بسمه‌تعالی

گزارش فنی بدافزار Bedep

معرفی بدافزار

از اواخر ماه ژانویه تا اوایل ماه فوریه سال ۲۰۱۵، رویدادهای مربوط به سوء استفاده از آسیب‌پذیری‌های روز صفر در صدر اخبار امنیتی دنیا قرار گرفتند. این آسیب‌پذیری‌ها نسخه‌های خاصی از Adobe Flash Player را هدف قرار داده بودند که شامل دو آسیب‌پذیری CVE-2015-0311 و CVE-2015-0313 شامل می‌شدند.

در هر دوی این حملات، قربانیان با بازدید از وب‌سایت‌های به ظاهر بی‌خطر به واسطه تبلیغاتی که در این وب‌سایت‌ها قرار داده شده بود به سمت وب‌سایت‌هایی هدایت می‌شدند که بسته‌ی اکسپلویت Angler را میزبانی می‌کردند. این بسته‌ی اکسپلویت با سوء استفاده از آسیب‌پذیری‌های یاد شده بدافزاری را بر روی سیستم قربانی نصب می‌کرد که Bedep نامیده شده است.

بدافزار Bedep عمدتاً برای تقلب در تبلیغات اینترنتی مورد استفاده قرار می‌گیرد. به علاوه این بدافزار سیستم قربانی را به شبکه‌ی بات خود اضافه می‌کند. این کار به این بدافزار اجازه می‌دهد بدافزارهای دیگری را بارگذاری و نصب نماید، خود را به روز رسانی کند و یا هر کد دلخواه دیگری را از کارگزار کنترل و فرمان دریافت کرده و اجرا نماید.

شناسایی سیستم آلوده از طریق لاگ‌های شبکه

به دلیل استفاده بدافزار Bedep از یک الگوریتم تولید دامنه (DGA)، شناسایی سیستم‌های آلوده از طریق لاگ شبکه به سادگی امکان‌پذیر نیست. با این حال برخی از نام‌های دامنه‌ای که Resolve آن‌ها توسط یک سیستم می‌تواند نشانی از آلودگی باشد عبارتند از:

aohevoloaozrkak10.com
avuoujqzkfqimp.com
blrndbpidwnxbgj.com
dkatcqflcaqlumcxhd.com
dsricnohtnwbium.com
dsricnohtnwbium.com
emxgyboesbodszr6t.com
emxgyboesbodszr6t.com
ewhvktipgdwdhcxfv.com
ewhvktipgdwdhcxfv.com
exrhmkumgbuhq2g.com
favtcihswsqly.com
ggtjcszgresakw.com
hgfmdwdqutcwqlc.com
hnrmdcvwza0m.com

hppzynkovgjpth.com
hppzynkovgjpth.com
iqeuldlijtnnff.com
iwgqqmayowal.com
iwgqqmayowal.com
iyoxkwiwdvt6a.com
ndkcrwdfocxogjfxod.com
npbwstpnlqnrejm.com
npbwstpnlqnrejm.com
oyrqilsgusdcdvc4.com
oyrqilsgusdcdvc4.com
plwqwnzyigp7h.com
plwqwnzyigp7h.com
qibbfusbruoixkk.com
qysbxunmocpablwqmc.com
ynecbggcxu4x.com
ynecbggcxu4x.com
yrmbqqncmsevoxnoh.com

همچنین ارتباط با آدرس‌های زیر می‌تواند نه به صورت قطعی بلکه به صورت تقریبی نشانگر آلودگی سیستم‌ها باشد:

http://www.earthtools.org/timezone/0/0
http://www.ecb.europa.eu/stats/eurofxref/eurofxref-hist-90d.xml

بررسی وجود آلودگی

- وجود یک فایل DLL در مسیر زیر:

ProgramData\<UserID>\

- وجود کلید زیر در رجیستری ویندوز:

HKU\<User SID>\Software\Classes\CLSID\{F6BF8414-962C-40FE-90F1-B80A7E72DB9A}\InprocServer32

- وجود کلید زیر در رجیستری ویندوز:

HKU\<User SID>\Software\Classes\Drive\ShellEx\FolderExtensions\{F6BF8414-962C-40FE-90F1-B80A7E72DB9A}

نحوه پاک‌سازی سیستم

- حذف فایل‌های DLL مشکوک از مسیر:

ProgramData\<UserID>\

- حذف کلیدهای زیر از رجیستری ویندوز:

HKU\<User SID>\Software\Classes\CLSID\{F6BF8414-962C-40FE-90F1-B80A7E72DB9A}\InprocServer32
HKU\<User SID>\Software\Classes\Drive\ShellEx\FolderExtensions\{F6BF8414-962C-40FE-90F1-B80A7E72DB9A}

- راه‌اندازی مجدد سیستم

بررسی پاک بودن سیستم

- نبود فایل‌های DLL مشکوک از مسیر:

ProgramData\<UserID>\

- نبود کلیدهای زیر از رجیستری ویندوز:

HKU\<User SID>\Software\Classes\CLSID\{F6BF8414-962C-40FE-90F1-B80A7E72DB9A}\InprocServer32
HKU\<User SID>\Software\Classes\Drive\ShellEx\FolderExtensions\{F6BF8414-962C-40FE-90F1-B80A7E72DB9A}

توصیه‌های امنیتی برای پیشگیری

- خودداری از بازدید از وب‌سایت‌های ناشناس
- استفاده از افزونه‌های بلاک کردن تبلیغات بر روی مرورگر مانند افزونه AdBlock
- خودداری از کلیک بر روی لینک‌های ناشناس
- به روز رسانی Adobe Flash، مرورگر، افزونه‌های مرورگر، سیستم عامل و ...