باسمه تعالی

گزارش فنی بدافزار GameOver Zeus

توصیف کلی

بدافزار GameOver Zeus نخستین‌بار در سپتامبر ۲۰۱۱ شناسایی شده است. این بدافزار عمدتاً از طریق هرزنامه‌ها و شبکه‌های بات منتشر شده و از یک مکانیزم توزیع شده مبتنی بر شبکه‌های همتا-به-همتا (P2P) برای ارسال و دریافت فرامین و داده‌ها مابین سیستم‌های آلوده و کارگزارهای کنترل و فرمان استفاده می‌کند. یکی دیگر از روش‌های انتقال اطلاعات توسط این بدافزار، استفاده از ارتباطات http بر اساس نام دامنه‌های تصادفی است. عملکرد اصلی این بدافزار سرقت اطلاعات بانکی قربانیان و استفاده از سیستم‌های آلوده برای انجام حملات DDoS می‌باشد. به‌دلیل آن‌که از سیستم‌های آلوده به این بدافزار برای انجام حملات DDoS و سایر جرایم سایبری استفاده می‌شود، رسیدگی به وضعیت آلودگی سیستم‌های سازمان به این بدافزار ضروری به نظر می‌رسد چرا که انجام حمله DDoS با استفاده از سیستم‌های آلوده به این بدافزار می‌تواند مشکلات حقوق برای سازمان ایجاد نماید.

روش انتشار

بدافزار GameOver Zeus عمدتاً از طریق هرزنامه‌ها و سایت‌های جعلی (Phishing) و نیز از طریق سایر شبکه‌های بات (مخصوصا شبکه بات Cutwail) منتشر می‌شود. کاربران معمولاً از طریق مراجعه به سایت‌های مخرب و یا باز نمودن ایمیل‌های جعلی ارسال شده آلوده می‌گردند.

تاثیرات

عمده‌ترین فعالیت‌های انجام شده توسط این بدافزار عبارتند از:

۱. سرقت اطلاعات بانکی و سایر اطلاعات ورود کاربران سیستم‌های آلوده
۲. استفاده از سیستم‌های آلوده برای انجام حملات DDoS
۳. استفاده از سیستم‌های آلوده برای ارسال هرزنامه در مقیاس بزرگ
۴. آلوده‌سازی سیستم‌های آلوده به باج‌افزارها از جمله باج‌افزار CryptoLocker
۵. استفاده از سیستم‌های آلوده برای انجام سایر جرایم سایبری

روش انتقال اطلاعات

بدافزار GameOver Zeus از یک شبکه همتا به همتای رمز شده برای انتقال اطلاعات مابین سیستم‌های آلوده و کارگزاران کنترل و فرمان استفاده می‌کند. الگوریتم استفاده شده برای طراحی شبکه همتا به همتای بدافزار بسیار شبیه به پروتکل همتا به همتای Kademlia می‌باشد. همچنین یکی دیگر از تکنیک‌های مورد استفاده این بدافزار برای انتقال اطلاعات، استفاده از ارتباطات http بر مبنای نام‌های دامنه تولید شده به صورت تصادفی است. این نام‌های دامنه برای هر روز متفاوت هستند. در نتیجه قطع ارتباط این بدافزار با کارگزار کنترل و فرمان آن به سادگی امکان‌پذیر نیست.

راه‌کار تشخیص

در سطح میزبان:

۱. استفاده از محصولات ضد بدافزار و ابزارهای آنلاین بررسی آلودگی
۲. Resolve شدن نام‌های دامنه غیر عادی و طولانی مانند g8pf2nyuft5ls82ow51ju2b09.net توسط سیستم
۳. برقراری ارتباطات شبکه توسط پروسه‌ی Explorer.exe
۴. وجود کلید رجیستری مشکوک برای اجرای فایل‌هایی با نام تصادفی در هنگام بوت سیستم

در سطح شبکه:

۱. Resolve نام‌های دامنه غیرعادی مانند g8pf2nyuft5ls82ow51ju2b09.net توسط میزبان‌های شبکه
۲. تعداد زیاد کانکشن‌های برقرار شده از یک میزبان

راه‌کار پیشگیری

در سطح میزبان:

۱. تا جای ممکن از باز نمودن ایمیل‌های ناشناس خودداری شود.

۲. تا جای ممکن از بازدید از سایت‌های نامطمئن خودداری شود.
۳. سیستم‌عامل، نرم‌افزار ضد ویروس و نرم‌افزارهای نصب شده بر روی سیستم‌های سازمان به‌روز باشند.
۴. از دادن دسترسی مدیریت به کاربران عادی سیستم‌های سازمان خودداری شود.

در سطح شبکه:

۱. ممانعت از دسترسی کاربران شبکه به سایت‌های مخرب مشهور
۲. استفاده از ضد ویروس‌های تحت شبکه
۳. استفاده از UTM در ورودی شبکه
۴. استفاده از ضد بدافزار بر روی کارگزار پست الکترونیک سازمان
۵. استفاده از فیلترهای مناسب ضد هرزنامه بر روی پست الکترونیک سازمان
۶. استفاده از سامانه‌های مدیریت وصله مانند WSUS به منظور مدیریت آسیب‌پذیری سیستم‌ها و جلوگیری از سوء استفاده از نقاط آسیب‌پذیر آن‌ها برای نصب بدافزار

راه‌کار رفع آلودگی

در سطح میزبان:

۱. استفاده از محصولات ضد بدافزار برای رفع آلودگی من جمله:
   a. www.mcafee.com/stinger
   b. www.f-secure.com/en/web/home_global/online-scanner
   c. www.sophos.com/VirusRemoval
۲. تغییر تمامی گذرواژه‌ها و همچنین وادار ساختن کاربران به تغییر گذرواژه‌ها
۳. به‌روز رسانی سیستم‌عامل، نرم‌افزار ضد ویروس، مرورگر وب و سایر نرم‌افزارهای نصب شده بر روی سیستم‌های سازمان

در سطح شبکه:

به دلیل ماهیت همتا به همتای سیستم انتقال اطلاعات در بدافزار GameOver Zeus، قطع دسترسی سیستم‌های آلوده به کارگزار کنترل و فرمان به سادگی امکان پذیر نیست اما می‌توان با استفاده از روش‌های زیر تا حد ممکن از آثار ثانویه آلودگی جلوگیری نمود:

۱. محدود کردن ترافیک ICMP در خروجی شبکه (به منظور ممانعت از استفاده از سیستم‌های آلوده برای انجام حمله DDoS)
۲. محدود کردن ترافیک DNS در خروجی شبکه (به منظور ممانعت از استفاده از سیستم‌های آلوده برای انجام حمله DDoS)
۳. محدود کردن ارسال ایمیل از داخل شبکه (برای جلوگیری از ارسال هرزنامه توسط سیستم‌های آلوده)
۴. محدود کردن تعداد کانکشن‌ها به ازای هر آدرس IP (به منظور جلوگیری از انجام حمله DDoS، Syn Flood و همچنین تا حدی جلوگیری از دسترسی به شبکه‌های P2P)
۵. مسدود کردن دریافت ایمیل از MTAهای مشکوک و مخرب توسط کارگزار ایمیل
۶. جداسازی شبکه دسترسی به اینترنت از شبکه داخلی سازمان