بسمه‌تعالی

گزارش تحلیل بدافزار ZeroAccess

مقدمه

ZeroAccess یک بدافزار سطح-هسته‌ی پیشرفته است که به سرعت در حال تبدیل شدن به یکی از شایع‌ترین تهدیدات اینترنتی می‌باشد. قابلیت اجرا بر روی هر دو نسخه‌ی ۳۲ بیتی و ۶۴ بیتی ویندوز، استفاده از یک ساختار کنترل و فرمان نقطه-به-نقطه‌ی مقاوم و نیز به‌روزرسانی‌های مداوم برای بهبود عملکرد، نشان می‌دهد که ZeroAccess یک تهدید جدی جدید است که قابلیت حمله به شبکه‌های و سیستم‌عامل‌های جدید را دارد.

از انتشار ZeroAccess چندین سال می‌گذرد و تعداد ماشین‌های آلوده به این بدافزار در طول این چندسال همواره در حال افزایش بوده است. در طول این دوره، چندین بازبینی و تغییرات در کارایی این بدافزار، تغییر استراتژی آلوده‌کردن و نیز تغییر در نحوه‌ی پایداری بر روی سیستم قربانی، توسط توسعه‌دهنده‌گان این بدافزار صورت گرفته است. با این حال در طول این چندسال،هدف اصلی این بدافزار همواره ثابت مانده است که عبارت است از: در دست گرفتن کنترل کامل سیستم قربانی و افزودن آن به شبکه‌ی بات ZeroAccess و سپس بهره‌برداری از آن از طریق دانلود بدافزارهای دیگر.

در اصل ZeroAccess یک روتکیت سطح کرنل است که شباهت‌هایی با خانواده‌ی بدافزارهای TDL دارد. این بدافزار از تکنیک‌های پیشرفته برای مخفی ساختن حضور خود در سیستم استفاده می‌کند، قابلیت کار بر روی هر دو نسخه‌ی ۳۲ بیتی و ۶۴ بیتی ویندوز را داراست، مکانیزم‌هایی تهاجمی برای دفاع از خود دارد و به عنوان یک پلتفرم پیچیده برای تحویل سایر بدافزارها عمل می‌کند.

نحوه‌ی انتشار

نحوه‌ی انتشار ZeroAccess با نحوه‌ی انتشار سایر بدافزارهای سطح‌بالای کنونی شباهت بسیار زیادی دارد. به صورت کلی می‌توان روش‌های انتشار این بدافزار را به دو دسته‌ی کلی طبقه بندی کرد:

- بسته‌های اکسپلویت (Exploit Packs)
- مهندسی اجتماعی (Social Engineering)

بسته‌های اکسپلویت

بدافزار ZeroAccess رفته رفته به یکی از محبوب‌ترین Payloadها برای بسته‌های اکسپلویت موجود در بازار (به ویژه بسته اکسپلویت BlackHole) تبدیل می‌شوند. یک بسته‌ی اکسپلویت عموما در قالب یک سری اسکریپ‌های PHP که بر روی یک کارگزار وب تحت کنترل حمله کننده ذخیره می‌شوند، ارایه می‌شود. هنگامی که مرورگر کاربر از یک صفحه‌ی وب آلوده بازدید می‌کند، وب‌سایت سعی می‌کند با سوء استفاده از یکی از نقاط آسیب‌پذیری موجود بر روی سیستم‌کاربر، Payload خود را بر روی سیستم هدف اجرا کند. بسته‌های اکسپلویت معمولا حاوی تعداد بسیار زیادی از انواع مختلف اکسپلویت‌ها هستند که نرم‌افزارهای شایع مورد استفاده توسط کاربران سیستم عامل ویندوز (مانند Internet Explorer، Flash و Java) را هدف قرار می‌دهند.

کاربران به طرق مختلفی به سمت وب‌سایت‌های میزبان بسته‌های اکسپلویت هدایت می‌شوند. یکی از روش‌های شایع، استفاده از سایت‌های مورد تجاوز قرار گرفته است. سایت‌های مشروعی که توسط حمله‌کنندگان مورد تجاوز قرار گرفته‌اند (معمولا از طریق اطلاعات ورود FTP که به سرقت رفته است یا از طریق SQL Injection) برای میزبانی بسته‌های اکسپلویت و یا هدایت کاربران به سمت سایت‌های حمله‌ی اصلی، مورد استفاده قرار می‌گیرند. معمولا مقدار کمی کد Javascrpit در صفحه‌ی سایت مورد تعرض قرار گرفته، قرار داده می‌شود که کاربر را به سمت سایت حمله هدایت می‌کند.

سایت‌های تبلیغاتی نیز تا کنون اینگونه مورد حمله قرار گرفته‌اند که در صورتی که تبلیغات این سایت‌ها در سایت‌های بسیار بزرگ اینترنتی نمایش داده شود، سبب شیوع بسیار سریع بدافزار می‌گردد. همچنین از تکنیک‌های SEO برای بالا آوردن رتبه‌ی وب‌سایت‌های مورد تعرض قرار گرفته در لیست موتورهای جستجو استفاده می‌شود تا میزان بازدید کننده‌های سایت افزایش یابد.

استفاده از این شیوه‌ی انتشار با استفاده از هرزنامه نیز مشاهده شده است. یک هرزنامه که شامل یک لینک است به صورت گسترده توزیع می‌شود که زمانی که کاربر بر روی لینک موجود در این هرزنامه کلیک می‌کند به سمت وب‌سایتی هدایت می‌شود که میزبان یک بسته‌ی اکسپلویت است.

مهندسی اجتماعی

راهکار اصلی دیگر برای انتشار بدافزار ZeroAccess، استفاده از روش‌های گوناگون مهندسی اجتماعی است. هدف اصلی تمامی این روش‌ها، مجاب کردن کاربر به اجرای یک فایل اجرایی است که نبایستی اجرا کند. راهکاری که معمولا توسط حمله کنندگان استفاده می‌شود، آن است که فایل بدافزار را در داخل یک فایل دیگر که قالبا تحت عنوان یک بازی کامپیوتری یا یک فایل کرک یا کیجن ارایه می‌شود، مخفی‌سازی می‌کنند. این فایل تروجان سپس بر روی سایت‌های دانلود و تورنت‌ها قرار می‌گیرد.

به عنوان نمونه، شکل زیر فایلی را نشان می‌دهد که خود را به عنوان کیجن نرم‌افزار DivX Plus 8 برای ویندوز جا می‌زند. این فایل در واقع یک برنامه‌ی خود بازکننده‌ی NSIS است که شامل کیجن معرفی شده است. اما همراه با آن، یک فایل رمزنگاری شده‌ی zip7 نیز وجود دارد. وقتی برنامه اجرا می‌شود، کیجن را اکسترکت کرده و اجرا می‌کند.

اما در پس‌زمینه، فایل zip7 ذکر شده نیز بازگشایی و اجرا می‌شود که حاوی بدافزار ZeroAccess است.

نصب‌کننده (Dropper)

نصب‌کننده‌های ZeroAccess نیز همزمان با تغییرات خود بدافزار، به مرور زمان تغییر یافته‌اند. در حال حاضر، نصب‌کننده‌ها معمولا با یکی از پکرهای (Packer) چندریختی، پک شده‌اند. این پکرها یکی از نمونه‌های معمول از راهکارهایی است که بدافزارهای نوین برای دشوارسازی فرآیند تحلیل و نیز مخفی‌کردن خود از دید ابزارهای امنیتی، مورد استفاده قرار می‌دهند. فرآیند پک کردن بدافزار در طول روز چندین بار انجام

می‌شود و هر بار نیز فایل پک شده پیش از انتشار بر روی چندین نرم‌افزار ضد بدافزار بررسی می‌شود تا از عدم شناسایی آن توسط این نرم‌افزارها اطمینان حاصل شود.

این پکرها، حاوی تعداد بسیار زیادی تکنیک ضد-شبیه‌سازی و ضد-دیباگ هستند تا از این راه، از تحلیل بدافزار در یک محیط کنترل شده و اجرای بدافزار در محیط شبیه‌سازی شده‌ی ابزارهای ضدبدافزار جلوگیری کنند. یکی از نکات جالب در رابطه با نصب‌کننده‌های ZeroAccess آن است که یک نصب‌کننده قادر است بر حسب سیستمی که بر روی آن در حال اجراست، نسخه‌ی ۳۲ بیتی و یا ۶۴ بیتی از بدافزار را بر روی آن سیستم نصب کند.

فرآیند نصب

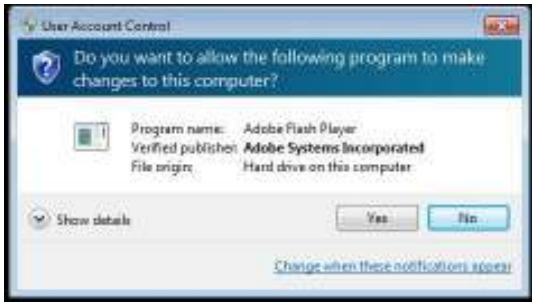
در ابتدا ZeroAccess بررسی می‌کند که آیا بر روی یک نسخه‌ی ۳۲ بیتی از ویندوز در حال اجراست یا بر روی یک نسخه‌ی ۶۴ بیتی. این کار با استفاده از APIی ZwQueryInformationProcess انجام می‌گیرد.

```
push    eax
push    4
lea     eax, [esp+1D8h+IsX64]
push    eax
push    1Ah                             ; ProcessWow64Informatio
push    0FFFFFFFFh
call    ds:ZwQueryInformationProcess ; check if 64 bit
cmp     [esp+1D0h+IsX64], edi
jz      short x32
```

این بخش، همان بخشی است که تصمیم‌گیری در رابطه با نصب نسخه‌ی ۳۲ بیتی و یا ۶۴ بیتی از بدافزار، صورت می‌پذیرد. پس از آن، نصب‌کننده تلاش می‌کند تا دسترسی SE_DEBUG_PRIVILEGE را برای خود احراز کند.

```
mov     ebp, esp
sub     esp, 14h
push    ebx
push    esi
push    edi
lea     eax, [ebp+var_1]
push    eax                             ; enabled
xor     edi, edi
push    edi                             ; CurrentThread
push    1                               ; enable
push    14h                             ; SE_DEBUG_PRIVILEGE
call    ds:RtlAdjustPrivilege
test    eax, eax
jl      short priv_adjust_failed
xor     eax, eax
jmp     done
```

اگر این عمل موفقیت آمیز بود، مسیر نصب به صورت عادی ادامه می‌یابد در غیر این صورت بدافزار از راه دیگری مجددا برای به دست آوردن این سطح دسترسی، تلاش می‌کند. ZeroAccess برای نصب موفق، به دسترسی سطح بالا نیاز دارد. برای رسیدن به این سطح دسترسی بر روی سیستم‌هایی که سامانه‌ی UAC ویندوز بر روی آن‌ها فعال است و یا کاربر جاری سیستم سطح دسترسی مدیریت ندارد، یک پیام UAC نمایش داده خواهد شد. اما کاربران معمولا به نمایش چنین پیغامی توسط فایلی که تازه از اینترنت دانلود کرده‌اند و یا فایلی که نمی‌شناسند، مشکوک می‌شوند. بنابراین کاربر ممکن است با رد این درخواست، مانع از ادامه‌ی فرآیند نصب بدافزار گردد. برای دور زدن این مانع، ZeroAccess به‌گونه‌ای عمل می‌کند که پیام UAC از سوی برنامه‌ی دیگری که کاربر به آن اعتماد دارد (مانند InstallFlashPlayer.exe) نمایش داده شود.



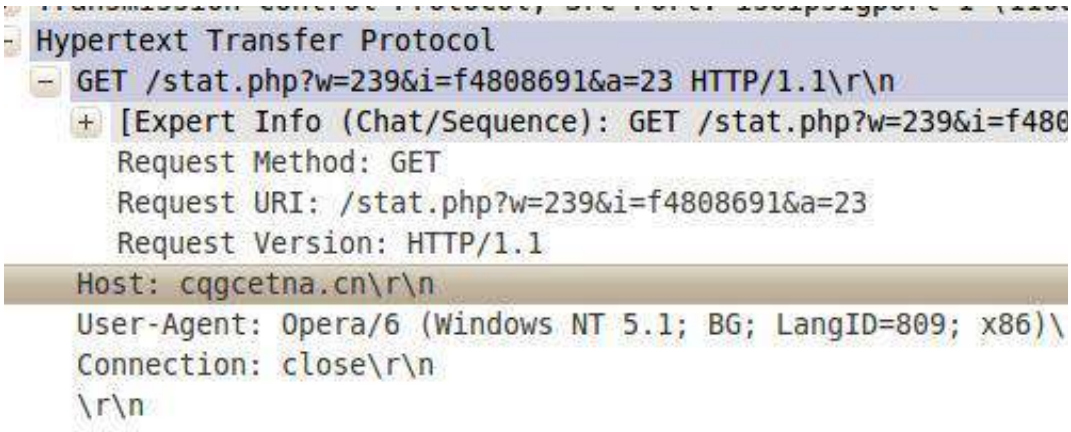
پس از این، بدافزار با غیرفعال کردن برخی از سرویس‌های امنیتی ویندوز، اقدام به پایین آوردن سطح ایمنی سیستم آلوده می‌نماید. فایروال ویندوز خاموش می‌شود و به‌روزرسانی‌ها دیگر به صورت خودکار از مایکروسافت دانلود و نصب نمی‌شوند. لیست کامل سرویس‌هایی که این بدافزار سعی در غیرفعال کردن آن‌ها دارد عبارتند از:

- BFE (Base FilteringEngine Service)
- iphlpsvc (IP Helper service)
- mpssvc (Windows firewall service)
- WinDefend (Windows Defender service)
- wscsvc (Windows Security Center Service)
- WinHttpAutoProxySvc (Proxy Auto Discovery Service)

تولید دامنه‌های شبه‌تصادفی

در حین نصب، بسیاری از نمونه‌های ZeroAccess اطلاعاتی از ماشین آلوده‌شده را به یک آدرس IP قرار داده شده در کد برنامه، گزارش می‌دهند. این عمل با ارسال یک درخواست HTTP Get که فیلد Host آن با یک نام دامنه‌ی شبه‌تصادفی تولید شده با پسوند .cn پر شده است، صورت می‌پذیرد. نام دامنه‌ی تولید شده وجود خارجی ندارد و نیازی هم به وجود آن نیست چرا که هیچگونه درخواستی برای تماس با این نام دامنه ارسال نمی‌شود. برای تولید نام دامنه از تاریخ روز و یک Seed استفاده می‌شود بنابراین برای هر روز یک نام دامنه‌ی جدید تولید می‌شود.

این الگوریتم تولید نام دامنه (DGA) در جاهای مختلفی از بدازار ZeroAccess که نیاز به ارتباط Http هست مورد استفاده قرار می‌گیرد. این نام دامنه‌ی تصادفی، به عنوان یک مکانیزم شبه احراز اصالت میان کارگزار و بدافزار ZeroAccess استفاده می‌شود تا کارگزار مطمئن شود که با یک نمونه‌ی واقعی بدافزار در ارتباط است نه یک تحلیل‌گر و یا روبات. موقعیت و معماری سیستم آلوده نیز در قسمت User-Agent درخواست برای کارگزار ارسال می‌گردد.



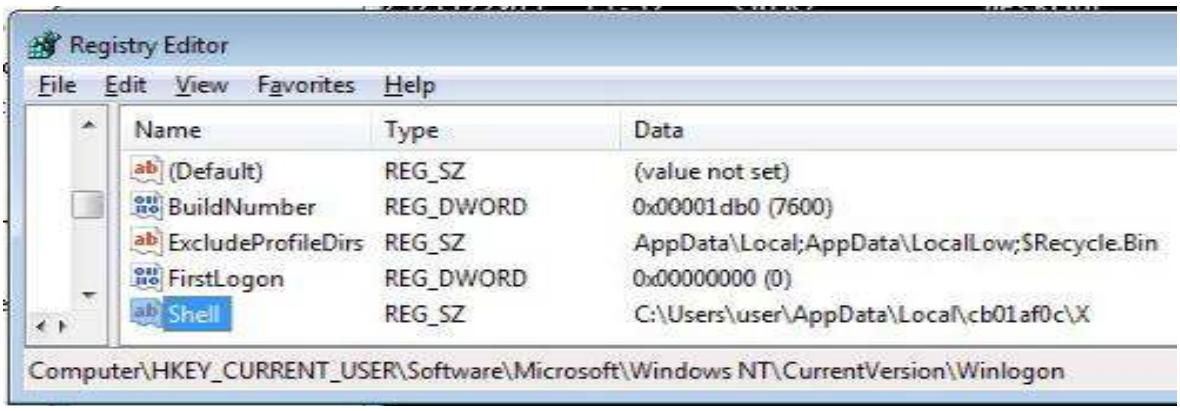
نصب نسخه‌ی ۳۲ بیتی

در صورت نصب در یک محیط ۳۲ بیتی، بدافزار ZeroAccess یک روتکیت سطح هسته نصب خواهد کرد (البته در نسخ جدیدتر این قابلیت حذف شده و مانند نسخه‌ی ۶۴ بیتی که در ادامه توضیح داده خواهد شد، از مولفه‌های سطح کاربر استفاده می‌شود). برای بارگذاری کد بدافزار در هسته‌ی سیستم عامل، یکی از درایورهای موجود بر روی دیسک، بازنویسی خواهد شد. فایل درایور و سایر فایل‌های دانلود شده توسط بدافزار بر روی بخش رمزنگاری شده‌ای از دیسک که توسط سایر برنامه‌ها قابل دسترس نیست، ذخیره‌سازی می‌شود.

نصب نسخه‌ی ۶۴ بیتی

نسخه‌ی ۶۴ بیتی از هیچ کد سطح هسته‌ای استفاده نمی‌کند و تمامی فرآیند اجرای آن در فضای کاربر صورت می‌پذیرد. از همان تکنیک Flash Player برای به دست آوردن سطح دسترسی بالا به سیستم استفاده می‌شود. پایداری بر روی سیستم از طریق ایجاد یک فایل در فولدر AppData کاربر و ایجاد کلید زیر در رجیستری ویندوز، حاصل می‌شود:

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon



همچنین، بدافزار سعی می‌کند با قرار دادن فایل‌های خود در Global Assembly Cache (GAC) آن‌ها را از دید کاربر مخفی کند. GAC مکانی برای ذخیره‌سازی فایل‌های .NET بر روی سیستم عامل ویندوز است که در مسیر %windir%\assembly قرار دارد. برای نمایش محتویات این فولدر، ویندوز از ابزار Assembly Cache Viewer استفاده می‌کند و در نتیجه فایل‌های غیر از .NET که در این فولدر قرار بگیرند در Windows Explorer نمایش داده نمی‌شوند.

استقرار در حافظه

هنگامی که ZeroAccess در حافظه قرار گرفت، دو حوزه‌ی عمده‌ی فعالیت دارد: Rootkit و Payload

Rootkit

در صورت اجرا بر روی ویندوز ۳۲ بیتی، بدافزار روتکیت سطح هسته‌ی خود را نصب می‌کند که اهداف زیر را دارد:

- پنهان‌سازی درایور آلوده بر روی دیسک
- فراهم آوردن امکان خواندن و نوشتن در فایل‌های رمزشده
- دفاع از خود

Payload

کارکرد اصلی Payload ارتباط با شبکه‌ی بات نقطه-به-نقطه‌ی ZeroAccess و دانلود فایل‌های اضافی است. ارتباط با این شبکه معمولا از طریق درایور بدافزار و یا از طریق مولفه‌ی سطح کاربری که در یکی از پروسه‌های Explorer.exe، Svchost.exe تزریق شده است، انجام می‌گیرد.

هنگام آغاز به کار، ZeroAccess همراه خود فایلی دارد که شامل یک لیست ۲۵۶تایی از آدرس‌های IP است. هر آدرس IP همراه خود یک عدد نیز دارد که زمان آخرین دسترسی به آن آدرس را نشان می‌دهد. این لیست لیست اولیه‌ای از ماشین‌های شبکه‌ی بات است که بدافزار به آن‌ها متصل می‌شود. بدافزار تلاش می‌کند بر روی یک پورت ثابت که در کد برنامه ذخیره‌سازی شده است به این آدرس‌ها متصل شود. پس از

موفقیت در برقراری ارتباط با هریک از این آدرس‌ها، دستورات موردنظر به سمت آن‌ها ارسال می‌شود. بات همچنین بر روی همان پورت شروع به گوش کردن می‌کند تا سایر بات‌ها بتوانند به آن متصل شوند.

تمامی ارتباطات در این شبکه‌ی نقطه-به-نقطه با استفاده از الگوریتم RC4 و با یک کلید ثابت رمزنگاری می‌شوند. این کلید رمزنگاری برای تمامی نسخ مختلف بدافزار ثابت است. پس از برقراری ارتباط، هر بات از بات‌های دیگر لیست آدرس‌های آی‌پی و تمامی فایل‌هایی که در اختیار دارند را می‌گیرد و بدین ترتیب همواره بات‌ها آخرین نسخه از فایل بدافزار را در اختیار خواهند داشت.

عملکرد اصلی این بدافزار، دانلود بدافزارهای دیگر که در واقع افزونه‌های این بدافزار هستند، می‌باشد. این بدافزار ۳ افزونه اصلی دارد که هر کدام کاربرد متفاوتی دارند. این افزونه‌ها عبارتند از:

- **Click Fraud**: وظیفه‌ی این مولفه، هدایت کردن کاربر به آدرس‌های URL خاص و نیز ارسال درخواست به آدرس‌های مشخصی می‌باشد. هدف اصلی، کسب درآمد برای توسعه‌دهندگان بدافزار از طریق کلیک بر روی لینک‌های تبلیغاتی است. به ازای هر کلیک مبلغ مشخصی توسط آژانس‌های تبلیغاتی به حساب مجرمین واریز می‌شود.
- **Spam Bot**: وظیفه‌ی این مولفه، دریافت لیستی از آدرس‌های ایمیل و ارسال هرزنامه به این آدرس‌هاست.
- **Bitcoin Mining**: این مولفه، از قدرت پردازنده‌ی سیستم‌های قربانی برای تولید Bitcoinهای جدید و در نتیجه کسب درآمد برای مجرمین، استفاده می‌کند.
- **سایر مولفه‌ها**: از قبیل مانیتورینگ سیستم، به‌روز رسانی بدافزار، دانلود و اجرای فایل دلخواه و ...

شیوه‌ی مقابله در سطح شبکه

از آن‌جایی که این بات از یک شبکه‌ی کنترل و فرمان نقطه به نقطه استفاده می‌کند، امکان مسدودسازی دسترسی بات به آدرس‌های شبکه‌ی کنترل و فرمان وجود ندارد اما می‌توان در صورت امکان، پورت‌هایی که این بدافزار بر روی آن‌ها فعالیت دارد را بر روی دیوار آتش مسدود کرد. دسترسی این پورت‌ها بایستی هم از داخل به خارج و هم از خارج به داخل مسدود شود. این پورت‌ها عبارتند از:

- 21810
- 22292
- 34354
- 34355
- 16464
- 16465
- 16470
- 16471

به علاوه می‌توان با استفاده از آنتی‌ویروس‌های تحت شبکه و نیز دیوارهای آتش، از دسترسی کاربران به وب‌سایت‌های آلوده به بسته‌های اکسپلویت و نیز انتقال فایل بدافزار از روی شبکه جلوگیری کرد.

شیوه‌ی مقابله در سطح میزبان

برای پیشگیری از آلودگی به بات، بایستی بر روی میزبان‌ها نرم‌افزار ضد بدفزار به‌روز رسانی شده نصب کرد، آخرین به‌روز رسانی‌های ویندوز و برنامه‌های جانبی آن را بر روی میزبان‌ها اعمال و ترجیحا از مرورگرهای امن‌تر مانند کروم برای مرور صفحات وب استفاده کرد. در صورتی که میزبان‌ها به هر دلیل به این بدافزار آلوده شده باشند بایستی از ابزارهای موجود که لیست برخی از آن‌ها در ادامه ارایه شده است، برای پاک‌سازی سیستم هدف استفاده نمود.

- http://download.avg.com/filedir/util/avgrem/avg_remover_zeroaccess.exe
- http://www.symantec.com/content/en/us/global/removal_tool/threat_writeups/FixZeroAccess.exe
- http://www.mcafee.com/in/downloads/free-tools/rootkitremover.aspx

در صورتی که نیاز به پاک‌سازی دستی میزبان‌ها می‌باشد، می‌توان از راهنمای ارایه شده در یکی از لینک‌های زیر استفاده نمود:

- http://www.symantec.com/security_response/writeup.jsp?docid=2011-121607-4952-99
- http://malwaretips.com/blogs/trojan-zeroaccess-removal/