سوءاستفاده هکرها از ترس مردم از ویروس کرونا

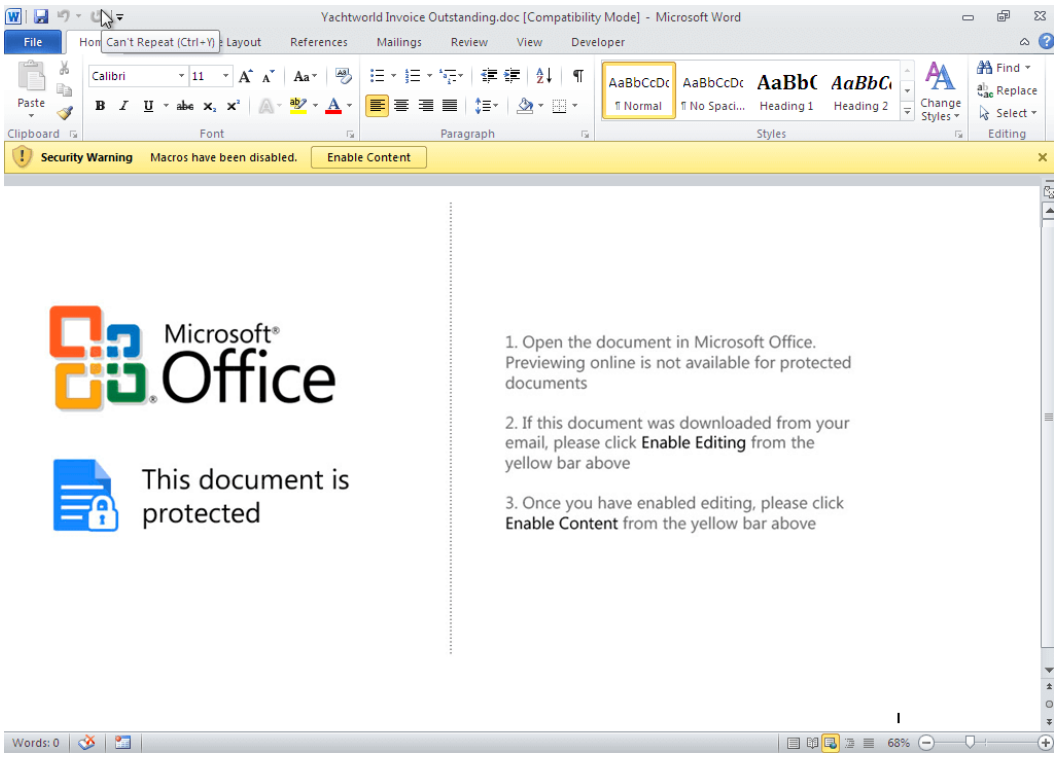
با توجه به شیوع ویروس کرونا که در این روزها بسیار مردم را وحشت زده کرده است هکرهای کلاه سیاه نیز از این موقعیت سوءاستفاده‌های خود را انجام داده و با استفاده از حملات گسترده مهندسی اجتماعی اقدام به سرقت اطلاعات و ... می‌کنند.

ترس از این ویروس باعث شده که مردم به مطالعه مستندات مختلف بپردازند تا اطلاعات خود را در مورد این ویروس و روشهای پیشگیری و ... آن افزایش دهند. حال هکرها از این موقعیت با ارسال ایمیل‌ها و مستندات آلوده انبوه مختلف با موضوعات تحریک‌آمیز و استفاده از شبکه‌های اجتماعی می‌توانند سوءاستفاده‌های لازم را به منظور دستیابی به اهداف خود داشته باشند که در زیر سعی می‌کنیم این روش‌ها را همراه با روش‌های مقابله نام ببریم:

- ایجاد مستندات Microsoft Office آلوده به بدافزار
- ایجاد مستندات PDF آلوده به بدافزار
- ایجاد لینک‌های آلوده به بدافزار
- ایجاد اپلیکیشن‌های آلوده
- ایمیل‌های آلوده و یا جعلی
- آسیب‌پذیری‌های سیستم‌عامل و نرم‌افزارها

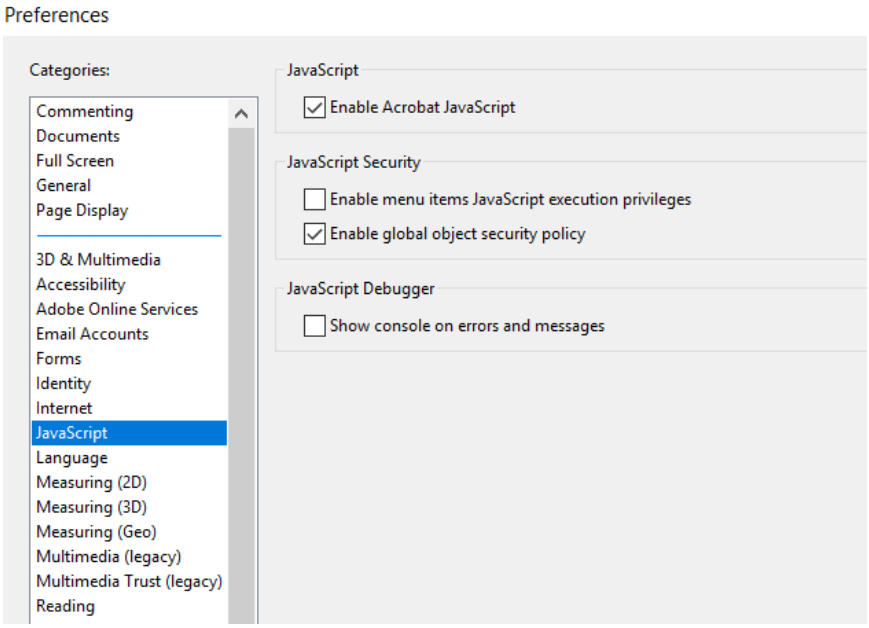
- **ایجاد مستندات Microsoft Office آلوده به بدافزار**

در صورتی که در فایل Word از کدهای VBA استفاده شده باشد پیغامی به شکل زیر برای کاربران نمایش داده می‌شود که از کاربر درخواست فعال کردن محتوای کدهای ماکرو را دارد. این کدها ممکن است که توسط هکر نوشته شده و حاوی یک کد مخرب باشد. پس در صورت اجرای فایل‌های مجموعه Microsoft Office به هیچ عنوان ماکروها را فعال نکنید.



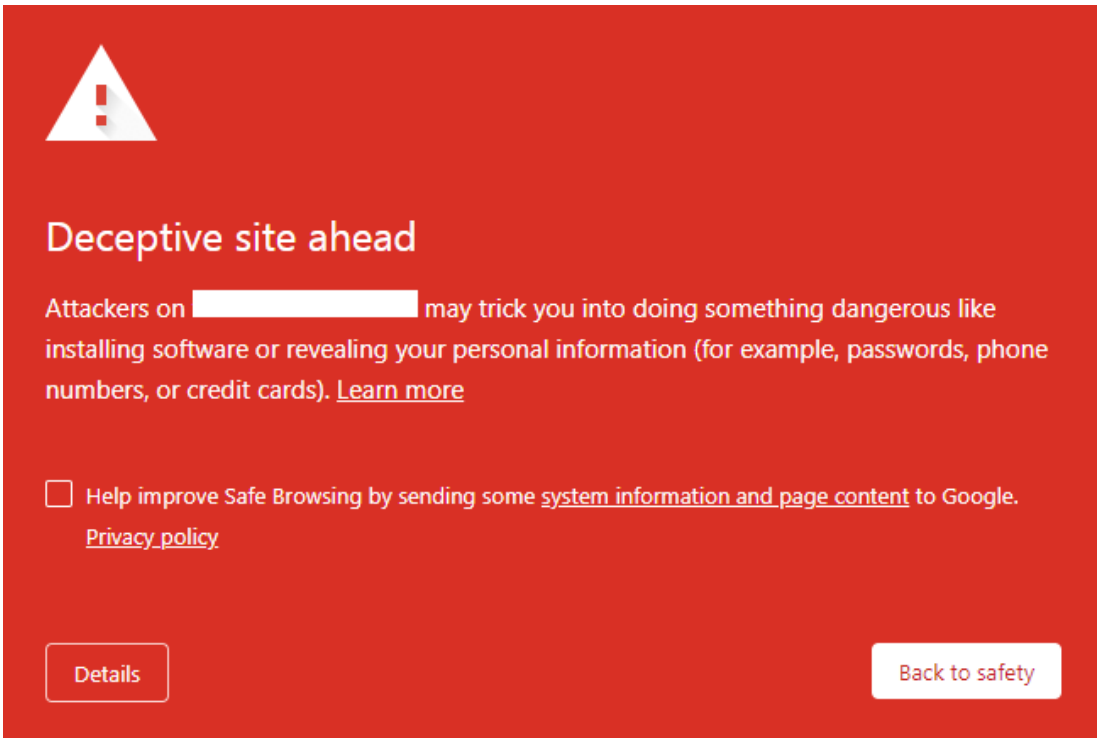
- **ایجاد مستندات PDF آلوده به بدافزار**

مستندات PDF هم قابلیت پشتیبانی از جاوا اسکریپت را دارند و همین امر باعث می‌شود که هکر این توانایی را داشته باشد که کدهای جاوا اسکریپت خود را در آن کپی و سپس ارسال نماید. برای جلوگیری از این موضوع طبق مورد نشان داده در شکل زیر تیک گزینه Enable Acrobat JavaSscript را بردارید.



- **ایجاد لینک‌های آلوده به بدافزار**

در حال حاضر برنامه‌نویس یک وب‌سایت می‌تواند از طریق اجرای کدهای جاوا در صفحه خاص وب‌سایت، اقدام به ارسال فایل به سمت سیستم کاربر نماید. به همین دلیل مرورگرهای جدید قابلیت شناسایی اینگونه وب‌سایت‌ها را دارند و در صورتی که با پیامی مانند شکل مواجه شدید فورا آن‌را ببندید.



جهت پیشگیری از این موضوع می‌توانید وب‌سایت آلوده را توسط ابزارهای آنلاین مختلفی که وجود دارد جهت شناسایی بدافزار در یک وب سایت پویش نمایید. وب‌سایت virustotal یکی از ابزارهایی است که برای ارزیابی امنیتی آدرس‌های مشکوک طراحی شده که در زیر آدرس آن قرار گرفته شده است.

Virustotal.com

- **ایجاد اپلیکیشن‌های آلوده**

اپلیکیشن‌هایی با اهداف خاص می‌تواند توسط هکرها طراحی شود و در شبکه‌های اجتماعی با نام‌های تحریک‌آمیز و اغواکننده به اشتراک گذاشته شود که حاوی یک بدافزار باشد که با باز کردن آنها امکان افشای اطلاعات شما وجود دارد. درنتیجه به کاربران توصیه می‌شود که از باز کردن و دانلود هرگونه برنامه مشکوک در شبکه‌های اجتماعی و سایت‌های غیرمعتبر جلوگیری به عمل آید و در صورت نیاز می‌توانید برنامه مشکوک را جهت پویش امنیتی به وب سایت virustotal.com دهید تا آلوده بودن و یا نبودن آن برای شما مشخص گردد.

همچنین توصیه می‌شود که انتی‌ویروس‌های خود را به روزنمایید تا در هنگام ورود اینگونه نرم‌افزارهای جعلی به سیستم توسط انتی‌ویروس شناسایی شود.

- **ایمیل‌های آلوده و یا جعلی**

ارسال یک ایمیل آلوده یا یک ایمیل جعلی بسیار ساده و بدون دردسر می‌باشد و یک مهاجم به سادگی می‌تواند اقدام به ارسال یک ایمیل آلوده نماید. در نتیجه اگر با یک ایمیل تحریک‌آمیز مواجه شدید موارد امنیتی که در ادامه به آنها می‌پردازیم را مد نظر داشته باشید.

ایمیل‌های جعلی از روی هدر آن‌ها قابل تشخیص می‌باشند. کافیست به مقدار مقابل عبارت SPF توجه نمایید. در صورتی که ایمیل جعلی نباشد مقدار آن کلمه Pass می‌باشد به شکل زیر:

```
Received-SPF: pass (Last token {ip4:167.89.99.122} (res=PASS)) client-ip=167.89.99.122; envelope-from=
<bounces+3427894-c712-m.haghighian=uok.ac.ir@delivery.tenable.com>; x-ip-name=o1678999x122.outbound-
mail.sendgrid.net;
Received: from o1678999x122.outbound-mail.sendgrid.net (unverified [167.89.99.122])
        by uok.ac.ir (SurgeMail 7.2d) with ESMTP (TLS) id 2603310-1301732
        for <m.haghighian@uok.ac.ir>; Wed, 05 Dec 2018 04:15:27 +0330
Return-Path: <bounces+3427894-c712-m.haghighian=uok.ac.ir@delivery.tenable.com>
```

و در صورتی که مقدار آن کلمه غیر از pass باشد مانند کلمه Fail به معنی جعلی بودن ایمیل و عدم ارسال آن توسط شخص صاحب ایمیل می‌باشد. به شکل زیر:

```
Received-SPF: none (Cache: No spf1 record for (certcc.ir) ) client-ip=94.182.27.34; envelope-from=
<taslimi@certcc.ir>; x-ip-name=94-182-27-34.shatel.ir;
X-Default-Received-SPF: fail (Last token {-all} (res=FAIL)) client-ip=94.182.27.34; envelope-from=
<taslimi@certcc.ir>; x-ip-name=94-182-27-34.shatel.ir;
Received: from DESKTOP-EHDP84T (unverified [94.182.27.34])
        by uok.ac.ir (SurgeMail 7.2d) with ESMTP (TLS) id 665374-1301732
        for <m.haghighian@uok.ac.ir>; Wed, 19 Jun 2019 14:28:45 +0430
```

نکته اول: بسیاری از ایمیل سرورهای قدرتمند، خود دارای سیستم قدرتمندی برای تشخیص ایمیل‌های جعلی می‌باشند و اینگونه ایمیل‌ها را در پوشه اسپم قرار می‌دهند.

نکته دوم: در صورت ارسال هرگونه فایل یا لینک مشکوک می‌توانید آنها را به وب سایت virustotal بدهید تا آن‌را ارزیابی نماید.

نکته سوم: از سرویس‌های ایمیل معتبر استفاده نمایید.

- **آسیب‌پذیری‌های سیستم‌عامل و نرم‌افزارها**

همواره آسیب‌پذیری‌های سیستم‌عامل از مهمترین عوامل برای انتقال یک بدافزار یا نفوذ به سیستم شما می‌باشد. شرکت‌های بزرگ کامپیوتری همیشه از طریق متخصصین خود به صورت حضوری و آنلاین اقدام به ارزیابی امنیتی محصول خود می‌کنند تا آسیب‌پذیری‌ها را به آنها گزارش دهند و تمامی آنها را در قالب به‌روزرسانی امنیتی برای کاربران خود ارسال می‌نمایند. پس بهترین روش برای جلوگیری از این نوع آسیب‌پذیری‌ها، به‌روزرسانی سیستم‌عامل و نرم‌افزارهای خود است.