

نكتشف نظاماً بيئياً مزدهراً من التلاعب بالسمعة على نطاق واسع الخدمات على Facebook التي تستفيد من مبدأ التواطؤ. تجمع شبكات التواطؤ الرموز المميزة للوصول إلى OAuth من الأعضاء المتواطئين وإساءة استخدامها لتقديم إعجاب وهمية أو تعليقات على أفراد. نتسلل إلى شبكات التواطؤ الشائعة باستخدام مصادم 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 الإجراءات المضادة التي تعمل على تخفيف إساءة استخدام رمز OAuth للوصول دون التوضيح قابلية استخدام منصة التطبيق لطرف ثالث وبعدها نفذ Facebook مجموعة من التغييرات غير ذات الصلة في بنيتها التحتية لمواجهة شبكات التواطؤ. نحن الأول للإبلاغ عن رمز وصول OAuth واسع النطاق وتخفيفه بشكل فعال سوء المعاملة في البرية. أصبحت الشبكات الاجتماعية 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 الاحتمالية هو سباق التسلح المستمر بين المحتالين ومشغلي الشبكات الاجتماعية. لفهم مدى تشكل شبكات التواطؤ المشكلة ، توواطؤ الشبكات التي تجمع رموز وصول OAuth للتطبيقات التي تستخدم الوضع الضمني في OAuth 2. ثم يتم استخدام رموز الوصول هذه للقيام بأنشطة نيابة عن هذه التطبيقات وتواطؤ الحسابات. توفر شبكات التواطؤ الإعجابات والتعليقات لأعضائها على أساس الطلب. الوصول إلى تسرب رمزي وإساءة استخدام شبكات التواطؤ. نحن أول من أبلغ عن نطاق واسع OAuth الوصول إلى تسرب رمزي وإساءة الاستخدام. شبكات التكاثر بالحلب باستخدام Honeypots إجراء دراسة قياس واسعة النطاق على الفيسبوك شعبية شبكات التواطؤ. والانضمام إلى شبكات التواطؤ ، نحن بعد ذلك مراقبة وتحليل مصادم مخترقي الشبكات لدينا لفهم الاستراتيجيات تستخدمها شبكات التواطؤ للتلاعب بالسمعة. نحدد حجم العضوية في التواطؤ الشبكات عن طريق تتبع عدد الحسابات الفريدة التي تحب نكشف عن النتائج التي توصلنا إليها على Facebook والعمل معهم للتخفيف من هذه التلاعب في السمعة المستندة إلى التواطؤ خدمات. على سبيل المثال ، لا نقوم بحظر تطبيقات الطرف الثالث التي يتم استغلالها بواسطة شبكات التواطؤ لأنها سوف تؤثر سلباً على الملايين من المستخدمين الشرعيين. نحن نقيم حدوداً إضافية ونضع قائمة سوداء في عناوين IP والأنظمة الذاتية (ASes) المستخدمة من قبل شبكات التواطؤ لوقف عملياتها تماماً المساهمات الرئيسية. We تثبت كيف شبكات التواطؤ استغلال تطبيقات Facebook الخاصة بجهات خارجية ذات شعبية ضعيفة إعدادات الأمان لاسترداد الرموز المميزة للوصول إلى OAuth وإساءة الاستخدام لهم لتلاعب سمعة. لدينا تدابير مضادة قادرة على وقف عمليات شبكة التواطؤ دون الحاجة إلى أي تعديلات على OAuth الإطار. يناقش نحن تصف لنا مصيدة نشر لقياس شبكات التواطؤ الأنشطة. نستعرض الأعمال ذات الصلة في هذا القسم ، والترفيه ، والتعليم ، والمرافق ، عشرات الملايين من المستخدمين النشطين ويقومون بعمليات القراءة والكتابة بشكل روتيني العمليات نيابة عن مستخدميها. ينفذ Facebook إطار تفويض [30] OAuth 2. 0 والذي يسمح لتطبيقات الطرف الثالث بالحصول على قيود الوصول إلى حسابات المستخدمين دون مشاركة بيانات اعتماد المصادقة (على سبيل المثال ، هذا الوصول الرمز المميز عبارة عن سلسلة مبهمه تحدد بشكل فريد مستخدم ويمثل نطاق إذن محدوداً مُمَنحاً للتطبيق لتنفيذ إجراءات القراءة / الكتابة نيابة عن المستخدم. النوع الأول من الأذونات الأساسية لا يتطلب Facebook موافقة. النوع الثاني من الأذونات الحساسة على سبيل المثال ، وتوليد الإعجابات والتعليقات. 2 كلا سير العمل تتشابه مع بعض التغييرات في معلومات الطلب وبعضها خطوات إضافية في تدفق جانب الخادم. يوضح الشكل 1 تدفق OAuth 2. تطبيق المعرف هو معرف فريد يتم تعيينه لكل تطبيق Facebook. تم تكوين URI إعادة التوجيه في التطبيق إعدادات. يتم تعيين نوع الاستجابة على أنه "رمز مميز" لإرجاع 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 عموماً طلب لتمير التطبيق المعرف وسر التطبيق ورمز الوصول المقابل. كما هو مبين في الشكل 2 (أ) ، يوفر Facebook خياراً لتعطيل تدفق العميل من إعدادات التطبيق. عادةً ما يسمح بالتدفق من جانب العميل بالتطبيقات التي تجعل من واجهة برمجة تطبيقات Graph من Google مكاملة فقط من جانب العميل. قد لا يكون بعض التطبيقات من جانب العميل تطبيقاً



توجيه عناوين URL لإعادة توجيه المستخدمين مؤقتاً إلى مستخدمين آخرين نطاقات القائمة البيضاء والإعلانات الصورية من شبكات إعلانات مختلفة على الصفحة المعاد توجيهها. يقوم mg-likers. بعض شبكات التواطؤ إعادة توجيه إلى خدمات تقصير URL مدفوعة مثل مثل adf. خطط ممتازة. فمثلاً، تباع شبكات التواطؤ خطأً متميزة تسمح بذلك المستخدمين للحصول على المزيد من إبداءات الإعجاب / التعليقات والتغلب على القيود الأخرى حتى عام 2000 يحب لخطوة أعلى من قبل mg-likers. هم أيضاً تقدم تلقائياً يحب دون الحاجة للمستخدمين يدويا تسجيل الدخول إلى مواقع شبكة التواطؤ لكل طلب. نلاحظ أن مواقع شبكة التواطؤ تستخدم مختلفاً تقنيات لإخفاء هويتهم. للبقية شبكات التواطؤ ، في الواقع ، نشير إلى ذلك أن معلومات المسجل المستخرجة من سجلات WHOIS و يمكن أن يتم تنظيم حسابات وسائل التواصل الاجتماعي من قبل المالكين الفعليين. com كان لديه أكثر من 9 مليون متابع في وقت هذه الكتابة. ومن الجدير بالذكر أيضاً أن حسابات honeypot لدينا هي في كثير من الأحيان تستخدم لإعجاب صور الملف الشخصي وغيرها من منشورات الجدول الزمني لهذه حسابات الفيسبوك. 6 متلازمة نحن تلقى مراجعة رسمية من مجلس المراجعة المؤسسية المحلي لدينا (IRB) لأننا نجمع بعض معلومات الحساب المتاحة للعامة مثل المشاركات وإبداءات الإعجاب. نفصح عن نتائجنا إلى Facebook لإزالة كل التحف من التلاعب بالسمعة خلال القياسات وكذلك التحقيق في التدابير المضادة للتخفيف أنشطة شبكة التواطؤ. تجري تجارب مصيدة لـ تقريبا عشرة أيام لإنشاء خط الأساس لأنشطة شبكة التواطؤ. نحن نكرر تجارب حلب honeypot للتواطؤ الشعبي الشبكات ابتداء من أغسطس 2016 (وتستمر حتى منتصف أكتوبر يوضح الشكل 5 متوسط عدد عمليات الإعجاب التي تم تلقيها بواسطة honeypots لشعبيين تواطؤ شعبية . في 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 حالياً بعض التطبيقات (المدرجة في القائمة في الجدول 3) للقيام بأنشطة التلاعب بالسمعة. تعليق هذه التطبيقات هو نسبياً 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 الخضراء في الشكل 5. فإن المتوسط عدد من الإعجابات المقدمة من الرسمي -liker. 6.2 Honeypot based Access Token. Invalidation me و official-liker. نتوقع أن إبطال هذه الرموز الوصول سيحد من أنشطة شبكة التواطؤ. نقوم بإبطال عينة 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.