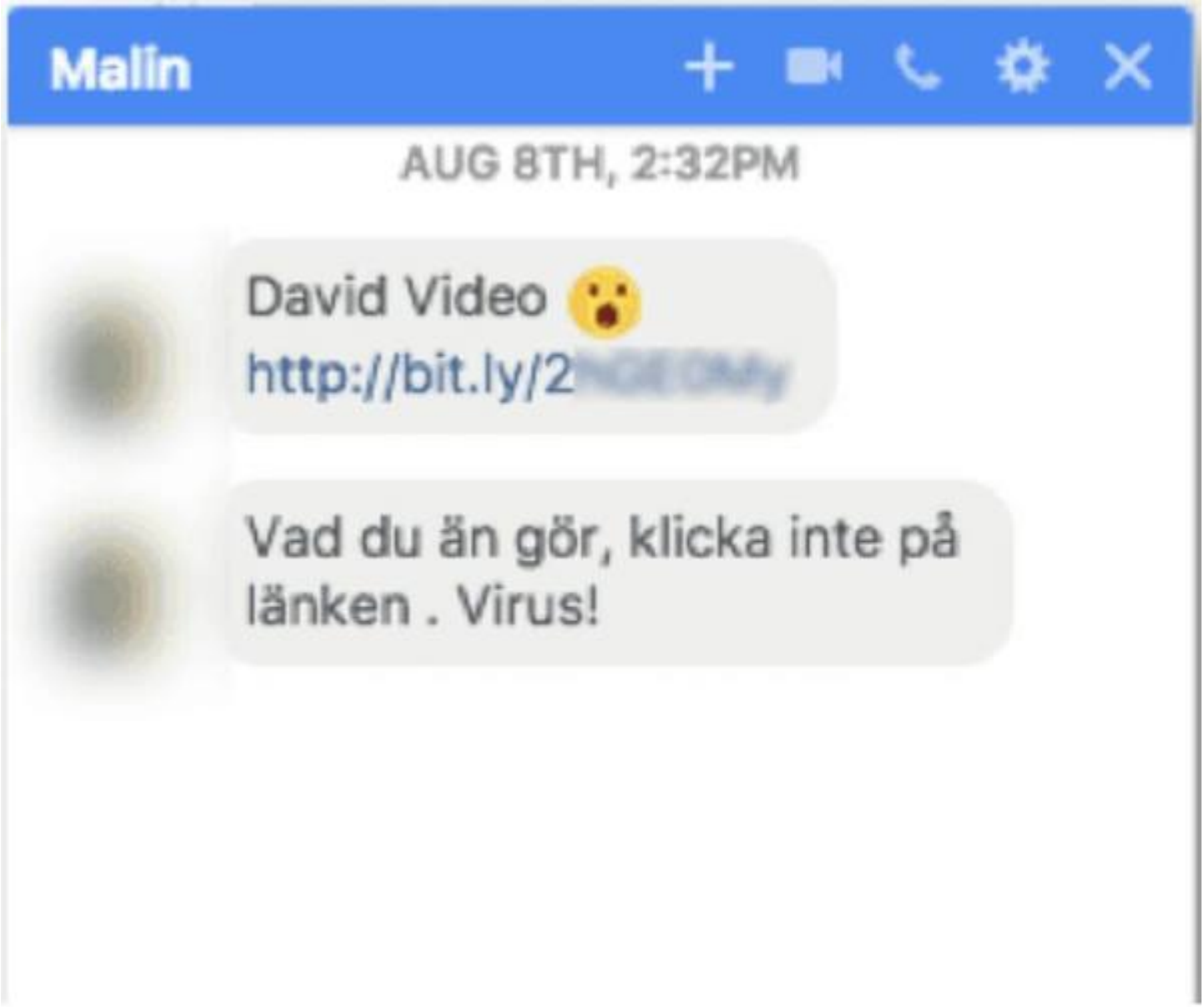
فيروس ماسنجر ينتشر عبر ويندوز، وماكنتوش، ولينكس



إياك والنّقر على رسالة فيسبوك Facebook تحتوي على فيديو مرسلة من أحد أصدقائك بصورته الشخصية.

هذا ما رصدته مختبرات كاسبرسكي **Kaspersky Labs**، حيث يتلقى مستخدمو فيسبوك رابط فيديو ينقلهم إلى موقع ويب مزيّف لتثبيت برامج الفيروس الخبيثة.



1

على الرغم من معرفة هذه الهجمة، إلا أنّ انتشار هذا الفيروس ما يزال غير واضح، حيث يعتقد الباحثون أن مُرسلي هذه الرسائل يستخدمون حسابات وهمية أو متصفحات مخترقة، وربما يستتخدمون تقنية **clickjacking** لنشر برمجياتهم الخبيثة.

ويستخدم المخترقون خاصية الهندسة الاجتماعية لخداع المستخدمين للنقر على رابط الفيديو، حيث يدّعي أنه أحد أصدقائهم على فيسبوك، مع رسالة معنونة بـ "<اسم صديقك> فيديو" يتبعها **bit.ly**، ورسالة أخرى تقول لك ألا تخبر أحداً آخر عن هذا الفيديو كونه سري.

وإليكم كيفية عمل هذه البرامج الخبيثة عبر المنصة

3

يُعيد عنوان الويب توجيه الضحايا إلى مستند غوغل، فيَعرض صورة مصغرة للفيديو على هيئة فِيلم قابل للتشغيل أُنشِئت بطريقة ديناميكية معتمداً على صور المرسِل، وعند النقر عليها يُنقل الضحية إلى صفحة ويب أخرى تختلف وفقاً للمتصفح ونظام التشغيل الخاص به.

على سبيل المثال، يُعاد توجيه مستخدمي موزيلا فايرفوكس **Mozilla Firefox** على ويندوز **Windows** إلى موقع ويب يعرض إشعاراً وهمياً لتحديث مشغل فلاش **Flash Player Update**، ثم يُعرض ملف ويندوز قابل للتنفيذ.

2

أما مستخدمو غوغل كروم **Google Chrome**، فيُنقلون إلى موقع ويب يتنكر على أنه يوتيوب **YouTube** ويحمل شعاراً مشابهاً له، ويعرض رسالة وهمية تخدع الضحية لتحميل برنامجاً ملحقاً **add-on** ضاراً لمتصفح الكروم من سوق غوغل الإلكتروني.

4

الحال لا يختلف كثيراً بالنسبة لمستخدمي نظام التشغيل الخاص بشركة أبل ماكنتوش **Mac OS** ومتصفحه سفاري **Safari**، حيث يُنقل المستخدم إلى صفحة ويب تشبه تلك التي نُقل إليها مستخدم نظام ويندوز عند استخدامه متصفح فايرفوكس، لكنها خُصصت لمستخدمي ماك، وعند النقر على رابط تحديث فلاش ميديا بلير الوهمي؛ يؤدي إلى تحميل ملف ذو امتداد **dmg..**

والحال نفسه يتكرر مع مستخدمي نظام ليونكس **Linux** حيث يُنقلون لصفحات خُصصت لمستخدمي هذا النظام.

ولا يستخدم المخترقون أي من حصان طروادة **Trojans** أوالتروجانات المصرفية **banking trojan**، بل يستخدمون برمجيات خبيثة **Adware** للحصول على المال الكثير عن طريق الربح من الإعلانات.

حملات الرسائل غير المرغوب بها **spam** ليست جديدة على الفيسبوك، بل معروفة منذ بضع سنين. حيث وجد الباحثون بأن مجرمي الإنترنت يخفون برمجياتهم الخبيثة في ملفات الصور ذات الامتداد **JPG**. حيث يقوم البرنامج الخبيث بتشفير جميع ملفات حاسوب الضحية، ولا يمكنه استرجاعها إلا بعد دفعه لفدية معينة، لكنها اليوم تأتي ببرمجيات أخرى وأشكال متطور.

للحفاظ على سلامتك

إذا كنت ترغب في تجنب فيروس الفيسبوك، يجب عليك الابتعاد عن الروابط المشبوهة التي تسعى لإثارة فضولك، وخصوصاً إذا كنت لا تتوقع رسالة من صديقك، فحينها يجب أن تتجاهل تقرير الرابط حول بعض الفيديوهات أو الصور.

وإذا كنت ممن لا يستطيعون مقاومة الفضول، أرسل لصديقك رسالة قبل النقر على الرابط المرسل لك واسأله فيما إذا كان هو المرسل أم لا. بالإضافة إلى ذلك، تجنب الوصول إلى كل لعبة أو تطبيق على الشبكة الاجتماعية، لأنه قد يكون اختراق من قبل مجرمي الإنترنت.

إذا خدعك فيروس الفيسبوك، يجب عليك تغيير كلمة السر الخاصة بحسابك في أسرع وقت ممكن من أجل تجنب سرقة هويتك وفقدان معلوماتك الشخصية. بالإضافة إلى ذلك، اتصل بأصدقائك وأخبرهم باختراق حسابك. وأخيراً، قم بتحميل برامج **Reimage** أو **Plumbytes Anti-Malware** لفحص حاسوبك ومنع تسلل البرامج الضارة. فهي تمكنك من إزالة فيروس الفيسبوك، وتظهر نتائجها في غضون عدة دقائق.

إذا كان فيروس الفيسبوك يزعجك، يرجى اتباع الخطوات التالية

التحقق من إعدادات التطبيق:

- تسجيل الدخول إلى حساب الفيسبوك الخاص بك والنقر على هذا المثلث الصغير على يمينك.
- انقر على الإعدادات لفتح نافذة إعدادات الحساب العامة.
- انظر إلى يسارك وحدد التطبيقات.
- انقر على زر 'تعديل' في خيارات التطبيقات ومواقع الويب والإضافات.
- حدد 'تعطيل' لحماية حسابك من الدخول غير المصرح به لتطبيقات الجهات الخارجية.

5

إذا أصبت بفيروس فيسبوك بالفيديو، فيجب إعادة تعيين غوغل كروم باتباع الخطوات التالية

- انتقل إلى إعدادات غوغل كروم.
- انتقل إلى متقدم أو **Advanced**.
- اختر إعادة تعيين.
- انقر على زر 'إعادة تعيين'.
- إحذف جميع الإضافات غير الضرورية وغير المعروفة لديك.

إذا كنت لا تزال تتلقى شكاوى حول الرسائل الضارة المرسلة من حسابك، فهذا يعني أن إعادة تعيين كروم لم يساعد على حذف الفيروس. في هذه الحالة، يجب إزالة كروم من الجهاز نظراً لأن هذا الإصدار من الفيروسات ينتشر عبر إضافات كروم التي قد يكون من المستحيل إزالتها.

تغيير كلمة مرور فيسبوك

- انقر على المثلث الصغير نفسه على يمينك.
- انقر على 'تعديل' بجوار خيار كلمة المرور.
- أدخِل كلمة المرور الحالية، ثم الجديدة. أعد كتابتها وحدد حفظ التغييرات.

- افحص جهاز الكمبيوتر الخاص بك مع برنامج للأمان.

ويوصى بإجراء مسح كامل للنظام لمنع حدوث المزيد من الضرر من فيروس الفيسبوك، وذلك عن طريق تشغيل 'مسح كامل' مع **Reimage** أو برامج مماثلة، سوف تضمن بذلك إزالة برمجيات طروادة وفيروسات الفدية وما شابه ذلك من البرامج الضارة التي انتشرت بمساعدة هذا الفيروس.

نصائح عامة

- لا تثق بأي روابط تصلك من أي شخص، ولاتقم بفتحها، وحاول تجنبها قدر المستطاع.
- ابتعد كل البعد عن المواقع التي تقوم بفتح نوافذ أخرى كنوافذ الإعلانات وغيرها.
- استخدامك لمضاد الفيروسات لا يعني أنك محمي تماماً من الفيروسات.

بهذه النصائح يمكنك تجنب فيروس ماسنجر الفيسبوك وغيره من الفيروسات الضارة.

- التاريخ: 2017-08-27
- التصنيف: تكنولوجيا

#الفيسبوك #البرمجيات الخبيثة #فيروسات الكمبيوتر #فيروس ماسنجر

المصادر

- thehackernews
- spyware-2

المساهمون

- ترجمة
  - سارة الراوي
  - رؤى سلامة
- تحرير
  - حسن شوفان
- تصميم
  - Tareq Halaby
- نشر
  - مي الشاهد