التي تستفيد من مبدأ التواطؤ. تجمع Facebook نكتشف نظامًا بيئيًا مزدهرًا من التلاعب بالسمعة على نطاق واسع الخدمات على من الأعضاء المتواطئين وإساءة استخدامها لتقديم اعجاب وهمية أو OAuth شبكات التواطؤ الرموز المميزة للوصول إلى تعليقات على أفراد. نتسلل إلى شبكات التواطؤ الشائعة باستخدام مصائد مخترقي الشبكات وتحديد أكثر من مليون متعاطف على الفيسبوك الحسابات عن طريق "حلب" شبكات التواطؤ هذه. نحن نكشف نتائجنا على الفيسبوك والتعاون معهم لتنفيذ سلسلة من للوصول دون التضحية قابلية استخدام منصة التطبيق OAuth الإجراءات المضادة التي تعمل على تخفيف إساءة استخدام رمز مجموعة من التغييرات غير ذات الصلة في بنيتها التحتية لمواجهة شبكات التواطؤ. نحن Facebook لطرف ثالث وبعدها نفذ واسع النطاق وتخفيفه بشكل فعال سوء المعاملة في البرية. أصبحت الشبكات الاجتماعية OAuth الأول للإبلاغ عن رمز وصول عبر الإنترنت الطريقة الأساسية للاتصال بين الأشخاص والتواصل مع بعضهم البعض ، السمعة هي العقيدة الأساسية الاجتماعية على الإنترنت الشبكات. ينتشر الاحتيال على مستوى سمعته عبر الإنترنت شبكات اجتماعية. تعتمد هذه الخدمات على عدد كبير من الإنترنت حسابات الشبكة الاجتماعية لإجراء التلاعب في سمعة في مقياس. أو تجند المستخدمين للانضمام إلى التواطؤ الشبكات [58]. تحاول الشبكات الاجتماعية على الإنترنت مواجهة التلاعب بالسمعة الأنشطة على المنصات الخاصة بهم عن طريق إزالة الإعجابات وهمية وتعليق حسابات مشبوهة. الدفاع ضد التلاعب بالسمعة الاحتيالية هو سباق التسلح المستمر بين المحتالين ومشغلي الشبكات الاجتماعية. لفهم مدى تشكل شبكات التواطؤ المشكلة ، تواطؤ الشبكات التي تجمع رموز وصول ثم يتم استخدام رموز الوصول هذه للقيام بأنشطة نيابة عن هذه .OAuth 2 للتطبيقات التي تستخدم الوضع الضمني في OAuth التطبيقات وتواطؤ الحسابات. توفر شبكات التواطؤ الإعجابات والتعليقات لأعضائها على أساس الطلب. الوصول إلى تسرب الوصول إلى تسرب رمزي وإساءة الاستخدام. OAuth رمزي وإساءة استخدام شبكات التواطؤ. نحن أول من أبلغ عن نطاق واسع لإجراء دراسة قياس واسعة النطاق على الفيسبوك شعبية شبكات التواطؤ.Honeypots شبكات التكاثر بالحلب باستخدام والانضمام إلى شبكات التواطؤ ، نحن بعد ذلك مراقبة وتحليل مصائد مخترقي الشبكات لدينا لفهم الاستراتيجيات تستخدمها شبكات التواطؤ للتلاعب بالسمعة. نحدد حجم العضوية في التواطؤ الشبكات عن طريق تتبع عدد الحسابات الفريدة التي تحب والعمل معهم للتخفيف من هذه التلاعب في السمعة المستندة إلى التواطؤ Facebook نكشف عن النتائج التي توصلنا إليها على خدمات. على سبيل المثال ، لا نقوم بحظر تطبيقات الطرف الثالث التي يتم استغلالها بواسطة شبكات التواطؤ لأنها سوف تؤثر والأنظمة الذاتية IP سلبًا على الملايين من المستخدمين الشرعيين. نحن نقيم حدودًا إضافية ونضع قائمة سوداء في عناوين تثبت كيف شبكات التواطؤ We .المستخدمة من قبل شبكات التواطؤ لوقف عملياتها تماما المساهمات الرئيسية (ASes) الخاصة بجهات خارجية ذات شعبية ضعيفة إعدادات الأمان لاسترداد الرموز المميزة للوصول إلى Facebook استغلال تطبيقات وإساءة الاستخدام لهم لتلاعب سمعة. لدينا تدابير مضادة قادرة على وقف عمليات شبكة التواطؤ دون الحاجة إلى أي OAuth الإطار. يناقش نحن تصف لنا مصيدة نشر لقياس شبكات التواطؤ الأنشطة. نستعرض الأعمال ذات الصلة OAuth تعديلات على في هذا القسم ، والترفيه ، والتعليم ، والمرافق ، عشرات الملايين من المستخدمين النشطين ويقومون بعمليات القراءة والكتابة والذي يسمح لتطبيقات الطرف [30] 0 .OAuth 2 إطار تفويض Facebook بشكل روتيني العمليات نيابة عن مستخدميها. ينفذ الثالث بالحصول على قيود الوصول إلى حسابات المستخدمين دون مشاركة بيانات اعتماد المصادقة (على سبيل المثال ، هذا الوصول الرمز المميز عبارة عن سلسلة مبهمة تحدد بشكل فريد مستخدم و يمثل نطاق إذن محددًا مُمنحًا للتطبيق لتنفيذ إجراءات موافقة. النوع الثاني من الأذونات Facebook القراءة / الكتابة نيابة عن المستخدم. النوع الأول من الأذونات الأساسية لا يتطلب الحساسة على سبيل المثال ، وتوليد الإعجابات والتعليقات. 2 كلا سير العمل تتشابه مع بعض التغييرات في معلمات الطلب تطبيق المعرف هو معرف فريد يتم تعيينه لكل .OAuth 2 وبعضها خطوات إضافية في تدفق جانب الخادم. يوضح الشكل 1 تدفق إعادة التوجيه في التطبيق إعدادات. يتم تعيين نوع الاستجابة على أنه "رمز مميز" لإرجاع URI تم تكوين .Facebook تطبيق الوصول الرمز المميز في تدفق من جانب العميل ويتم تعيينه كـ "رمز" لإرجاع رمز التفويض في تدفق من جانب الخادم. يتضمن الطلب معرف التطبيق ، طلب تبادل رمز ترخيص للوصول ثم يتم استخدام الرموز المميزة للوصول من قبل التطبيقات المراد تنفيذها مطلوب عموما طلب لتمرير التطبيق المعرّف وسر التطبيق ورمز الوصول المقابل. كما هو مبين في الشكل 2 (أ) ، يوفر خيارًا لتعطيل تدفق العميل من إعدادات التطبيق. عادةً ما يسمح بالتدفق من جانب العميل بالتطبيقات التي تجعل من Facebook مكالمة فقط من جانب العميل. قد لا يكون بعض التطبيقات من جانب العميل تطبيقًا Google من Graph واجهة برمجة تطبيقات

فقط من المتصفح كما هو موضح في الشكل 2 (ب) ، 49 ، 54 Graph الخادم على الإطلاق وتنفيذ طلبات واجهة برمجة تطبيقات URL نحن استرجاع الرمز المميز للوصول من جانب العميل من التطبيق عنوان ، UAuth redirection URI ، 54] ، باستخدام لتسجيل الدخول. المدى القصير تشكل الرموز المميزة للوصول تهديدًا محدودًا نظرًا لأنها مطلوبة ليتم تحديثها بعد كل 1–2 ساعة.

كما ناقشنا من قبل ، التطبيقات الحساسة ذات النفاذ الطويل الأجل الرموز المميزة بين أفضل 100 تطبيق colllon 3 شبكات نحن نجمع قائمة من هذه المواقع واستخدام اليكسا [2] لتلخيص التواطؤ شعبية الشبكات. حيث يتم تصنيفها ضمن .Facebook المواقع. من المثير للاهتمام أن نلاحظ أن شبكات التواطؤ الأخرى قد حصلت أيضًا معظم حركة المرور الخاصة بهم Kأعلى 3 من دول مثل الهند ومصر وتركيا ، وفيتنام. نحن نحقق في شبكات التواطؤ الشائعة لفهم الميزات التي تقدمها والتعرف على تطبيقات الفيسبوك أنهم استغلال. يسرد الجدول 3 التطبيقات المستخدمة من قبل شبكات التواطؤ الشعبية جنبا إلى جنب مع في المرتبة 40 ولديها ترتيب مليون مستخدم .Facebook إحصاءاتها استردادها من واجهة برمجة تطبيقات الرسم البياني على وبالمثل ، سوني اريكسون الهاتف الذكي في المرتبة 886 ولديها ترتيب من عشرة آلاف يوميا المستخدمين .(DAU) نشط يوميًا Facebook النشطين. من الجدير بالذكر أن شبكات التواطؤ لا يمكن أن تخلق واستخدام تطبيقاتهم الخاصة لأنهم لن يمروا على عملية مراجعة يدوية صارمة للتطبيقات التي تتطلب إرسال الأذونات [3]. معظم شبكات التواطؤ لديها واجهة ويب مماثلة وأنها توفر كل مستخدم مماثل إلى حد ما تجربة. يوضح الشكل 3 سير العمل في تواطؤ فيس بوك الشبكات. يزور أحد المستخدمين موقع الويب الخاص بشبكة التواطؤ وينقر عليه الزر لتثبيت التطبيق. الموقع يعيد التوجيه ال يطلب من المستخدم منح الأذونات المطلوبة وتثبيته تطبيق. ● يعود المستخدم إلى موقع شبكة التواطؤ بعد التثبيت التطبيق والنقر على الزر لاسترداد رمز الوصول.

يقوم مربع حوار التخويل بإعادة توجيه المستخدم إلى صفحة يحتوي على الرمز المميز للوصول كسلسلة استعلام في عنوان لاستخدامها كصناديق نشيطة نشطة لدراسة التواطؤ الشعبي الشبكات. في Facebook نسجل 22 حساب جديد على .URL بانتظام تحديثات الحالة في المخططات الزمنية وطلب honeypot محاولة لإشراك شبكات التواطؤ بشكل نشط ، تنشر حسابات تفرض بعض شبكات التواطؤ تأخيرات ثابتة أو عشوائية بين .them شبكات التواطؤ لتقديم إبداءات الإعجاب / التعليقات على من أجل تسجيل الدخول وقبل كل طلب. CAPTCHA طلبين متتاليين. تتطلب العديد من شبكات التواطؤ من المستخدمين حل تلقائيًا [19] لـ تقديم الطلبات لشبكات Selenium و CAPTCHA لحل أوتومات [4] CAPTCHA فإننا نستخدم خدمة حل التواطؤ. نحن نشر باستمرار تحديثات الحالة وطلبات شبكات التواطؤ على مدار المدة ما يقرب من ثلاثة أشهر من نوفمبر 2015 لتسجيل الإعجابات Facebook إلى فبراير عام 2016. نحن نزحف بانتظام إلى المخططات الزمنية لمصيدة لدينا حسابات والتعليقات الواردة المقدمة لاحظ أن تقدير العضوية لدينا هو بدقة أقل لأننا قد لا نلاحظ كل التواطؤ حسابات الشبكة ، نقوم أيضًا بالزحف إلى سجلات الأنشطة الخاصة بمصيدة لدينا حسابات لجمع الإعجابات والتعليقات الصادرة على وجه التحديد، بسبب و com إلى عن على .honeypot أخذ عينات عشوائية من المستخدمين من قاعدة بيانات الوصول ، تحديثات الحالة لحساب بسعر 178 كيلوبايت. ال حجم عضوية جميع شبكات التواطؤ في دراستنا تلخيص إلى 1، بعض الحسابات monkeyliker. com لكل منها مئات الآلاف من الأعضاء (انظر .goo مثل كما يوفر URL جزء من متعددة شبكات التواطؤ. 008, 021 خدمات تقصير الطويل. قد لا تعطينا أعداد النقرات هذه URL الجدول4). نلاحظ أن العديد من عناوين المواقع القصيرة تشير إلى نفس عنوان ما يقرب من 400 و 250 و 100 إعجاب لكل طلب ، على myliker. com وتقدم .f8–autoliker ، تقديرًا دقيقًا في المجمل يحب على مشاركات 1. العديد من شبكات التواطؤ تقدم أيضا خدمات "التعليق 8K. autolike ، التوالي. على سبيل المثال التلقائي". مطلوب من المستخدمين لتحديد الوظائف المستهدفة للحصول على تعليقات. نلاحظ أن شبكات التواطؤ توفر ما معدله 16 شبكة فقط التعليقات لكل منشور. من الجدير بالذكر أن العدد الإجمالي للفريدة التعليقات تشكل جزءًا صغيرًا من جميع التعليقات المقدمة من قبل شبكات التواطؤ. (ب) الاستخدام غير الضروري لعلامات الترقيم مثل "؟؟ رائع ؟؟؟ ؟؟؟؟؟؟؟ ؟؟؟؟ "، نستنتج ذلك التواطؤ شبكات توليد عدد قليل جدا من التعليقات الفريدة محدودة مفردات اللغه. 5.1 تسييل يستخدم مشغلو شبكات التواطؤ آليتين رئيسيتين لتحقيق الدخل خدماتهم: (1) الإعلان و (2) خطط قسط التأمين. إعلان. تجذب شبكات التواطؤ عددًا كبيرًا من المستخدمين لمواقعهم كل يوم. أذكر من الجدول رقم 5 ذلك تعرض شبكات التواطُع إعلانات مختلفة شبكات الإعلانات لاستثمار حركة المستخدم على مواقعهم على الويب. نحن تحديد شبكات الإعلانات والتعقب على مواقع شبكة التواطؤ للتغلب على هذه المشكلة ، العديد من شبكات التواطؤ استخدام عمليات إعادة ، DoubleClick مثل .[9] Ghostery باستخدام

لإعادة توجيه المستخدمين مؤقتًا إلى مستخدمين آخرين نطاقات القائمة البيضاء والإعلانات الصورية من URL توجيه عناوين بعض شبكات التواطؤ إعادة توجيه إلى خدمات تقصير .mg-likers شبكات إعلانات مختلفة على الصفحة المعاد توجيهها. يقوم خطط ممتازة. فمثلا، تبيع شبكات التواطؤ خططًا متميزة تسمح بذلك المستخدمين للحصول على .adf مدفوعة مثل مثل URL هم .mg-likers المزيد من إبداءات الإعجاب / التعليقات والتغلب على القيود الأخرى حتى عام 2000 يحب لخطة أغلى من قبل ايضا تقدم تلقائيا يحب دون الحاجة للمستخدمين يدويا تسجيل الدخول إلى مواقع شبكة التواطؤ لكل طلب. نلاحظ أن مواقع شبكة التواطؤ تستخدم مختلفًا تقنيات لإخفاء هويتهم. للبقية شبكات التواطؤ ، في الواقع ، نشير إلى ذلك أن معلومات المسجل com .و يمكن أن يتم تنظيم حسابات وسائل التواصل الاجتماعي من قبل المالكين الفعليين WHOIS المستخرجة من سجلات لدينا هي في كثير من honeypot كان لديه أكثر من 9 مليون متابع في وقت هذه الكتابة. ومن الجدير بالذكر أيضا أن حسابات الأحيان تستخدم لإعجاب صور الملف الشخصي وغيرها من منشورات الجدول الزمني لهذه حسابات الفيسبوك. 6 متلازمة نحن لأننا نجمع بعض معلومات الحساب المتاحة للعامة مثل (IRB تلقى مراجعة رسمية من مجلس المراجعة المؤسسية المحلي لدينا لإزالة كل التحف من التلاعب بالسمعة خلال القياسات وكذلك Facebook المشاركات وإبداءات الإعجاب. نفصح عن نتائجنا إلى التحقيق في التدابير المضادة للتخفيف أنشطة شبكة التواطؤ. نجري تجارب مصيدة لـ تقريبا عشرة أيام لإنشاء خط الأساس للتواطؤ الشعبي الشبكات ابتداء من أغسطس 2016 (وتستمر حتى honeypot لأنشطة شبكة التواطؤ. نحن كرر تجارب حلب لشعبين تواطؤ شعبية . في honeypots منتصف أكتوبر يوضح الشكل 5 متوسط عدد عمليات الإعجاب التي تم تلقيها بواسطة حين أننا نعتبر مجموعة واسعة من التدابير المضادة ، فإننا نقرر لتنفيذ التدابير المضادة التي توفر مقايضة مناسبة بين الكشف عن إساءة استخدام رمز الوصول ومنصة التطبيق قابلية الاستخدام لمطوري الجهات الخارجية. تستغل شبكات التواطؤ حاليًا بعض التطبيقات (المدرجة في القائمة في الجدول 3) للقيام بأنشطة التلاعب بالسمعة. تعليق هذه التطبيقات هو نسبيا مضاد بسيط لتنفيذ ؛ يمكننا تفويض سر التطبيق (وبالتالي فرض عمليات جانب الخادم) لتروق / تعليق الأنشطة 18]. لن تكون شبكات التواطؤ قادرة على القيام بسمعة أنشطة التلاعب حتى لو كانوا يستردون رموز الوصول من تواطؤ المستخدمين. 6.1 الوصول إلى حدود معدل الرمز المميز نحن نحد من الحد الأقصى للسعر بأكثر من مبلغ من الحجم في اليوم 12 كما هو ملحوظ من قبل الدوائر liker. 6.2 Honeypot based Access Token_الخضراء في الشكل 5. فإن المتوسط عدد من الإعجابات المقدمة من الرسمي نتوقع أن إبطال هذه الرموز الوصول سيحد من أنشطة شبكة التواطؤ. نقوم بإبطال عينة .official-liker و Invalidation me عشوائية 50٪ من رموز الوصول المحلاة في يوم 23 كما هو ملحوظ من قبل الصليب الأسود في الشكل 5. 5 نلاحظ هذا الانخفاض لم يكن دائما ومتوسط عدد يحب زيادة تدريجيا مرة أخرى خلال الأيام القليلة المقبلة.