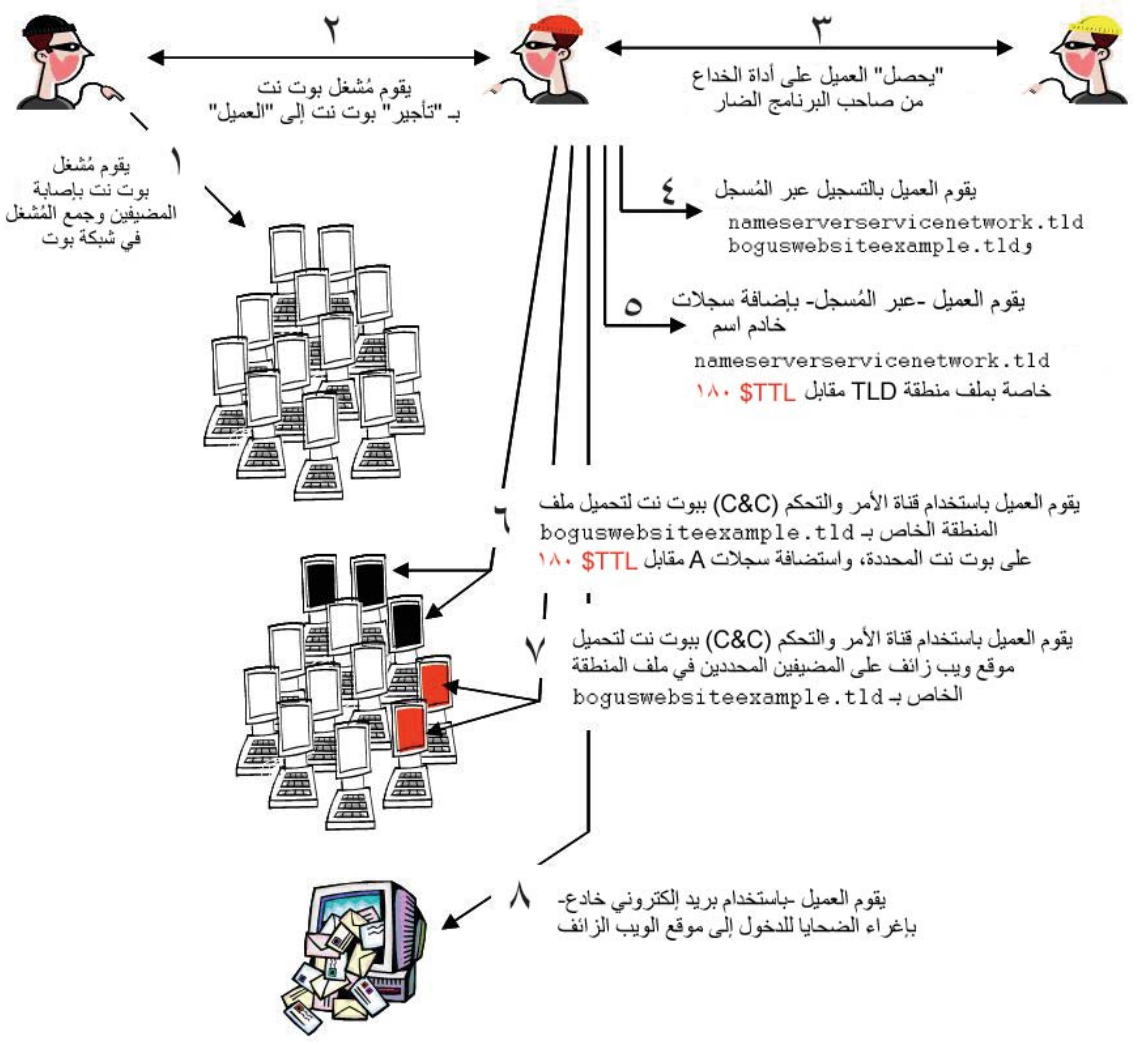
يُعد مصممو البرامج الضارة ومُشغلات botnet *مزودو سلع*، بالنسبة لمجتمع المجرمين الإلكترونيين. ويستخدم مزودو السلع قنوات دردشة إنترنت جماعية (iRC) مشفرة وخاصة/آمنة أو أماكن اجتماعات خفية مشابهة، للإعلان عن سلعهم الإجرامية وإيجاد مشترين لها[2]. أما السلع الإجرامية التي ينتجها مشغل botnet فهي في الأساس البرامج التي يمكنه إتاحتها مقابل رسوم أو بالإيجار. ويقوم المشغل بتأجير القيادة والتحكم لعدد من النظم المشبوهة -التي يتم التفاوض بشأنها- للعميل الذي يكون له الحق في استخدامها مباشرة أو إدارتها نيابة عن مخادع آخر، وفي الحالة الثانية يعمل عميل مُشغل botnet كمزود لخدمات استضافة التمويه السريع. وفي هذا النظام الاقتصادي المعقد والخفي، قد يتفاوض الطرف الذي يهتم بإجراء أنشطة إجرامية مع عدة أطراف للحصول على قائمة بريد مزعج (مخادع) ونشر نظام خداعي أو أدوات هجوم أخرى وbotnet وإجراء الهجوم بنفسه، أو قد يقوم بالتفاوض مع طرف واحد -مُشغل شبكة خدمة تمويه سريع- لتوجيه هجمات مخادعة لصالحه.

يتم استخدام شبكات خدمة التمويه السريع، في استضافة التمويه السريع، لسببين هما:

1) **لاستضافة مواقع ويب الإحالة**. لا تقوم برامج bot في شبكة الخدمة هذه عادةً باستضافة محتوى عميل التمويه السريع، ولكنها تقوم بإعادة توجيه حركة الويب إلى خادم الويب، حيث يستضيف عميل التمويه السريع أنشطة غير مصرح بها أو غير قانونية. وعندما تكون هذه هي الشبكة الوحيدة التي يتم تشغيلها لاستضافة التمويه السريع، ينطبق عليها مصطلح *التمويه الفردي*.
2) **لاستضافة خوادم الاسم**. تقوم برامج bot في شبكة الخدمة هذه بتشغيل مواقع إحالة خادم الاسم لعميل التمويه السريع. وتقوم خوادم الاسم هذه بتوجيه طلبات DNS إلى خوادم اسم مخفية، تقوم باستضافة مناطق تحتوي على سجلات مورد A الخاصة بـ DNS لمجموعة من مواقع ويب الإحالة. ولا تقوم خوادم الاسم المخفية بنقل الاستجابات مرة أخرى عبر خادم اسم الإحالة، ولكنها تقوم بالرد على المضيف المستفسر مباشرةً. وعندما تعمل هذه الشبكة الثانية بالارتباط مع (1) لتحسين الخداع، يتم استخدام مصطلح *التمويه المزدوج*.

[2] انظر "نشاط السوق" كما هو موصوف في استفسار حول "طبيعة ثروة مخادعي الإنترنت وأسبابها"، انظر http://www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf

يوضح الشكل 1 هذه العلاقات.



الشكل 1. مكونات هجمة استضافة "تمويه مزدوج"

استغلال خدمة الاسم: استضافة التمويه المزدوج

يقوم عملاء التمويه السريع كثيرًا بتسجيل أسماء النطاق لأنشطتهم غير القانونية لدى مكتب تسجيل معتمد أو موزع. وفي أحد أشكال الهجوم، يقوم عميل التمويه السريع بتسجيل اسم نطاق (لشبكة خدمة تمويه) لاستضافة مواقع ويب غير قانونية (boguswebsitesexample.tld) واسم/أسماء نطاق (أخرى أو متعددة) لشبكة خدمة تمويه لتقديم خدمة تحليل اسم (nameserverservicenetwork.tld). ويقوم عميل التمويه السريع بتحديد هذه النطاقات لمُشغل شبكة خدمة التمويه السريع الخاص به. يستخدم مُشغل شبكة خدمة التمويه السريع تقنيات آلية، لتغيير معلومات خادم الاسم بسرعة في سجلات التسجيل التي يحتفظ بها مُسجل هذه النطاقات، وتحديدا يقوم مُشغل شبكة خدمة التمويه السريع بـ

- تغيير عناوين IP الخاصة بخوادم اسم النطاق، للإشارة إلى مضيفين مختلفين في النطاق nameserverservicenetwork.tld و
- تعيين مدة الاستمرار (TTL) في سجلات عنوان خوادم الاسم هذه على قيمة صغيرة جدًا (من الشائع التعيين على دقيقة إلى ثلاثة دقائق).

وقد تظهر سجلات المورد المرتبطة بنطاق خادم اسم مستخدَم في استضافة التمويه السريع، في ملف منطقة TLD كما يلي:

```
$TTL 180
boguswebsitesexample.tld.      NS
NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.      NS
NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A  10.0.0.1
NS2.nameserverservicenetwork.tld.   A  10.0.0.2
```

لاحظ أنه تم تعيين مدة استمرار (TTL) سجلات المورد على قيمة صغيرة جدًا (180 ثانية في المثال). وعند انتهاء مدة الاستمرار (TTL)، تقوم عملية التشغيل الآلي لمُشغل شبكة خدمة التمويه السريع على ضمان استبدال المجموعة الحالية بمجموعة جديدة من سجلات A الخاصة بخوادم الاسم:

```
$TTL 180
boguswebsitesexample.tld.      NS
NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.      NS
NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A  192.168.0.123
NS2.nameserverservicenetwork.tld.   A  10.10.10.233
```

ونتيجةً لذلك، تنخفض إمكانية تحديد خوادم الاسم التي تدعم هجمة التمويه السريع هذه وإغلاقها.

تشير سجلات المورد في nameserverservicenetwork.tld إلى مضيفي البروكسي أو مواقع الإحالة أكثر منها إلى برامج bot التي توفر خدمة تحليل الاسم لـ boguswebsitesexample.tld. ويستمع مضيفو مواقع الإحالة إلى المنفذ 53، ويقومون بتوجيه استفسارات DNS إلى برنامج bot الخاص بـ "DNS" الذي يقوم باستضافة ملف منطقة لـ boguswebsitesexample.tld. كما يقوم بتحليل اسم النطاق الخاص بموقع ويب الخداع إلى عنوان بروتوكول الإنترنت (IP) الخاص بمضيف في شبكة خدمة تمويه الويب، ويقوم بإعادة رسالة الاستجابة مباشرة إلى المحلل المستفسر. وفي هذه المرحلة، يُعرف عنوان بروتوكول الإنترنت (IP) لبرنامج DNS bot فقط لمجموعة كبيرة محتملة من مضيفي مواقع الإحالة وتتغير عناوين بروتوكول الإنترنت (IP) الخاصة بمواقع الإحالة كل 180 ثانية.

استضافة تمويه ويب الإحالة

في القسم السابق، قمنا بوصف كيفية قيام استضافة التمويه المزدوج بإضافة مستوى من الخداع من خلال توظيف برامج bot في شبكة nameserverservicenetwork.tld وتغيير سجلات A الخاصة بمضيفي خادم ويب الإحالة بشكل سريع في شبكة boguswebsitesexample.tld. كما تتم أيضًا تهيئة سجلات موارد A الخاصة بخوادم ويب الإحالة باستخدام مدة استمرار (TTL) قصيرة. وعند انتهاء مدد الاستمرار (TTL) الخاصة بمضيفي خوادم الويب، تقوم عملية التشغيل الآلي لمُشغل شبكة خدمة التمويه السريع مرةً أخرى بضمان استبدال المجموعة الحالية بمجموعة جديدة من سجلات A الخاصة بخوادم الاسم. لذلك، يكون إطار الفرصة لتحديد خادم ويب الإحالة التي تدعم هجمة التمويه السريع هذه وإغلاقها صغيرًا جدًا.

قد تظهر السجلات المرتبطة بموقع الويب غير القانوني في ملف منطقة TLD تتم استضافته على برنامج bot خاص بـDNS في شبكة nameserverservicenetwork.tld مثل:

```
boguswebsitesexample.tld.     180  IN   A    192.168.0.1
boguswebsitesexample.tld.     180  IN   A    172.16.0.99
boguswebsitesexample.tld.     180  IN   A    10.0.10.200
boguswebsitesexample.tld.     180  IN   A    192.168.140.11
```

لاحظ مرةً أخرى أنه تم تعيين مدة استمرار (TTL) سجلات المورد على قيم صغيرة جدًا (180 ثانية في المثال). وعند انتهاء مدة الاستمرار (TTL)، يجب تعديل سجلات المورد آليًا للإشارة إلى برامج bot الأخرى التي تقوم باستضافة موقع الويب غير القانوني هذا. وبعد مرور دقائق، قد تتم قراءة ملف المنطقة:

```
boguswebsitesexample.tld.     180  IN   A    192.168.168.14
boguswebsitesexample.tld.     180  IN   A    172.17.0.199
boguswebsitesexample.tld.     180  IN   A    10.10.10.2
boguswebsitesexample.tld.     180  IN   A    192.168.0.111
```

تكون الآثار المتراكمة الناتجة عن التحديث السريع لسجلات A في منطقة boguswebsitesexample.tld وسجلات A الخاصة بخادم الاسم في منطقة TLD، ذات آثار سلبية في الحفاظ على المواقع غير القانونية قيد التشغيل لفترات زمنية أطول من فترات المواقع التي لا تستخدم التمويه السريع.

استضافة التمويه السريع: هل تتعلق باختبار اسم النطاق؟

بالنسبة للبعض، يبدو اختبار اسم النطاق والخداع نشاطان متصلان[3]. وقد قامت مجموعة عمل مكافحة الاحتيال (APWG) بنشر تقرير حول العلاقة بين أسماء النطاق التي تم اختبارها والهجمات الخداعية. ويلخص التقرير نتائج دراستين، استهدفتا تحديد الأطراف التي تقوم باختبار أسماء النطاق وتستخدم هذه الأسماء لتسهيل الهجمات الخداعية. ويبدأ أحد أعضاء مجموعة عمل مكافحة الاحتيال (APWG) بالحديث عن مجموعة من أسماء النطاق التي تم استخدامها في الهجمات الخداعية، وحاول تحديد ما إذا كان قد تم إلغاء هذه الأسماء أثناء "فترة السماح الإضافية". بينما قام عضو ثان في مجموعة عمل مكافحة الاحتيال (APWG) بمطابقة أسماء النطاق المستخدمة في هجمات خداعية بقائمة تصل إلى ما يقرب من ثلاثة ملايين اسم نطاق تم اختبارها على مدى أسبوع واحد. وتُشير

[3] انظر خلفية CADNA، http://www.cadna.org/en/index.html

نتائج كل من الدراستين إلى "وجود حالات قليلة جدًا من اختبار اسم النطاق يقوم بها مخادعون، وتحتوي الحالات الموجودة على تفسيرات ممكنة لا تتعلق بالاختبار"[4].

تستخدم هجمات الاحتيال استضافة التمويه السريع (وخاصة الهجمات التي تستهدف المؤسسات المالية الكبرى) بشكل متزايد، لذلك، انتهى تقرير SSAC إلى عدم وجود علاقات ذات قيمة بين اختبار اسم النطاق واستضافة التمويه السريع. كما لاحظ تقرير SSAC أيضًا عدم تطابق أهداف استضافة التمويه السريع مع اختبار اسم النطاق. وتعد إطالة الفترة الزمنية لموقع يستضيف أنشطة غير قانونية ثبت من قبل أنها تهدف إلى الربح وتشمل أرباحها المعلومات المالية وسرقة بطاقات الائتمان، أحد الأهداف الأساسية لاستضافة التمويه السريع. ويتم استخدام بطاقات الائتمان المسروقة في الدفع مقابل رسوم التسجيل في اسم نطاق موقع خداعي، لذلك ليست هناك دوافع لتسجيل اسم ثم التخلص منه. وعلى وجه المقارنة، يتركز اهتمام مختبري النطاق فقط على دفع رسوم التسجيل مقابل أسماء النطاقات التي يثبت أنها تهدف إلى الربح في إطار تجريبي لعدة أيام.

بدائل التهدئة الحالية والمحتملة

يمكن تنفيذ عدة بدائل تهدئة لتقليل التهديد الذي تفرضه استضافة التمويه السريع.

إغلاق برامج bot التي تستضيف برامج التمويه السريع

يقوم مشغلو botnet بإصابة أجهزة الكمبيوتر الموجودة في شبكات الشركات والمنازل. ومع ذلك، يقوم مُشغل botnet باستغلال أجهزة كمبيوتر قليلة الحماية متصلة بدوائر وصول داخلية ذات نطاق عريض (مودم كبل وDSL)، حيث تزداد فرص العثور على مضيف يمكن استغلاله في هذه الحالة أكثر من الشبكات التي يديرها موظفو تكنولوجيا معلومات ذوو خبرة. ويُعد مضيفو المواقع التعليمية والحكومية والشركات عُرضة للإصابة بهذه النظم، ولكنهم -في المعتاد- أقل عُرضة لمحاولات الإصابة والاستغلال، نظرًا لزيادة المخاطرة في الاكتشاف من قِبل مسؤولي الشبكات.

تشمل طرق التهدئة المتاحة حاليًا، والتي يمكن تنفيذها على نطاق واسع لتقليل عدد أجهزة الكمبيوتر التي يمكن استغلالها واستخدامها في استضافة برنامج bot (ولا تقتصر بالطبع على) ما يلي:

أ) مقاييس أمان سطح المكتب المُحسَّنة (برامج مكافحة الفيروسات والبرامج المضادة للتجسس وبرامج جدار الحماية الشخصية وبرامج اكتشاف تطفل المضيف) على مضيفين موجودين على شبكات خاصة وعامة (خدمة وصول داخلية ذات نطاق عريض مثلاً).
ب) نشر بوابات برامج مضادة للبرامج الضارة بواسطة مقدمي خدمة الإنترنت للعملاء المحليين المشتركين في شبكات وصول ذات نطاق عريض، من خلال مزودي خدمة أمان مدربين أو مسؤولي أمان داخليين للشبكات التجارية، وزيادة تبني بوابات البرامج المضادة للبرامج الضارة من خلال مسؤولي أمان الشبكات الخاصة.
ج) التعليم والوعي والتدريب، مع التركيز بشكل خاص على فهم وتطبيق سياسات صارمة لحركة المرور للخارج.

وتتضمن طرق التهدئة الإضافية التي ينبغي مراعاتها ما يلي:

د) معالجة قائمة بيضاء قابلة للتنفيذ.
هـ) أدوات تحكم الوصول/الدخول إلى الشبكة.
و) تحليل سلوكيات botnet المعروفة وتطوير تقنية الاكتشاف (مثل التوقيع) التي يمكن استخدامها لحظر النشاط على بوابة أمان "إدارة التهديد". هذا امتداد طبيعي للعنصر (ب)، أعلاه).

[4] APWG: العلاقة بين الخداع واختبار اسم النطاق،
http:// www.antiphishing.org/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

لم تُثبت الطريقتان (أ) و(ب) فعالية في تهدئة تهديد البرامج الضارة، وذلك على الرغم مما يبدو من أنهما الأكثر فعالية. ويمكن أن يقوم مصممو برنامج العاصفة[5] والبرامج الضارة الشبيهة الأخرى بتغييرها وتوزيعها دوريًا، باستخدام برامج bot لم يتم اكتشافها بعد[6] ومقاييس برامج مضادة للبرامج الضارة تعتمد على التوقيع غير فعالة في استئصال البرامج الضارة مثل برنامج طروادة العاصفة[7]. وتقوم أجهزة الكمبيوتر التي تصيبها هذه البرامج الضارة بتوسيع المجموعة بصورة أسرع مما يمكن أن يحددها المجتمع ويقوم بإزالة الإصابات من أجهزة الكمبيوتر المشبوهة. ومما يدعو للأسف أن عملية التعليم والوعي (ج) هي عملية بطيئة. وقد أوضح تقرير مسح جرائم وأمان الكمبيوتر الصادر عن FBI/CSI، أن نسبة 97% من أجهزة الكمبيوتر تقوم بتشغيل برامج مكافحة الفيروسات، بينما تقوم نسبة 79% من الأجهزة بتشغيل برامج مضادة للتجسس، ومع ذلك تسجل إصابات برامج bot نسبًا مرتفعة بشكل مخيف: في يونيو 2007، أعلن مكتب التحقيقات الفيدرالية FBI الأمريكي مبادرته المستمرة لجرائم الإنترنت لمكافحة botnet التي تم تحديدها على مليون جهاز كمبيوتر مشبوه وبرامج bot، بحيث تكون من اختصاصه وحده[8]. تنطبق هذه الأرقام على شبكات المؤسسات/الشركات. ويُعد استخدام برامج مكافحة الفيروسات والبرامج المضادة للتجسس -ليس كبيراً كالحالة السابقة- أحد الاستخدامات الشائعة بين مستخدمي الشبكات الداخلية ذات النطاقات العريضة، حيث يتم تجاهل الأمان وتهيئة الشبكة كثيراً، وغالبًا ما تنتهي تحديثات الاشتراكات الخاصة بتحديث عمليات التعرف على البرامج المضادة للبرامج الضارة بدون تجديد.

تُعد عملية معالجة قائمة بيضاء قابلة للتنفيذ، تقنية مضادة للبرامج الضارة تقوم بتنفيذها السياسة التنفيذية، وبصفة خاصة، لأنه يمكن منع جميع التطبيقات والعمليات المتصلة بها -عدا مجموعة موثوق بها منها- من العمل على جهاز الكمبيوتر. ولا يتم تنفيذ إجراء القائمة البيضاء القابلة للتنفيذ على نطاق واسع، وخاصة بين مستخدمي الإنترنت الداخليين/العملاء. ويُعد تنوع التطبيقات ومسار تقديم تطبيقات جديدة وقلة العروض التجارية المفيدة للعميل، والخدمات التي تبدو كأنشطة موثوق بها للقوائم البيضاء (إذا كان هذا النموذج سهلاً)، أهم العوامل التي تعوق تبني ذلك.

ويتم حاليًا تطوير حلول أدوات تحكم الوصول/الدخول إلى الشبكة؛ بهدف منع أطراف غير محمية من الاتصال بشبكات LAN وشبكات WLAN. كما يتم إجراء تقديرات أمان على جهاز كمبيوتر لتحديد ما إذا كان خالياً من برامج الملفات التنفيذية الضارة قبل السماح لهذا الكمبيوتر بالاتصال بالإنترنت. وإذا كان جهاز الكمبيوتر يعمل كجهاز مشبوه، يتم تعليقه ولا يمكن إعادة توصيل الجهاز ما لم يتم تصحيح انتهاك الأمان للنطاق العريض الداخلي (هـ) لم يتم تنفيذه على نطاق واسع وهو يتطلب معايير إضافية وتطوير للبرامج. يشير مزودو خدمة الإنترنت ISP ومزودو وصول النطاقات العريضة إلى أنه لا يمكنهم تحمل تكلفة التنفيذ وإدارة وصول الشبكة وفلترة حركة الدخول.

إغلاق مضيفي التمويه السريع

عدد كبير من المضيفين المشبوهين المستخدَمين في مثل هذه الهجمات عبارة عن أجهزة كمبيوتر متصلة بخدمات نطاق عريض داخلية. تستضيف أجهزة الكمبيوتر هذه برامج bot لمواقع ويب الإحالة وخادم الأسماء.

ويعد كل من الاكتشاف العرَضي والعزل والاستجابة هي أهم إجراءات التهدئة المتبعة حاليًا. أولاً، يتم تحديد نظام -أو الإبلاغ عنه- بأنه يستضيف أنشطة غير قانونية. وفي مخطط استضافة التمويه السريع، قد يكون هذا موقع ويب إحالة أو خادم اسم أو النظام الذي يستضيف موقع ويب غير قانوني، يقوم فريق الاستجابة المكافح للجريمة بجمع معلومات حول الموقع، مثل: مكان نظام الاستضافة ودائرة الاختصاص ومالك النطاق ومسؤول الموقع ومزود خدمة الإنترنت

[5] هجمة دودة العاصفة DDoS، -http://www.secureworks.com/research/threats/view.html?threat=storm worm

[6] *مخادعو وسائل العاصفة غير الكاملة*، http://www.securityfocus.com/news/11442

[7] الإحصاء الشائع للبرامج الضارة CME- برنامج تنزيل طروادة 711. http://cme.mitre.org/data/list.html

[8] *يوجد أكثر من مليون ضحية محتملة للجرائم الإلكترونية المتعلقة ب botbotnet*، http://www.fbi.gov/page2/june07/botnet061307.htm

ونوع النشاط غير القانوني. يستخدم فريق الاستجابة خدمات WHOIS ووسائل أخرى لتحديد عدة أطراف والاتصال بهم -بالتوازن وبشكل متكرر- حتى يتلقون المساعدة في إغلاق النشاط غير القانوني[9]:

- في حالة ظهور أنشطة غير قانونية كأنشطة مُستضافة على نظام مشبوه (مثلاً على خادم ويب يقوم بإجراء أعمال قانونية، ولا يعلم المسؤول أن الخادم يستضيف موقعًا غير قانوني أيضًا)، يتم الاتصال بمالك النطاق لتقديم المساعدة في الإغلاق.
- ويتم الاتصال بمزود خدمة الإنترنت أو مزود الاستضافة لطلب إنهاء هذه الخدمة من المضيف
- وفي حالة طلب فريق الاستجابة لمساعدة محلية (ترجمة فورية إلى لغة أو إثبات أن فريق الاستجابة ممثلون ذوو نوايا حسنة، أو مساعدة في الحصول على مزيد من المعلومات)، يتم الاتصال بفريق "طوارئ الكمبيوتر المحلي" أو "فريق استجابات الطوارئ" (CIRT/CERT). (في بعض البلدان، تقوم فرق CERT بتشجيع فريق الاستجابة على الاتصال بها مبكرًا في هذه العمليات قدر الإمكان).
- في حالات وجود برامج bot على خوادم اسم مضيف جهاز الكمبيوتر، يتم الاتصال بالمُسجلين أو بمزودي الامتداد، لإزالة سجلات خادم الاسم من ملفات منطقة TLD أو تعليق النطاقات.

قد تقوم المواقع غير القانونية نفسها بالعمل من خوادم مشبوهة على نطاقات قانونية أو لدى مزودي موقع الويب التي تتشارك الاستضافة أو تسهيلات استضافة الويب (شبه) القانونية "المشبوهة"[10]. وفي الحالات التي لا يكون التعاون فيها وشيكًا -حيث لا يعترف المشغلون أو السلطات المحلية بهوية فريق الاستجابة أو لا يثقون بهم، أو لا يرغبون في الاستجابة بناءً على المعلومات التي يزود بها فريق الاستجابة وفرق CERT- يكون لدى فريق الاستجابة الحق في طلب المساعدة من مؤسسات تنفيذ القانون (LEA) أو طلب أمر قضائي يرغم المشغل على إغلاق الموقع. وتعد هذه هي إجراءات المحاولة الأخيرة، حيث تتطلب الإطارات الزمنية لتحديد مؤسسات تنفيذ القانون LEA والتنسيق معها، والحصول على إجراء قضائي في دائرة الاختصاص أيامًا وأسابيع، بينما يطلب فريق الاستجابة إغلاق المواقع غير القانونية خلال ساعات.

التعديل السريع لسجلات موارد A التي يتم تحليلها إلى خوادم ويب الإحالة يحبط الكشف عن مواقع استضافة التمويه السريع ويعيق إجراءات إغلاقها. وفي بعض الحالات، يطول المدى الزمني للموقع الذي يستضيف تمويها سريعًا وفقًا لمتوسط يبلغ أربعة أيام تقريبًا[11].

تشمل إصلاحات هذا النموذج للتهدئة ما يلي:

1) تبني إجراءات من شأنها الإسراع بتعليق اسم نطاق؛ لإزالة مشكلة المواقع غير القانونية التي يتم إغلاقها، ولكن سرعان ما تتم استضافتها على خادم مختلف لدى مزود خدمة إنترنت مختلف.
2) التنسيق الجيد ومشاركة المعلومات مع فريق الاستجابة وLEA وفرق CERT. كما تشمل قاعدة/قواعد بيانات تحتوي على مراكز اتصال (باللغات المنطوقة) ومعلومات حول متطلبات دوائر الاختصاص والعادات المتبعة والمعلومات الأخرى التي تفيد في أنشطة التعليق المشابهة.

---

[9] هذا المخطط، يتم التعبير عن المراسلات الشخصية المتعلقة بفريق الاستجابة في طرق مستخدمة للاستجابة للهجمات الخداعية حيث تتم الاستفادة من استضافة التمويه السريع بشكل عدواني.

[10] تشير الاستضافة المشبوهة إلى مزودي استضافة بريد إلكتروني إضافي ومواقع ويب يضعون بنود وشروط خدمة محدودة – أو لا يضعون نهائيًا – لإدارة المحتوى والأنشطة المستضافة على مراكز الخدمة الخاصة بهم. يتم استخدام المصطلح "المشبوهة" لتأكيد أن الخدمات المستضافة لدى مزودي الخدمة هؤلاء لم يتم إغلاقها. لا يعمل العديد من مزودي خدمة الاستضافة المشبوهة بنوايا حسنة مع مؤسسات تنفيذ القانون ومكافحة الجريمة، ولكنهم يعملون في دوائر اختصاص تقدم فيها السلطات المحلية وقوانين الإنترنت ملاذًا آمنًا للأنشطة غير القانونية.

[11] ذكر تقرير صادر عن إحصائيات APWG الشهرية من ديسمبر 2006 حتى أغسطس 2007 أن: لدى مواقع الخداع متوسط مدة على الإنترنت يتراوح بين 3.3 و4.5 يومًا، انظر http://www.apwg.org/phishReportsArchive.html، ومع ذلك يتم احتساب المتوسط بدون تمييز بين مواقع الخداع المستضافة عادةً وتلك التي تستخدم التمويه السريع. وحيث تتغير عناوين IP الخاصة بالتمويه السريع بسرعة، ساهمت استضافة التمويه السريع في خفض المدة.

إزالة النطاقات المستخدمة في استضافة التمويه السريع من الخدمة

في بعض مخططات الإغلاق، عندما يقرر فريق استجابة مكافحة الجريمة أن اسم نطاق يتم استخدامه لهجمات تمويه سريع، اذهب إلى مكتب التسجيل أو صاحب السجل الذي يتم تسجيل اسم النطاق لديه، وقم بشرح طبيعة المشكلة وإقناع مكتب التسجيل باستبعاد اسم النطاق عن الخدمة.

ولا تُلزم السياسة أصحاب السجلات أو مكاتب التسجيل بالاستجابة بصفة خاصة لشكاوى تتعلق باستضافة التمويه السريع، ولا تعد تقنية التمويه السريع في حد ذاتها نشاطًا غير قانوني ما لم ترتبط بشكل واضح بنشاط غير قانوني (إساءة استخدام جهاز كمبيوتر والاحتيال وانتحال الهوية). يضع أصحاب السجلات و مكاتب التسجيل سياساتهم الخاصة بهم فيما يتعلق بإساءة الاستخدام ويقومون بتنفيذ إجراءات الاستجابة وفقًا لها. ومع ذلك، توجد بعض الممارسات الشائعة. وطلب أصحاب السجلات معلومات كافية؛ حتى يثبتوا بوضوح أن اسم النطاق يُساء استخدامه أو يتم من خلاله توجيه سلوكيات إجرامية، وبالتالي سيقومون بإجراء تحرياتهم اللازمة. إذا أثبتت تحريات صاحب السجل الخاصة صحة البيانات التي قدمها أحد أفراد فريق الاستجابة أو المدَّعي، يكون لدى صاحب السجل الحق في تقديم هذا الدليل إلى مكتب التسجيل ، الذي يتحرك بدوره بسرعة لحل المشكلة محل النزاع. تؤثر كل من سياسة مكتب التسجيل الخاصة واتفاقية RAA التي عقدتها ICANN (إن كانت تنطبق على TLD المسجَّل به اسم النطاق) على استجابة مكتب التسجيل ، الذي قد يقوم بتعليق النطاق (مثلاً يستخدم حالة "معلَّق" لمنع DNS من تحليل الاسم)، أو يقوم بتعليق اسم النطاق وتغيير سجل التسجيل لإظهار أن اسم النطاق محل نزاع أو يتم إساءة استخدام سياسة التسجيل، أو تعليق اسم النطاق وحذفه من المنطقة. يستجيب أصحاب السجلات بالمثل لطلبات ترد من مؤسسات تنفيذ القانون والأوامر القضائية والنيابية بشكل عاجل. لدى العديد من أصحاب السجلات ومكاتب التسجيل أقسام عامة للتعامل مع إساءة الاستخدام، وغالبًا ما تصل الأسئلة الشائعة ونماذج الاتصال إلى المتصفح. وقد يزود المُسجلون ومزودو الامتداد بأسئلة شائعة ونماذج اتصال شبيهة لتسهيل وتعجيل الاتصال بـ LEA ومراكز استجابة مكافحة الجريمة.

التعديل السريع لسجلات موارد A التي يتم تحليلها إلى خوادم ويب الإحالة يحبط الكشف عن مواقع استضافة التمويه السريع ويعيق إجراءات إغلاقها.

تتضمن طرق التهدئة المتبعة حاليًا -ولكن ليست بانتظام- ما يلي:

- توثيق الاتصالات قبل السماح بإجراء تغييرات على عمليات تهيئة خادم الاسم.
- تنفيذ مقاييس لمنع إجراء تغييرات آلية (مخططة) على عمليات تهيئة خادم الاسم.
- تعيين حد أدنى لمدة الاستمرار (TTL) المسموح بها (30 دقيقة مثلاً)، وهي كافية لإعاقة عنصر التمويه المزدوج الخاص باستضافة التمويه السريع.
- تنفيذ أنظمة مراقبة إساءة الاستخدام أو توسيعها للإبلاغ عن تغييرات تهيئة DNS المفرطة.
- نشر اتفاقية "بنود وشروط عالمية للخدمة" تمنع استخدام نطاق مسجَّل وخدمات استضافة (DNS والويب والبريد) التي تقوم بتوجيه أنشطة غير قانونية أو غير مرغوب فيها (حسب ما يرد بالاتفاقية) وتطبيق هذه الاتفاقية.

وهناك طرق أخرى إضافية مقترَحة للاكتشاف والتهدئة. وتشمل ما يلي:

- **تعليق (واحتواء) أسماء النطاق.** بناءً على مجموعة من المعايير التي يجب تحديدها، قام المُسجل بتعليق تحديثات خادم اسم لأسماء النطاق المشتبه في صلتها بهجمات تمويه سريع. وأثناء فترة التعليق، لاحظ ودوَّن (سجَّل) كافة أنشطة حساب مزود الامتداد، كما سجَّل محاولات التحديث. وذلك يعمل على توسيع إطار التحليل العرَضي ويعطي المحققين فرصة لتتبع مصدر التحديثات وتحديد برامج bot.

- **تحديد معدل التغيير (محدود برقم لكل ساعة/يوم/أسبوع) لخوادم الاسم المرتبطة باسم نطاق مسجَّل.** يقوم أصحاب السجلات ومكاتب التسجيل بتطبيق تقنيات تحديد المعدل على خدمات WHOIS القائمة على استفسارات لإعاقة إساءة الاستخدام. تحديد معدل التغيير الذي (أ) يناسب التطبيقات القانونية ذات مدة الاستمرار القصيرة (TTL) لسجلات خادم الاسم في ملفات منطقة TLD و(ب) يزود المحققين بإطار يمنحهم فرصة تتبع مصدر التحديثات وتحديد برامج bot و(ج) يقلل من فائدة مدد الاستمرار (TTL) القصيرة لمهاجمي التمويه السريع.

- **فصل "تحديثات مدة الاستمرار (TTL) القصيرة" عن إجراء تغيير التسجيل العادي.** التعامل مع طلبات تعيين مدة الاستمرار ضمن حد معين كطلبات خاصة تتطلب بعض أشكال التحقق.

- **استخدام نطاقات معلقة لتدريب العملاء.** لا تقم فوراً بإعادة النطاقات التي ثبت استخدامها في أغراض غير قانونية، بل قم بإنشاء صفحة مقصودة للزائرين توضح أن هذا النطاق معلَّق لأنه يُستخدم في أنشطة غير قانونية أو غير مرغوب فيها وإعادة توجيههم إليها، وإخبار المستخدمين بطرق اكتشاف الخداع وتجنب الوقوع كضحية نتيجة للخداع وأنشطة إجرامية أخرى.

النتائج

يقدم تقرير SSAC النتائج التالية بهدف دراسة المجتمع لها:

1) تُمكّن استضافة التمويه السريع بنية تحتية لإطلاق هجمات عالية الدقة، مما يعمل على استغلال خدمات تحليل اسم النطاق بشكل متزايد لتوجيه أنشطة غير قانونية وغير مرغوب فيها.

2) لم تثبت الطرق الحالية لإعاقة استضافة التمويه السريع من خلال اكتشافه وتفكيك botnet، أية فاعلية.

3) كما يقوم التمويه المزدوج بإحباط الكشف عن وإعاقة إجراءات غلق مواقع ويب استضافة التمويه السريع.

4) تمثل التعديلات المتكررة لسجلات خادم الاسم (NS) من خلال مسجّل اسم نطاق ومدة الاستمرار القصيرة في سجلات A الخاصة بخادم الاسم في ملفات منطقة TLD، علامات يمكن مراقبتها لتحديد حالات إساءة الاستخدام المحتملة لخدمات الاسم.

5) تظهر المقاييس المتخذة لمنع التغييرات الآلية لمعلومات DNS وتعيين حد أدنى أطول لمدة استمرار سجلات A الخاصة بخادم الاسم في ملفات منطقة TLD، لتكون فعالة ولكن لا تتم ممارستها بانتظام.

6) تم اقتراح مقاييس إضافية لمواجهة استضافة التمويه السريع، وتحقيق أقصى استفادة من الدراسة.

التوصيات

تُمثل استضافة التمويه السريع مشكلة خطيرة ومتزايدة، يمكن أن تؤثر على خدمات الاسم في كافة TLD. وقد حثت SSAC منظمة ICANN أصحاب السجلات ومكاتب التسجيل على النظر بعين الاعتبار للممارسات المذكورة في هذه التقرير، لإنشاء أفضل الممارسات التي من شأنها تهدئة استضافة التمويه السريع، ودراسة ما إذا كان ينبغي تضمين مثل هذه الممارسات في اتفاقيات في المستقبل.