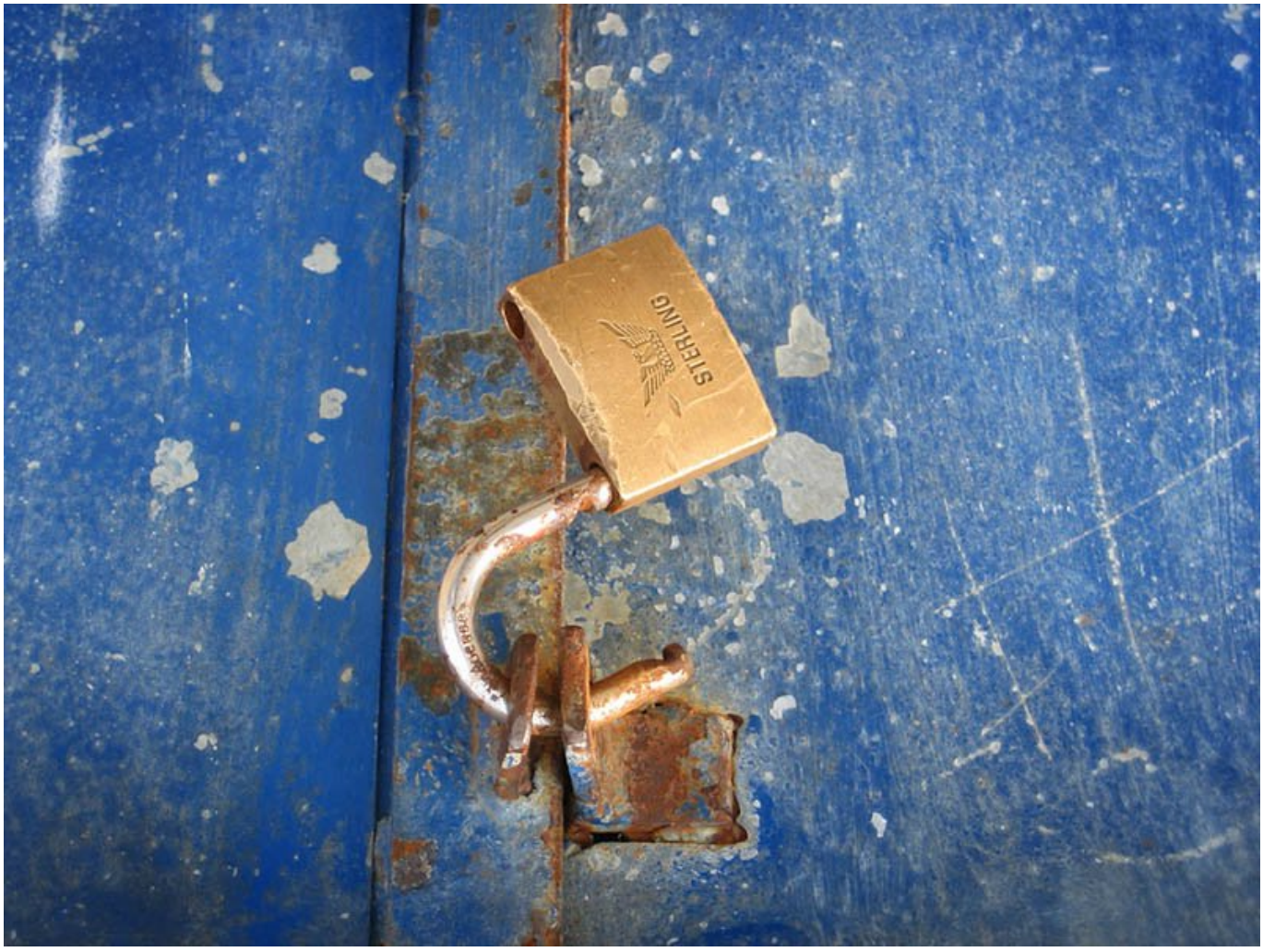


禪

مایکروسافت هشدار میدهد

همهچیز درباره حملات بدافزارهای مبتنی بر ماکروها

روند رو به رشد افزایش قدرت محاسباتی کامپیوترها و تجهیزات همراه باعث شده است تا زندگی برای حرفهایها سادهتر شود . اینترنت نه تنها کاربران را قدرتمند میسازد، بلکه انجام وظایف را هم سادهتر از گذشته میکند . همانگونه که قدرت و راحتی برای حرفهایها به همراه میآورد، برای هکرها نیز راحتی به همراه میآورد . پیادهسازی طیف گستردهای از حملات بدافزاری و دستکاری گسترده رباتهای تحت شبکه به جای آنکه برای هکرها به یک کابوس وحشتناک و یک واقعیت سخت تبدیل شود، به یک کار بسیار ساده تبدیل شده است. به طور مثال، در سالی که گذشت حملات بدافزاری مبتنی بر ماکروها به طور چشمگیر و فزایندهای قدرتمندتر از گذشته به وقوع پیوست .

ترفندهای مهندسی اجتماعی درها را به روی حملات بدافزاری ماکرو گشوده است . اما سؤال اینجاست چگونه میتوان این در را بست؟

اسناد مملو از بدافزارهای ماکرو، هدفشان ایمیلهای کاربران بوده و از طریق ایمیل اسپم عمدتا به تحریک حس کنجکاوی هر کاربری میپردازند . ایمیلهایی که با عنوان فاکتور فروش، رزومه، صورتحسابهای

120000
100000
80000
60000
40000
20000
0
2014-04
2014-05
2014-06
2014-07
2014-08
2014-09
2014-10
2014-11
2014-12
2015-01
2015-02
2015-03
Sum of UniqueSha1Count
Sum of UniqueMachineCount

125665
106387
28713
23718
21849
19544
19056
16087
13954
7596
United States
United Kingdom
Mexico
Poland
Italy
France
Germany
Canada
Australia

[illegible]

[illegible] Disable all macros with notification [illegible]

[illegible] macro downloader [illegible] CnC [illegible] Command [illegible] and Control [illegible]

:[illegible]

- Adnel

[illegible] Adnel [illegible].

- Bartallex

[illegible] Bartallex [illegible].

- Donoff

[illegible].

- Jeraps

[illegible].

- Ledod

.Jeraps

TrojanSpy:MSIL/Golroted

:

TrojanDownloader:Win32/Drixed

TrojanDownloader:Win32/Chanitor

Backdoor:Win32/Drixed

Backdoor:Win32/Vawtrak

"".

2007 doc .

اطمینان حاصل کنید تنظیمات Trust Center برای بارگذاری نکردن نسخههای قدیمیتر آفیس پیکربندی شده باشد .

1.به Word Options رفته روی گزینه Trust Center و سپس Trust Center Settings کلیک کنید .

Word Options
?
General
Display
Proofing
Save
Language
Advanced
Customize Ribbon
Quick Access Toolbar
Add-Ins
Trust Center
Show the Microsoft Word privacy statement
Microsoft Trustworthy Computing
Trust Center Settings...
OK
Cancel

Help keep your documents safe and your computer secure and healthy.

Protecting your privacy

Microsoft cares about your privacy. For more information about how Microsoft Word helps to protect your privacy, please see the privacy statements.

Security & more

Visit Office.com to learn more about protecting your privacy and security.

Microsoft Word Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

2. در پنجره Trust Center گزینه File Block Settings را انتخاب کنید . سپس نسخههای از ورد که میخواهید آنرا بلوکه کنید انتخاب کنید .

Trust Center
?
Trusted Publishers
Trusted Locations
Trusted Documents
Trusted App Catalogs
Add-ins
ActiveX Settings
Macro Settings
Protected View
Message Bar
File Block Settings
Privacy Options
File Block Settings
Restore Defaults
OK
Cancel

For each file type, you can select the Open and Save check boxes. By selecting Open, Word blocks this file type, or opens it in Protected View. By selecting Save, Word prevents saving in this file type.

File Type	Open	Save
Word 2007 and later Documents and Templates	☑	☑
OpenDocument Text Files	☐	☐
Word 2007 and later Binary Documents and Templates	☑	☑
Word 2003 Binary Documents and Templates	☑	
Word 2003 and Plain XML Documents	☑	☐
Word XP Binary Documents and Templates	☑	
Word 2000 Binary Documents and Templates	☑	
Word 97 Binary Documents and Templates	☑	
Word 95 Binary Documents and Templates	☑	
Word 6.0 Binary Documents and Templates	☑	
Word 2 and earlier Binary Documents and Templates	☑	
Web Pages	☐	☐
RTF Files	☑	☐
Plain Text Files	☐	☐
Legacy Converters for Word	☐	☐
Office Open XML Converters for Word	☐	☐
PDF Files	☑	

Open behavior for selected file types:

● Do not open selected file types

○ Open selected file types in Protected View

○ Open selected file types in Protected View and allow editing

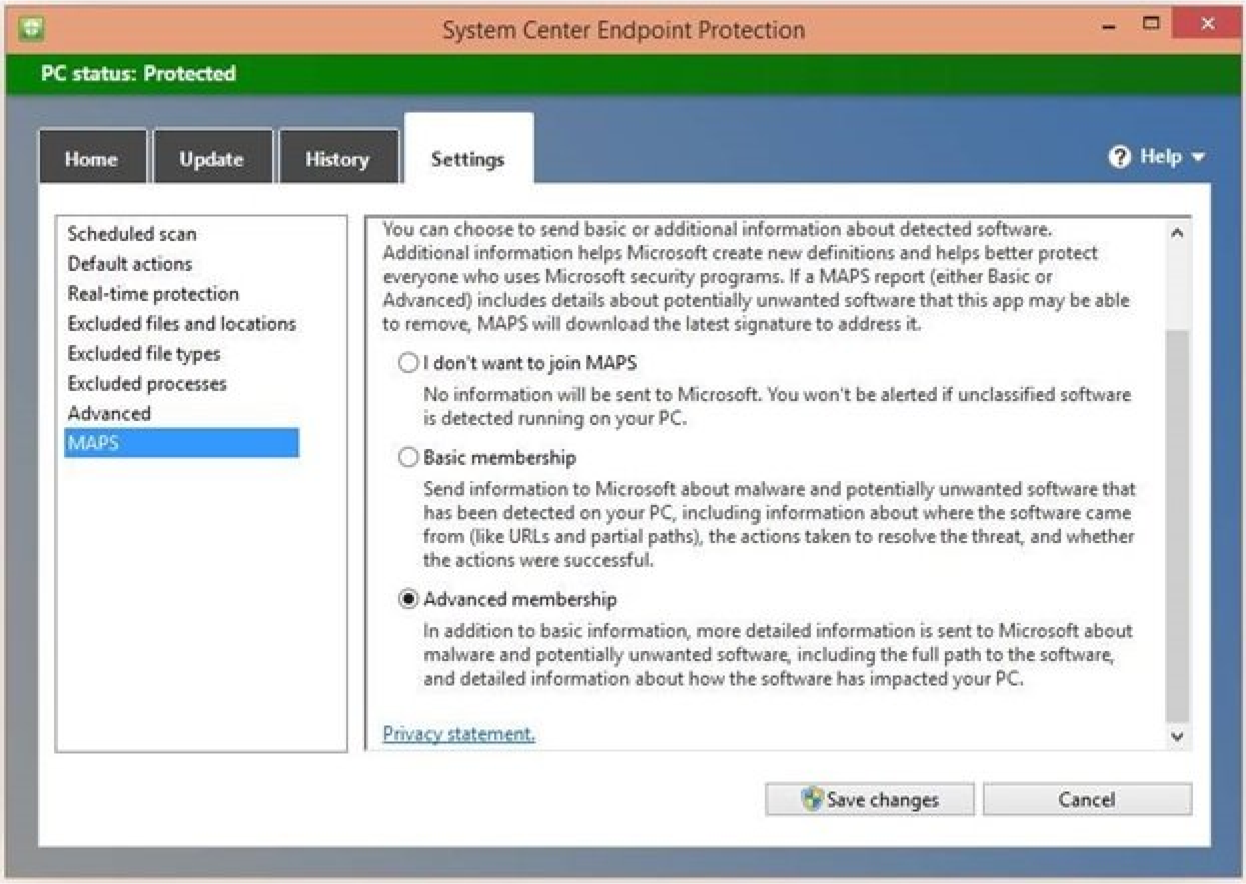
فرآیند باز کردن نسخههای قدیمی آفیس را بلوکه کنید .

از سرویس [Exchange Online Protection](#) متعلق به مایکروسافت که برای فیلتر کردن اسپمها و حذف ویروسهای کامپیوتری از پیامهای ایمیل مورد استفاده قرار گرفته و برای هر کسب و کاری ضروری است استفاده کنید . این سرویس نیازی به نصب برنامه کلاینتی ندارد .

آفیس 365 با بهرهمندی از تکنیک یادگیری ماشینی به شما در بلوکه کردن اسپمها کمک میکند .

پیامهای اسپم و پیامهای غیراسپم را برای تجزیه و تحلیل به این آدرس برای مایکروسافت ارسال کنید .

ویژگی MAPS (سرنام Microsoft Active Protection Service) را فعال کنید . کاربران با استفاده از MAPS از مزیتهای محافظت ابری مایکروسافت و محافظت در برابر جدیدترین بدافزارها ایمن خواهند شد . MAPS به طور پیشفرض روی Microsoft Security Essentials و ویندوز دیفندر (Windows Defender) در ویندوز 8.1 فعال است. برای اطمینان از اینکه آیا MAPS روی محصول امنیتی مایکروسافت فعال است یا خیر ، به زبانه Settings رفته و سپس MAPS را مشاهده کنید .



[illegible]

[illegible] 29 [illegible] scmagazine [illegible] BARTALEX [illegible] Dyre [illegible]

[illegible]

[illegible]:

[illegible]

[illegible]:

[illegible]

[illegible]:

17:11 - 19/02/1394

[illegible]:

macro malware - [illegible] - [illegible] - [illegible] - [illegible]

[illegible]:https://www.shabakeh-mag.com/security/608