حمـلات از طریق پودمان DDE

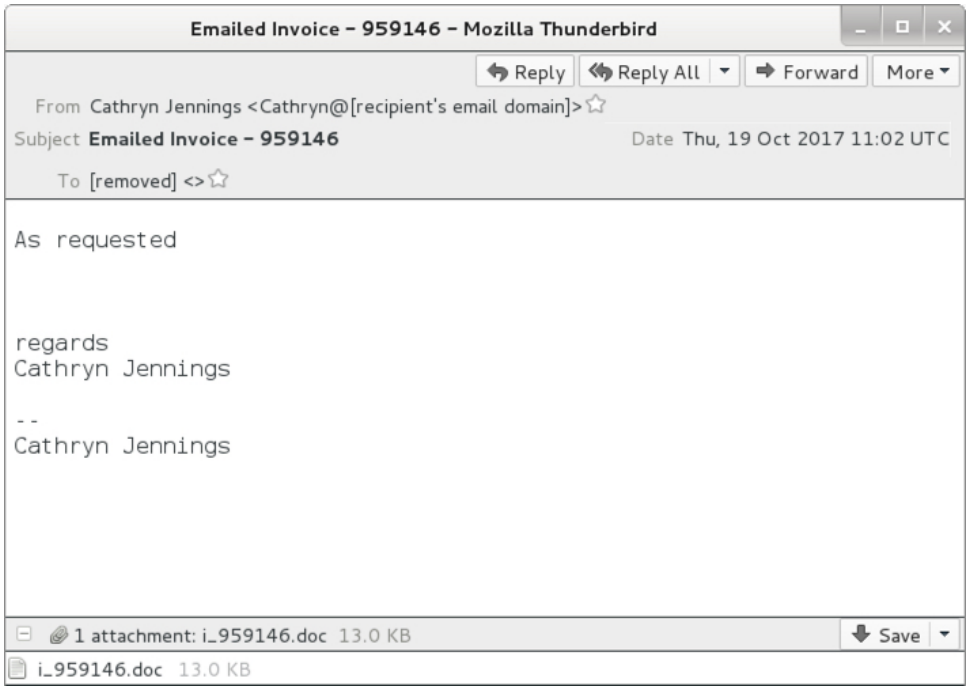
Dynamic Data Exchange

شبکه گستر
امنیت شما | وظیفه ما

نرم‌افزار Microsoft Office چندین روش انتقال و به اشتراک گذاری اطلاعات میان برنامه‌ها را ارائه می‌دهد. یکی از این روش‌ها Dynamic Data Exchange – به اختصار DDE – است. DDE پودمانی متشکل از مجموعه‌ای از پیام‌ها و راهنماهاست. این پودمان راهکاری برای به اشتراک گذاری داده‌ها و استفاده از حافظه‌ای مشترک برای تبادل داده‌ها میان چندین برنامه است.

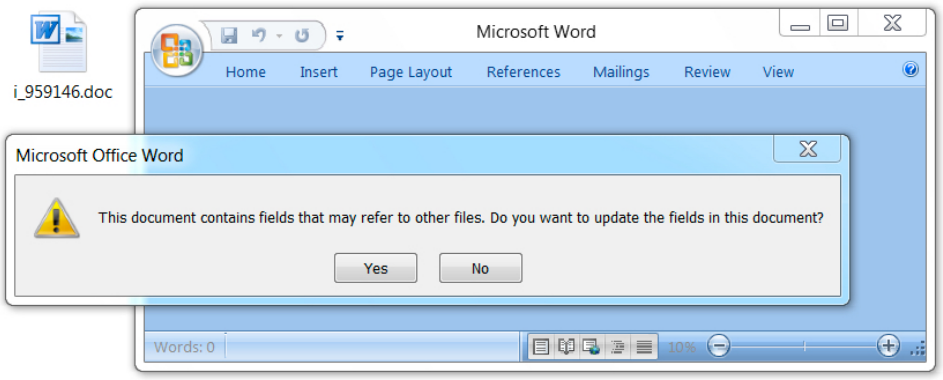
نمونه‌ای از حمله از طریق DDE

حمله‌ای را در تصور کنیم که در آن مهاجم با ارسال ایمیلی با عنوان و محتوای فریبنده و جذاب کاربر را تشویق به دریافت و اجرای فایل پیوست شده‌ای می‌کند که در آن کد مخرب با بهره‌جویی از پودمان DDE بر روی دستگاه اجرا می‌شود.



شکل ۱- نمونه‌ای از ایمیل حاوی فایل Word دستکاری شده

در این حمله، مهاجم باید کاربر را متقاعد به غیرفعال نمودن Protected Mode و یک یا چند کلیک بر روی پیام‌های ظاهر شده کند (شکل ۲).



شکل ۲- نمونه‌ای از پیام نمایش داده شده در نرم‌افزار Word در نتیجه وجود فیلد(های) مبتنی بر DDE

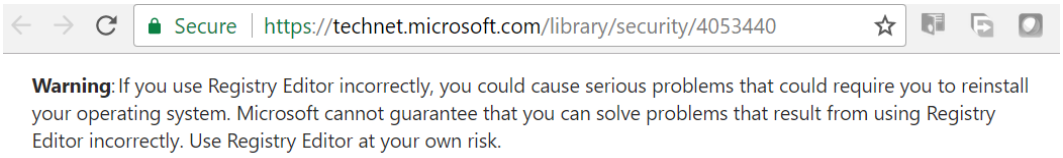
در صورت انجام اعمال مذکور توسط کاربر ناآگاه، کد مخرب به اجرا در آمده و با اتصال به سرور فرماندهی[۱] بدافزار را دریافت و بر روی دستگاه اجرا می‌کند.

[۱] Command and Control (C2)

پیشگیری از اجرای موفقیت‌آمیز حملات DDE

در نرم‌افزار Microsoft Office می‌توان از طریق چندین کلید کنترلی در Registry Editor که در ادامه این سند به آنها پرداخته شده تنظیمات مربوط به به‌روزرسانی از طریق DDE را مدیریت کرد.

هشدار! پیکربندی ناصحیح Registry Editor ممکن است اثرات مخربی بر روی سیستم عامل دستگاه بجا گذاشته و حتی سبب بالا نیامدن آن شود. مایکروسافت، خود نیز امکان حل مشکلات ناشی از پیکربندی نادرست Registry Editor را تضمین نمی‌کند (شکل ۳).



شکل ۳- هشدار مایکروسافت در خصوص خطر پیکربندی ناصحیح Registry Editor

در ادامه این سند متغیر <version> به عددی اشاره دارد که در جدول زیر با نسخه Office نصب شده بر روی دستگاه تطابق داده شده است.

نسخه مجموعه نرم‌افزاری Office	مقدار <version> در Registry Editor
Office 2007	12.0
Office 2010	14.0
Office 2013	15.0
Office 2016	16.0

جدول ۱- مقادیر معادل نسخه مجموعه نرم‌افزاری Office در Registry Editor

Microsoft Excel

برای جلوگیری از به‌روزرسانی خودکار داده‌ها در Excel (شامل DDE، OLE و سلول‌های خارجی[۲] و نامگذاری‌های تعریف شده[۳]) می‌بایست در مسیر زیر در رابط کاربری این نرم‌افزار، بخش Security settings for Workbook Links بر روی گزینه Disable automatic update of Workbook Links قرار داده شود (شکل ۴):

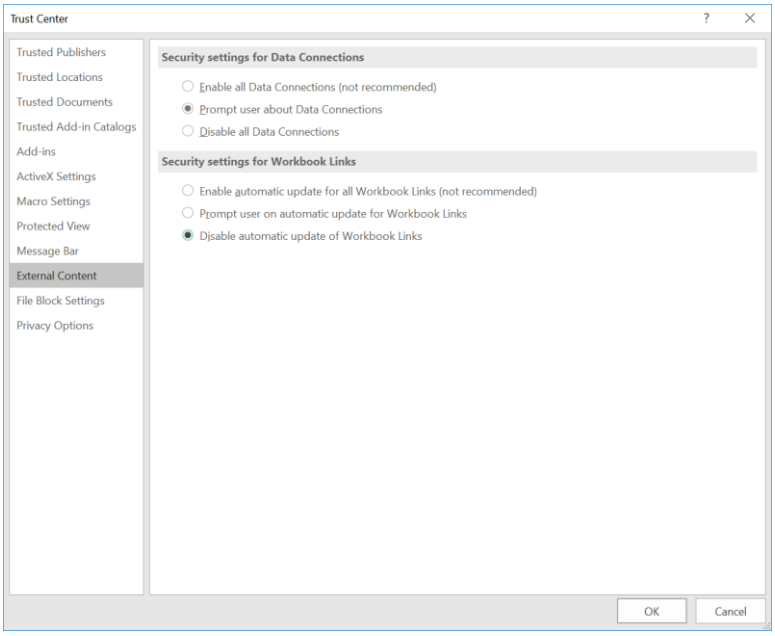
File -> Options -> Trust Center -> Trust Center Settings… -> External Content

برای غیرفعال نمودن از طریق Registry Editor نیز می‌بایست مقدار ۲ به کلید زیر تخصیص داده شود:

[KEY_CURRENT_USER\Software\Microsoft\Office\<version>\Excel\Security]
WorkbookLinkWarnings(DWORD) = 2

هشدار! غیرفعال نمودن این قابلیت ممکن است منجر به به‌روزنشدن خودکار داده‌های فایل شود. ضمن اینکه به کاربر نیز پیام‌هایی جهت یادآوری به‌روزرسانی محتوای فایل نمایش داده نخواهد شد.

[۲] External Cell
[۳] Defined Name References



شکل ۴- بخش مربوط به مدیریت نحوه به‌روزرسانی داده‌ها در رابط کاربری Excel

Microsoft Outlook

در نسخه 2010 نرم‌افزار Outlook و نسخه‌های بعد از آن برای غیرفعال نمودن به‌روزرسانی خودکار DDE می‌بایست مقدار ۱ به کلید زیر تخصیص داده شود:

[HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\Word\Options\WordMail]
DontUpdateLinks(DWORD)=1

در نسخه 2007 نیز باید مقدار ۱ به کلید زیر اختصاص داده شود:

[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\vpref]
fNoCalclinksOnopen_90_1(DWORD)=1

هشدار! اعمال این تنظیمات سبب غیرفعال شدن به‌روزرسانی خودکار فیلد DDE و لینک‌های OLE در نرم‌افزار Outlook می‌شود. هر چند کاربران همچنان می‌توانند با کلیک راست نمودن بر روی فیلد و انتخاب گزینه Update Field، داده‌ها را به‌روز کنند.

Microsoft Word

غیرفعال کردن به‌روزرسانی خودکار DDE در نسخه 2010 نرم‌افزار Word و نسخه‌های بعد از آن با اختصاص مقدار ۱ به کلید زیر امکان‌پذیر است:

[HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\Word\Options]
DontUpdateLinks(DWORD)=1

برای این منظور، در نسخه 2007 نیز باید به کلید زیر مقدار ۱ تخصیص داده شود:

[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\vpref]
fNoCalclinksOnopen_90_1(DWORD)=1

هشدار! اعمال تنظیمات مذکور، سبب غیرفعال شدن به‌روزرسانی خودکار فیلدهای DDE و OLE می‌شود. کاربران همچنان می‌توانند به‌روزرسانی را با کلیک راست بر روی فیلد و انتخاب گزینه Update Filed بصورت دستی انجام دهند.

Microsoft Publisher

جاسازی یک فایل Word حاوی کد مخرب مبتنی بر DDE در یک سند Publisher می‌تواند نمونه‌ای از روش حمله باشد. شما می‌توانید این راه را با غیرفعال کردن به‌روزرسانی خودکار DDE در نرم‌افزار Word مسدود کنید.

شبکه گستر
شـرکت مهندسی شـبـکه گسـتـر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

گروه فروش
داخلی ۱ ۴۲۰۵۲ | sales@shabakeh.net
گروه پشتیبانی
داخلی ۲ ۴۲۰۵۲ | support@shabakeh.net

تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net

شـناسـه سـند: SPT-E-0159-00