بسمه تعالی

شکست روش کلیدی ضد بدافزار در ویندوز ۱۰

بیش از یک دهه قبل، مایکروسافت روشی به نام ASLR ارایه داد. در این روش نواحی کلیدی حافظه به‌صورت تصادفی تغییر داده و در هر بار اجرای برنامه، داده‌های آن در مکان‌های مختلفی ذخیره می‌شوند. به دلیل وجود این ویژگی، مهاجم نمی‌تواند آدرس‌های موردنیاز خود را برای سوءاستفاده پیش‌بینی نماید.

در ویندوز ۱۰، به نظر می‌رسد در رابطه با این روش مشکلی وجود دارد و داده‌ها در مکان یکسانی ذخیره می‌شوند. برای درک اهمیت این مشکل مثالی ذکر می‌شود. در این مثال تصور شده است که فردی صندوق پستی ناامنی دارد که دائماً از آن سرقت می‌شود. یکی از راه‌های مقابله با این مشکل این است که چندین صندوق پستی پراکنده برای این فرد درنظر گرفته شود و کارمند پست هر روز، نامه‌های فرد را در زیرمجموعه‌ای از صندوق‌های پستی موجود (به‌طور مثال ۳۰ صندوق پستی کل) قرار دهد. با این کار برای یافتن نامه باید تمامی صندوق‌ها جستجو شوند که این کار برای دزد نامه‌ها زمان‌بر خواهد بود.

درواقع، در ویندوز ۷ و ASLR موجود در ابزار EMET (Enhanced Mitigation Experience Toolkit)، آدرس بارگذاری شده برای eqnedt32.exe در هر راه‌اندازی مجدد، متفاوت است؛ اما در ویندوز ۱۰، چه با EMET یا با WDEG (Windows Defender Exploit Guard)، آدرس پایه‌ی eqnedt32.exe هر بار 0×10000 است. درنتیجه ویندوز ۱۰ نمی‌تواند ASLR را همچون ویندوز ۷ اجرا کند!

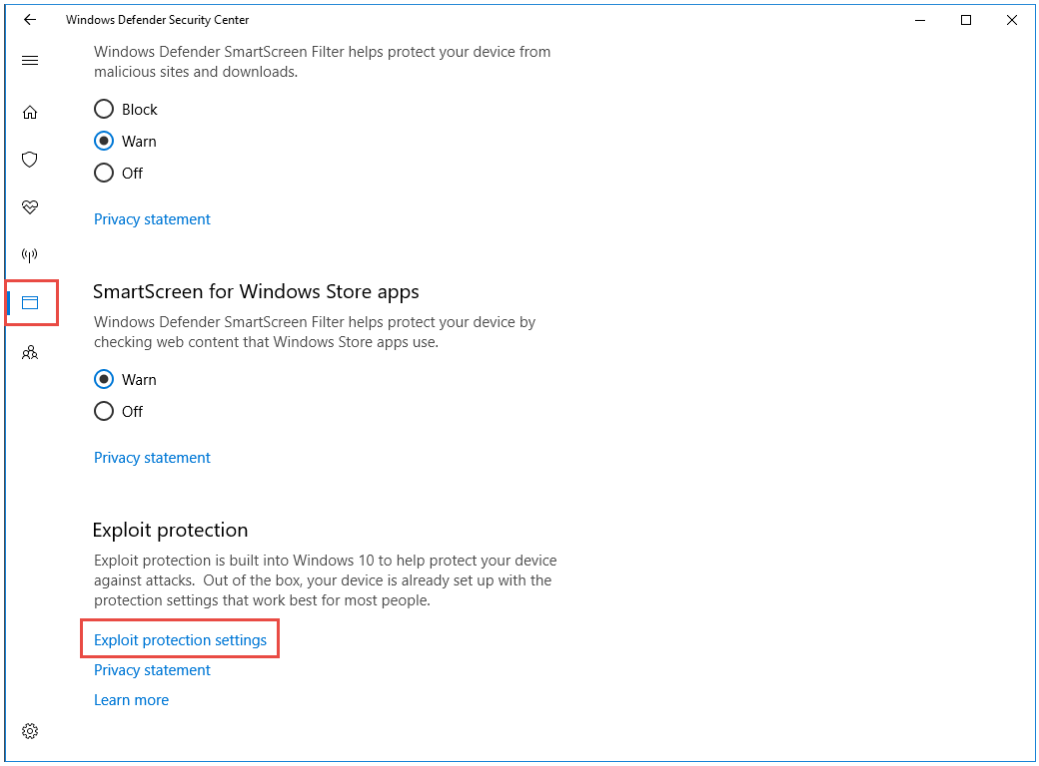
حال تصور می‌شود که به‌جای قرار دادن پنج نامه در پنج مکان مختلف، کارمند پستی آن‌ها را همیشه در مکان‌های یکسانی قرار دهد. درواقع این موضوع مشکل موجود در ویندوز ۸ و ویندوز ۱۰ است که بدون هیچ‌گونه تصادفی، حفاظتی نیز وجود نخواهد داشت.

دو راه برای فعال کردن ASLR وجود دارد:

۱- یک راه استفاده از پرچم /DYNAMICBASE است که توسط لینکر ویژوال C++ ارائه‌شده است. این روش به‌طور کامل و به‌خوبی کار می‌کند؛ اما باید توسط برنامه‌نویسان استفاده شود.

۲- به دلیل اینکه تکیه‌بر برنامه‌نویسان و یا تولیدکنندگان با فرض اینکه کدها را به‌صورت امن تولید و نگهداری کنند، فرض عاقلانه‌ای نیست؛ مایکروسافت ابزارهایی را نیز فراهم کرده است که به‌صورت خودکار استفاده از ASLR را برای برنامه‌ها فراهم می‌کند (چه آن‌ها برای انجام این کار طراحی‌شده باشند و چه نشده باشند). این قابلیت Fall Creators Update به‌عنوان WDEG شناخته می‌شود و قبلاً به‌عنوان EMET مایکروسافت (رابط گرافیکی کاربری برای فعال کردن اقدامات

امنیتی که قبلاً در سیستم‌عامل نصب شده بود) در دسترس بوده است. تصویر زیر WDEG جدید ویندوز ۱۰ را نشان می‌دهد:



مشکل این است که ظاهراً اجرای برنامه ASLR مایکروسافت قادر به فعال کردن روش اصلی مرتب‌سازی ASLR که به‌عنوان «ASLR پایین-بالا» شناخته می‌شود، نیست. فعال کردن ASLR بدون اینکه همزمان ASLR پایین به بالا فعال شود، به این معنی است که مقادیر حافظه در هر زمان و دقیقاً در یک مکان ذخیره می‌شوند.

این موضوع باعث می‌شود برنامه‌هایی که از پرچم DYNAMICBASE/ استفاده نمی‌کنند، بدون هیچ تصادفی جابه‌جا شوند. نتیجه این است که چنین برنامه‌هایی در هر بار راه‌اندازی مجدد سیستم و حتی در سیستم‌های مختلف در آدرسی یکسان قرار می‌گیرند. سیستم‌هایی با ویندوز ۸ و جدیدتر که ASLR سیستم را از طریق EMET یا WDEG فعال کرده‌اند، برنامه‌های غیر DYNAMICBASE/ را به مکان قابل پیش‌بینی منتقل می‌کنند؛ بنابراین در عمل از مزایای ASLR استفاده نکرده‌اند.

این مشکل امکان سوءاستفاده از برخی از کلاس‌های آسیب‌پذیری را راحت‌تر کرده است. در حال حاضر هیچ راه‌حلی برای رفع مشکل موجود وجود ندارد، اما افراد می‌توانند با واردکردن کلید رجیستری زیر ASLR امن را دوباره فعال کنند:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel]
“MitigationOptions”=hex:00,01,01,00,00,00,00,00,00,00,00,00,00,00,00,00
```

توصیه می‌شود تغییر رجیستری توسط کاربر مورداستفاده قرار نگیرد، مگر اینکه کاربر نحوه‌ی کار کردن با آن را بداند. لازم به ذکر است که این مشکل بر سیستم‌عامل ویندوز ۷ تاثیر نمی‌گذارد.