انتشار استاکس‌نت قبل از آسیب‌پذیری فایل lnk.

محمد مهدی واعظی نژاد
Mahdivaezi61@yahoo.com

کرم اینترنتی استاکس‌نت برای انتشار خود توسط درایوهای قابل جابه‌جایی، از ترفند و اتورانی که ایجاد یک فایل autorun.inf در ریشه درایوهای قابل جابه‌جایی است، بهره می‌برد.

برای اجرای فایل‌های دستکاری‌شده و مخرب در سیستم هدف می‌توان آنها را به‌صورت فایل اجرایی یا یک فایل autorun.inf در رایانه قرار داد.

هنگامی‌که ویندوز، فایل autorun.inf را تجزیه می‌کند، هر کاراکتری را که نتواند درک نماید، به‌عنوان بخشی از دستورات اتوران محسوب نمی‌کند و مانند کدهای زاید در نظر می‌گیرد و با توقف عملیات روی آنها، همچنان به تجزیه فایل ادامه می‌دهد.

استاکس‌نت با قراردادن فایل MZ در فایل autorun.inf از این واقعیت به نفع خود سوءاستفاده می‌کند.

هنگامی‌که ویندوز، فایل autorun.inf را تجزیه می‌کند، همه مقادیر MZ را به‌عنوان کدهای زاید نادیده می‌گیرد و تنها دستورات اتوران را که در انتهای فایل است، اجرا می‌نماید.

سرصفحه و پاورقی فایل autorun.inf را می‌توان در شکل‌های زیر مشاهده کرد.

سرصفحه فایل autorun.inf:

```
00000000: 4D5A9000 03000000 04000000 FFFF0000  MZ▌.........ÿÿ..
00000010: B8000000 00000000 40000000 00000000  ¸.......@.......
00000020: 00000000 00000000 00000000 00000000  ................
00000030: 00000000 00000000 00000000 E0000000  ............à...
00000040: 0E1FBA0E 00B409CD 21B8014C CD215468  ..º..´.Í!¸.LÍ!Th
00000050: 69732070 726F6772 616D2063 616E6E6F  is program canno
00000060: 74206265 2072756E 20696E20 444F5320  t be run in DOS
00000070: 6D6F6465 2E0D0D0A 24000000 00000000  mode....$.......
00000080: CF7A777C 8B1B192F 8B1B192F 8B1B192F  Ïzw|▌../▌../▌../
00000090: ACDD642F 9D1B192F ACDD622F 9C1B192F  ¬Ýd/▌../¬Ýb/▌../
000000A0: 8B1B182F 6D1B192F ACDD6B2F DA1B192F  ▌../m../¬Ýk/Ú../
```

پاورقی فایل autorun.inf:

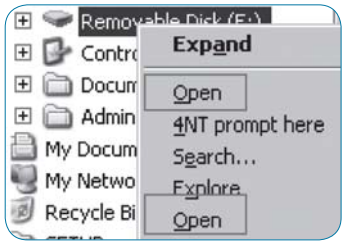
```
00041000: 0D0A5B61 75746F72 756E5D0D 0A6F626A  ..[autorun]..obj
00041010: 65637444 65736372 6970746F 723D7B42  ectDescriptor={B
00041020: 33313535 33372D36 3341422D 39353132  315537-63AB-9512
00041030: 2D393941 392D3246 34363737 32333541  -99A9-2F4677235A
00041040: 34347D0D 0A                          44}..
00041050: 636F6D6D 616E643D 2E5C4155 544F5255  command=.\AUTORU
00041060: 4E2E494E 460D0A                      N.INF..
00041070: 753D4025 77696E64 6972255C 73797374  u=@%windir%\syst
00041080: 656D3332 5C736865 6C6C3332 2E646C6C  em32\shell32.dll
00041090: 2C2D3834 39360D0A                    ,-8496..
000410A0: 0D0A 55736541 75746F50 4C41593D      ..UseAutoPLAY=
000410B0: 300D0A                               0..
```

با استخراج کدهای پاورقی مشاهده می‌شود که این فایل از دستورات عادی اتوران تشکیل شده است.

```
.?AVZdhrnpldcahnGvqzdhRnpldcahn@gfjjefwq@sr@@
[autorun]
objectDescriptor={B315537-63AB-9512-99A9-2F4677235A44}
Menu\command=.\AUTORUN.INF
Menu=@%windir%\system32\shell32.dll,-8496

UseAutoPLAY=0
```

توجه کنید که دستورات (درون کادر رنگی در تصویر) مشخص کرده است که autorun.inf به عنوان فایل اتوران اجرا شود. با استفاده از این ترفند، autorun.inf ابتدا مانند یک فایل اتوران معمولی و سپس همچون فایل اجرایی، کد کرم را اجرا خواهد کرد. علاوه بر این شگرد فریبنده، استاکس‌نت از ترفند دیگری نیز برای افزایش احتمال اجراشدن خود استفاده می‌کند. در دستورات اتوران نشان داده شده در شکل بالا، ویژگی AutoPlay نخستین بار خاموش است و یک دستور جدید نیز به منوی کلیک‌راست اضافه می‌شود. این دستور در مسیر %Windir%\system32\shell32.dll,-8496 ایجاد شده و همان‌طورکه در تصویر زیر دیده می شود، کاربر در هنگام مشاهده منوی زمینه برای درایو قابل جابه‌جایی، در واقع دو دستور «بازکردن» را مشاهده خواهد کرد.



یکی از این دستورات بازکردن، توسط استاکس‌نت به این منو اضافه شده است. اگر کاربر با استفاده از گزینه اضافه‌شده به وسیله کرم اقدام به بازکردن درایو کند، کد کرم طبق دستور فایل autorun.inf اجرا می‌شود و سپس یک پنجره اکسپلورر را باز می‌کند و محتویات درایو را نمایش می‌دهد.

موفقیت این ترفند، به تنظیمات AutoPlay و AutoRun در رایانه هدف بستگی دارد که در صورت غیرفعال‌کردن این گزینه‌ها، گسترش کرم نیز توسط درایوهای قابل جابه‌جایی متوقف خواهد شد.

لازم به ذکر است که در اواخر فروردین ماه ۱۳۸۹ نسخه جدیدی از کرم استاکس‌نت منتشر شده است که برای انتشار خود از یک کد مخرب یعنی آسیب‌پذیری فایل lnk.(BID43073) به جای ترفندهای فوق استفاده می‌کند.