الجمهورية العربية السورية

الهيئة الوطنية لخدمات الشبكة

مركز أمن المعلومات

National Agency for Network Services

Information Security Center

دراسة بحثية عن البرنامج الخبيث
TrickBot Trojan

الوصف Description

TrickBot هو برنامج خبيث من النوع حصان طروادة Trojan، وهو يهدف بشكل رئيسي إلى سرقة بيانات المستخدمين التي تتعلق بالحسابات المالية المختلفة، بالإضافة إلى قيامه بتحميل وتنصيب برمجيات خبيثة أخرى على الأنظمة المصابة.

يعتمد البرنامج الخبيث TrickBot بشكل رئيسي على هجوم Man-in-The-Browser من أجل كشف وسرقة بيانات المستخدمين كبيانات الدخول إلى الحسابات المصرفية، يقوم البرنامج الخبيث في هذا الهجوم بعمليات اعتراض وتلاعب بالبيانات المتبادلة بين البرنامج التنفيذي الرئيسي للمتصفح وآلية الأمان الخاصة به؛ يحظى TrickBot بعمليات تحديث وإضافات من قبل مطوريه وذلك بشكل مستمر.

النشر Dissemination

يعتمد ناشرو هذا البرنامج الخبيث على حملات البريد الالكتروني الواغل Malspam Campaigns، حيث يتم إرسال العديد من الرسائل باستخدام أسماء علامات تجارية معروفة لشركات مالية ومصرفية والتي تهدف إلى توجيه المستخدمين المستهدَفين لتحميل البرنامج من مواقع مشبوهة تم تجهيزها مسبقاً، أو خداع المستخدمين بمحاولة اقناعهم لفتح وتحميل ملفات مرفقة في هذه الرسائل من النوع Microsoft Word, Excel تحوي وحدات برمجية نوع Macros حيث عند فتح هذه المرفقات تقوم بدورها بالطلب من المستخدم تمكين المحتوى البرمجي لتنفيذ رمازات برمجية نوع VBScript أو رمازات نوع PowerShell لتحميل البرنامج الخبيث، بالإضافة إلى أن برنامج TrickBot يتم تحميله كبرنامج إضافي Second Payload بواسطة البرنامج الخبيث Emotet؛ حتى إن بعض مكونات البرنامج تعتمد على البروتوكول Server Message Block SMB لنشره ضمن الشبكات.

الإقلاع وبدء العمل Starting Up

يبدأ البرنامج TrickBot عمله على الأنظمة المصابة بإجراء عدد من الاختبارات للتأكد من أن النظام الحالي ليس بيئة اختبارية Sandbox، ثم يبدأ بمحاولات لإيقاف عمل التطبيقات المضادة للبرمجيات الخبيثة، بعدها سيقوم البرنامج بنشر نفسه ضمن المجلد %AppData%، ثم لاحقاً ولضمان استمرار عمله سيعتمد برنامج TrickBot على إنشاء عدد من المهام المجدولة.

لمعرفة العنوان الرقمي العائد لنظام التشغيل المضيف يقوم البرنامج بالاتصال بكل من المواقع الالكترونية التالية:

- hxxp://myexternalip.com/raw
- hxxp://api.ipify.org
- hxxp://icanhazip.com
- hxxp://bot.whatismyipaddress.com
- hxxp://ip.anysrc.net/plain/clientip

بعدها سيبدأ برنامج TrickBot باستقبال التعليمات والأوامر من مخدمات الإدارة والتحكم C2 Servers ويتهيأ لتحميل بقية المكونات والتي سيقوم بتحميلها مع ملف إعداد خاص بها على شكل ملفات مكتبات ربط ديناميكي DLLs. بدايةً سيرسل البرنامج معلومات تتعلق بالنظام المصاب المضيف إلى مخدمات الإدارة والتحكم والتي ستقوم بدورها بإرسال عنوان رقمي مع تاريخ صلاحية، هذا العنوان سيستخدمه البرنامج لتحميل بقية مكوناته وعند حصول أي تحديث لهذه المعلومات سيتم ارسال هذه التعديلات إلى البرنامج تباعاً من قبل المخدمات C2.

يستخدم برنامج TrickBot كلاً من البروتوكولات HTTP, HTTPS وكلاً من المنهجيات GET, POST لتحميل مكوناته ولإرسال المعلومات وبيانات دخول المستخدمين التي قام بسرقتها وذلك إلى مخدمات التحكم والإدارة C2 Servers.

تقنيات هجمات الويب المستخدَمة Web Attacks

يعتمد TrickBot على نوعين من أنواع هجمات الحقن عبر الويب من أجل سرقة البيانات المالية من جلسات المستخدمين التي تتعلق بالخدمات المصرفية عبر الانترنت:

- Redirection attacks: إعادة توجيه المستخدمين الضحايا إلى مواقع احتيالية تعمل ضمن مخدمات خاصة تطابق تماماً في الشكل العام مواقع مصرفية حقيقية، ويتم ذلك عند قيام هؤلاء المستخدمين بطلب المواقع المصرفية الحقيقية.
- Server side injection: اعتراض الاستجابة القادمة من المخدمات المضيفة لخدمات الويب المصرفية وحقن رمازات خبيثة إضافية نوع Client-side ضمنها، حيث ستقوم هذه الرمازات بسرقة بيانات الدخول

المصرفية التي يتم إدخالها ضمن نماذج HTML Forms، بالإضافة إلى إمكانية تسجيل ضربات مفاتيح المستخدمين باستخدام Keylogger.

يستخدم موزعو البرنامج الخبيث TtrickBot وسومات فريدة Gtags من أجل تمييز الدفعات والاصدارات المختلفة من البرنامج، يتم إرسال هذه المعرفات الفريدة ضمن الروابط وذلك عند تواصل البرنامج مع مخدمات الإدارة.
تقوم مكونات البرنامج TrickBot Modules بالعديد من المهام من أجل سرقة البيانات المصرفية، استطلاع واستكشاف الأنظمة والشبكات، جمع وسرقة بيانات الدخول المختلفة ونشر نفسها عبر الشبكات.

المكونات العامة Common TrickBot Modules

تعتبر المكونات التالية هي المكونات الأكثر شيوعاً علماً بأن مطوري البرنامج الخبيث TrickBot يقومون بتحديث البرنامج وتطوير مكونات إضافية:

مكونات سرقة المعلومات المصرفية Banking Information Stealers

- LoaderDll/InjectDll: مراقبة أنشطة تصفح المواقع المصرفية واستخدام تقنيات حقن الويب كالنوافذ المنبثقة التعسفية والحقول الزائدة المضافة بشكل مقصود وذلك من أجل سرقة البيانات المصرفية.
- Sinj: الاحتفاظ بمعلومات عن المواقع المصرفية المستهدَفة بالبرنامج TrickBot، واستخدام هذه المعلومات لإطلاق هجمات إعادة توجيه المستخدمين إلى مواقع خبيثة مماثلة للمواقع المصرفية الحقيقية لغاية سرقة بيانات دخول المستخدمين التي يستخدمونها للدخول لهذه المواقع.
- Dinj: الاحتفاظ بمعلومات عن المواقع المصرفية المستهدَفة بالبرنامج TrickBot، واستخدام هذه المعلومات لإطلاق هجمات اعتراض الاستجابة القادمة من المخدمات المضيفة لخدمات الويب المصرفية وحقن رمازات خبيثة ضمن صفحات الاستجابة حيث ستعمل هذه الرمازات على جمع البيانات التي سيدخلها المستخدمون ضمن نماذج الادخال بالإضافة الى تسجيل ضربات لوحات المفاتيح.
- Dpost: يحوي العناوين الرقمية وأرقام المنافذ العائدة للمعلومات المصرفية التي تمت سرقتها، يتم إضافة هذه المعلومات تباعاً عند إدخال المستخدم لبيانات مصرفية.

مكونات جمع المعلومات حول الأنظمة والشبكات System and Network Reconnaissance

- Systeminfo: جمع معلومات تفصيلية عن الأنظمة المصابة.
- Mailsearcher: مقارنة جميع الملفات الموجودة على القرص الصلب بقائمة تتضمن ملحقات الملفات.
- NetworkDll: جمع معلومات إضافية عن الأنظمة بالإضافة إلى جمع وتحديد تفاصيل الشبكات بأسلوب Network Mapping

سرقة بيانات الدخول ومعلومات المستخدمين Credential and User Information Harvesting

- ModuleDll/ImportDll: جمع وسرقة البيانات من متصفحات الانترنت مثل ملفات الارتباط وغيرها.
- DomainDll: جمع وسرقة بيانات الدخول والبيانات المتعلقة بالإعدادات من المتحكمات بالمجالات Domain Controllers ويتم ذلك بعد الوصول إلى مجلد النظام Sysvol بواسطة البروتوكول LDAP
- SqulDll: فرض تفعيل البروتوكول WDigest واستخدام الأداة مفتوحة المصدر Mimikatz، وذلك لكشف بيانات الدخول من أداة النظام LSASS.exe، حيث ستقوم مكونات البرنامج المعنية باستخدام هذه البيانات من أجل نشر البرنامج عبر الشبكات.
- Pwgrab: جمع وسرقة بيانات الدخول، معلومات التعبئة التلقائية، تاريخ التصفح، ومعلومات أخرى من متصفحات الانترنت بالإضافة إلى العديد من التطبيقات الأخرى.

مكونات النشر عبر الشبكة Network Propagation

- WormDll and ShareDll: وهي عبارة عن المكونات الدودية للبرنامج، حيث تقوم هذه المكونات باستغلال كل من البروتوكولات SMB, LDAP للتحرك والنشر عبر الشبكات.
- TabDll: استغلال الثغرة EternalRomance من أجل عمليات النشر عبر البروتوكول SMB

التوصيات والحماية Recommendations and Mitigations

1. تنصيب تطبيقات مكافحة البرمجيات الخبيثة والتأكد من تحديثها بشكل مستمر ودائم.
2. تعطيل تنفيذ وحدات Macros باستثناء تلك الموقعة رقمياً.
3. تحميل وتطبيق تحديثات أنظمة التشغيل بشكل مستمر.

4. وضع وتطوير سياسات أمنية مناسبة وبشكل خاص سياسة لاستخدام البريد الالكتروني تتضمن إبلاغ التقنيين المعنيين عن أي رسالة مشبوهة بشكل فوري.
5. وسم الرسائل الالكترونية القادمة من مصادر خارجية بإشارات أو علامات واضحة لتنبيه المستخدمين بأن يتوخوا الدقة والحذر في التعامل مع هذه الرسائل.
6. تطبيق قواعد التصفية Filters على مخدمات وبوابات البريد الالكتروني، وتحديثها بشكل مستمر.
7. حجب العناوين الرقمية المشبوهة بواسطة الجدران النارية.
8. تطبيق برتوكول المصادقة والتحقق DMARC، وهو عبارة عن بروتوكول يستخدم العديد من التقنيات كالتوقيع الرقمي وذلك للتأكد من هوية المرسل وصحة الرسالة.
9. إجراء دورات تدريبية مستمرة ووافية للمستخدمين على المواضيع الأمنية ذات الصلة كمواجهة هجمات التصيد الالكتروني وهجمات الهندسة الاجتماعية.
10. اعتماد سياسات المجموعات Group Policy، بحيث يتم توزيع السماحيات على المستخدمين كلٍ بحسب حاجته فقط وتقييد السماحيات الإدارية بعدد محدود قدر الإمكان.
11. في حال فتح رابط مشبوه أو تشغيل ملف يُعتقد باحتوائه على برنامج خبيث:
    - قطع الاتصال الشبكي عن الحواسب التي يشتبه بإصابتها.
    - إبلاغ التقنيين المعنيين كمدراء الشبكات والدعم الفني.
    - إجراء مسح شامل عن البرمجيات الخبيثة ضمن هذه الحواسب.
    - تغيير بيانات الدخول سواءً المحلية أو عبر متحكمات المجال بالإضافة إلى بيانات الدخول للتطبيقات الأخرى وخاصة تلك التي تجري المصادقة عبر الانترنت.
    - محاولة تحديد طريقة الإصابة وتوثيق كل ذلك في سجلات خاصة.

References المصادر

دراسات وأبحاث

CIS: Center for Internet Security: www.cisecurity.org

ماجد عبد المجيد اسماعيل

Digitally signed by ماجد عبد المجيد اسماعيل
DN: C=SY, OU=مركز أمن المعلومات, O=National Agency for Network Services (NANS), OID.0.9.2342.19200300.100.1.1=03170004738, CN=ماجد عبد المجيد اسماعيل
Reason: I am the author of this document
Location:
Date: 2019-04-24 14:05:10

سلمان علي سليمان

Digitally signed by سلمان علي سليمان
DN: c=SY, ou=مركز أمن المعلومات, o=National Agency for Network Services (NANS), 0.9.2342.19200300.100.1.1=101700 09529, cn=سلمان علي سليمان
Date: 2019.04.25 11:01:13 +03'00'