بسمه‌تعالی

گزارش تحلیل بدافزار Zeus

مقدمه

امروزه یکی از مهمترین تهدیداتی که کاربران اینترنت با آن مواجه هستند، تهدید بدافزارهاست. یکی از خطرناک‌ترین و شایع‌ترین این بدافزارها، بدافزار Zeus است که در این نوشتار به معرفی، بررسی جزئیات و نیز تحلیل آن خواهیم پرداخت.

زئوس در واقع یک مجموعه جرم‌افزار (Crimeware) است که هدف اصلی از طراحی آن (در کنار دیگر موارد) سرقت اطلاعات بانکی و مشخصات ورود (نام کاربری/گذرواژه) افراد است. این بدافزار ساخته دست مجرمین سازمان یافته‌ی اروپای شرقی است و توسط این مجرمین در بازارهای زیرزمینی مجرمین اینترنتی خرید و فروش می‌شود. قیمت زئوس در بازارهای زیرزمینی در حالت پایه حدود ۳۰۰۰ الی ۴۰۰۰ دلار است. زئوس با نام‌های مختلفی شناخته می‌شود که برخی از آن‌ها عبارتند از: Zbot (به سبب توانایی این بدافزار در ایجاد شبکه بات)، WSNPoem، PRG و غیره.

به صورت خلاصه، زئوس را می‌توان از دو دیدگاه بررسی نمود:

- از دیدگاه فنی، زئوس یک جرم‌افزار است که کاربرد اصلی آن سرقت پول از حساب‌های بانکی است.
- از دیدگاه غیرفنی، زئوس آغاز یک موج جدید در صنعت جرایم مالی اینترنتی است که در این صنعت سازمان‌های مختلفی با هم همکاری می‌کنند تا بتوانند بیشترین بهره‌برداری را از تقلب و سرقت اینترنتی داشته باشند.

هرچند مجرمین اصلی پشتوانه زئوس، ساکن اروپای شرقی و روسیه هستند، لیکن پس از ظهور ابزار ساخت زئوس در بازارهای زیرزمینی، امروزه تمامی افراد و گروه‌ها با دانش بسیار کم نیز به راحتی قادر به ایجاد و بهره‌برداری از یک شبکه بات زئوس هستند. با همه این تفاسیر، هنوز هم تفاوت عمده‌ای میان مجرمین حرفه‌ای و آماتور وجود دارد چرا که برای سرقت پول تنها داشتن بات‌نت کافی نیست بلکه مجرمین بایستی ارتباطات کاری و مالی نیز داشته باشند تا بتوانند پول سرقت شده را انتقال داده و عمل پول‌شویی را انجام دهند.

برخی از مهمترین ویژگی‌های زئوس عبارتند از:

- سرقت اطلاعات وارد شده در فرم‌های http
- سرقت اطلاعات حساب‌کاربری ذخیره شده در Windows Protected Storage
- سرقت گواهی‌های X.509 سمت کاربر
- سرقت اطلاعات حساب‌های FTP و POP
- سرقت/حذف کوکی‌های http و Flash
- تغییر کد HTML صفحات وب‌سایت‌های هدف به منظور سرقت اطلاعات
- تغییر مسیر کاربر از صفحات وب‌سایت هدف به سمت صفحات کنترل شده توسط حمله کننده
- عکس گرفتن از محیط کار کاربر و نیز دزدی کد HTML صفحات وب‌سایت‌های بازدید شده
- جستجو در میان فایل‌های موجود بر روی سیستم قربانی و آپلود آن‌ها در صورت نیاز
- تغییر فایل Hosts محلی
- دانلود و اجرای برنامه‌های دلخواه حمله کننده
- حذف مدخل‌های حساس رجیستری ویندوز به منظور خرابکاری و جلوگیری از بوت شدن ویندوز
- ارسال اطلاعات با استفاده از شبکه‌های P2P
- استفاده از نام‌های دامنه تصادفی برای برقراری ارتباط با کارگزار کنترل و فرمان
- استفاده از نام‌های تصادفی برای فایل‌ها و مسیرهای ایجاد شده توسط بدافزار
- داشتن نسخه مخصوص سیستم عامل‌های مختلف موبایل به منظور سرقت اطلاعات از موبایل افراد
- داشتن نسخه‌ی ۶۴ بیتی برای کار بر روی سیستم‌های اینچنینی

نکته‌ی جالب توجه دیگر در رابطه با این بدافزار، مکانیزم قوی جلوگیری از کپی غیر مجاز بدافزار است. فروشندگان این بدافزار از یک مکانیزم پیچیده‌ی مبتنی بر مشخصات سخت‌افزاری برای جلوگیری از کپی برداری ابزار سازنده توسط مجرمان استفاده می‌کنند. این نوع کنترل شدید برای جلوگیری از تکثیر غیر مجاز،

در میان بدافزارها برای اولین بار است که با این شدت اعمال شده است که این خود گواهی بر سود دهی فراوان فروش این بدافزار برای توسعه‌دهنده‌گان آن است.

ساختار کلی بدافزار زئوس

از دیدگاه فنی و خصوصاً از دیدگاه عملکردی، زئوس آنقدرها پیچیده نیست؛ هرچند که تکنیک‌های رمزنگاری و پنهان‌سازی این بدافزار پیچیده بوده و قادر به انجام اعمال متنوعی می‌باشد. اما توضیح عملکرد کلی این بدافزار بسیار ساده است. یک شبکه بات زئوس در کل از ۳ مولفه تشکیل شده است:

1. فایل اجرایی بدافزار زئوس (تروجان زئوس)
2. فایل پیکربندی زئوس
3. منطقه‌ی تخلیه زئوس (Drop Zone) که اطلاعات سرقت شده به آنجا ارسال می‌گردند.

زئوس در گام اول از روش‌های مختلفی برای نصب بدافزار بر روی سیستم هدف استفاده می‌کند که در بخش‌های بعدی بیشتر توضیح داده خواهد شد. پس از آنکه زئوس بر روی سیستم هدف اجرا شد، فایل پیکربندی خود را از مکان مشخصی بارگذاری کرده و با استفاده از اطلاعات دریافتی از فایل پیکربندی (که معمولاً شامل لیستی از بانک‌های منتخب، آدرس URL ورود به سامانه‌ی این بانک‌ها و اطلاعات اینجکتینی می‌باشد)، منتظر ورود قربانی به سامانه‌ی یکی از این بانک‌ها می‌ماند تا بتواند اطلاعات کاربر را سرقت کند.

بر خلاف Keylogger های سنتی، تروجان‌های زئوس از تکنیک فرد-در-مرورگر (men-in-the-browser) استفاده می‌کنند که اطلاعات حساس را از نشست مرورگر کاربر (مانند یک نشست بانکداری الکترونیک) سرقت می‌کنند. این ویژگی، میزان خطر این بدافزار را دوچندان می‌کند زیرا این بدافزار قادر است فیلدهای اضافه‌ای را به فرم‌های مجاز نشست وب افزوده و از این طریق کاربر را وادار به ورود اطلاعات حساسی کند که در حالت عادی نیازی به ورود آن‌ها نیست.

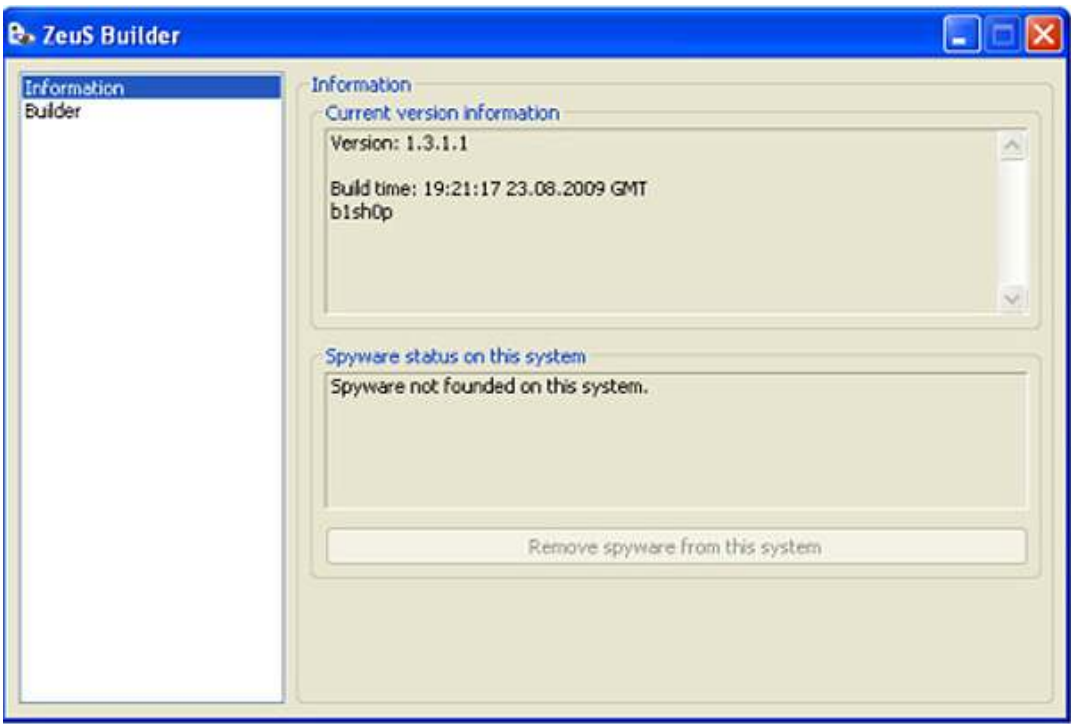
برخی از نسخه‌های زئوس ویژگی دیگری با نام JabberZeus دارند که قادر است اطلاعات حساس کاربر را به صورت برخط و به لحظه با استفاده از یک سرویس ارسال پیام لحظه‌ای (IM) برای مجرمین ارسال کند.

این ویژگی، مجرمین را قادر می‌سازد که بتوانند اغلب سامانه‌های احراز اصالت چند فاکتوری را دور زده و وارد حساب کاربری بانکی قربانیان شوند و به سرقت از حساب آنان بپردازند.

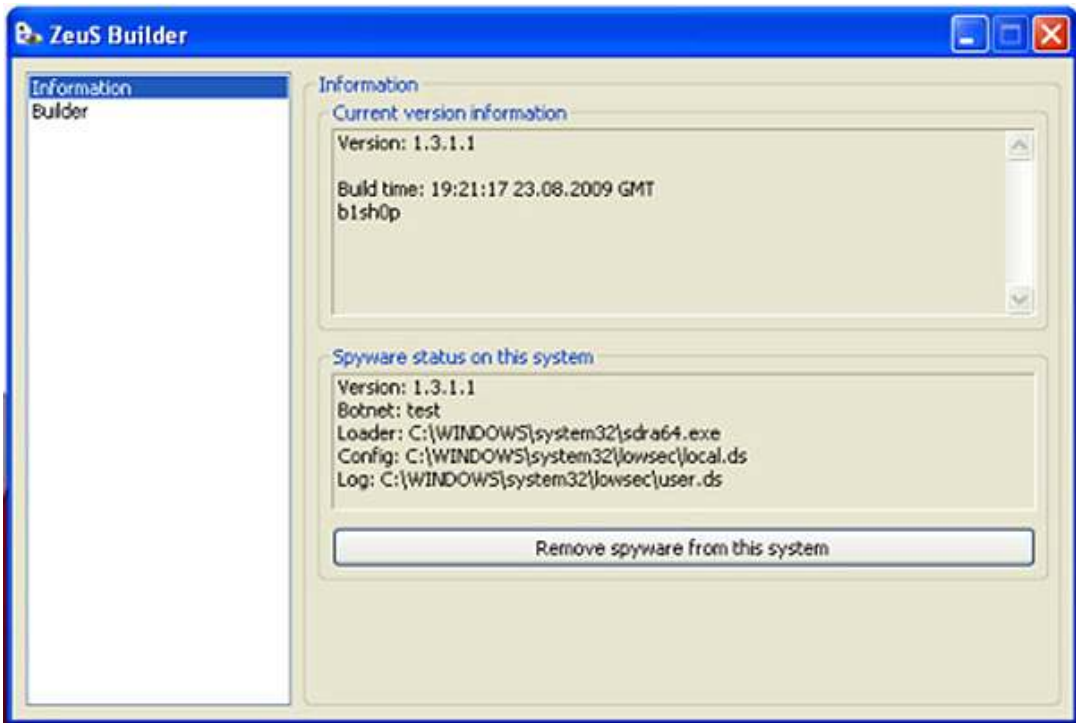
مولفه‌های بدافزار زئوس

Zeus Builder یکی از بخش‌های اصلی مجموعه Zeus است. وظیفه اصلی این ابزار، ساخت فایل اجرایی بدافزار زئوس (که شبکه بات با استفاده از آن ساخته می‌شود) و نیز فایل پیکربندی (که تمامی اطلاعات پیکربندی شبکه بات در آن ذخیره می‌شود) می‌باشد.

وقتی که مجرم برای اولین بار ابزار Zeus Builder را اجرا می‌کند، با یک صفحه‌ی ساده مواجه می‌شود که اطلاعات نسخه‌ای از زئوس که سفارش داده شده است را نشان می‌دهد. نکته جالب اینجاست که این ابزار همچنین بررسی می‌کند که آیا سیستم جاری به بدافزار زئوس آلوده است یا خیر و در صورت آلوده بودن امکان حذف بدافزار از سیستم‌جاری را نیز برای کاربر فراهم می‌کند.



شکل 1- صفحه اصلی ابزار Zeus Builder



شکل 2- صفحه اصلی ابزار Zeus Builder بر روی سیستمی که به بدافزار زئوس آلوده است.

تمامی شبکه‌های بات زئوس بر مبنای یک فایل پیکربندی بسیار انعطاف‌پذیر ساخته می‌شوند. این فایل شامل تنظیماتی مانند نام شبکه‌ی بات، بازه‌ی زمانی میان ارسال اطلاعات دزدیده شده به مجرم و نیز آدرس کارگزاری است که بدافزار بایستی به آن متصل شود. اطلاعات مهمتر دیگری که در این فایل وجود دارد، لیستی از نام بانک‌هایی است که زئوس آن‌ها را هدف قرار می‌دهد. زئوس نه تنها قادر به جمع‌آوری تمامی اطلاعات ورود به حساب بانکی و سایر حساب‌های کاربران است، بلکه می‌تواند با تزریق فیلدهای اضافی به فرم‌های سامانه‌ی بانکداری الکترونیک کاربر، کاربر را وادار به وارد کردن اطلاعات حساس دیگری نیز بنماید.

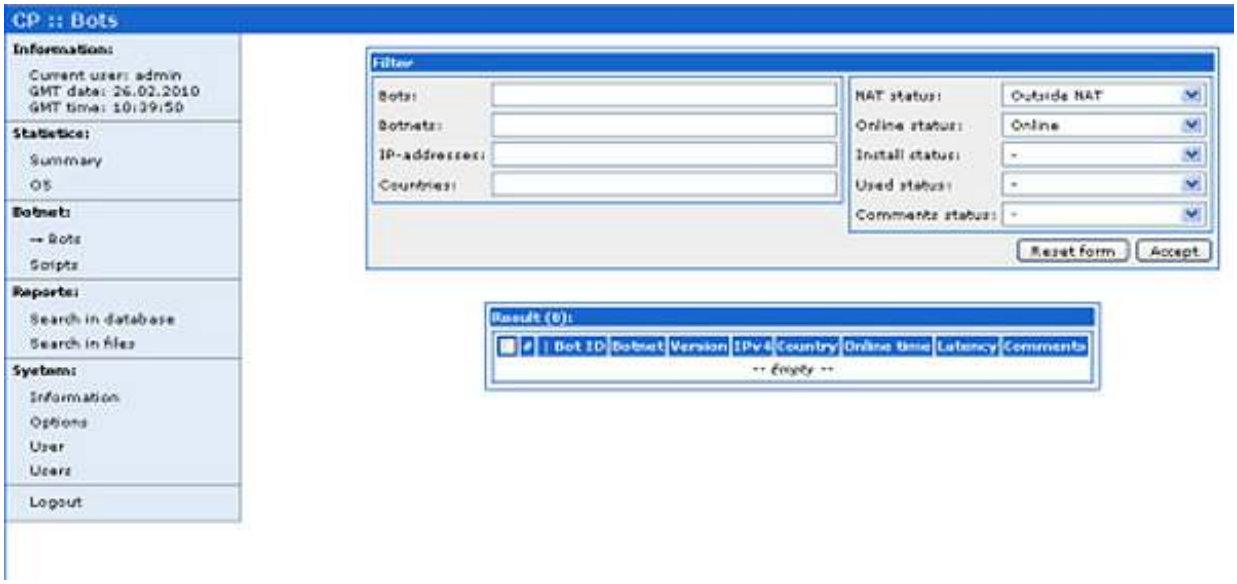
ابزار Zeus Builder سپس این فایل پیکربندی را دریافت کرده و آن را رمزگذاری می‌کند. تمامی بات‌های زئوس به صورت مداوم با کارگزار کنترل و فرمان در ارتباط بوده و فایل پیکربندی رمزگذاری شده را بارگذاری می‌کنند تا از دریافت آخرین دستورات اطمینان حاصل کنند.

شکل 3- بخشی از یک فایل پیکربندی زئوس که بانک‌های هدف قرار گرفته را نشان می‌دهد.

پس از تولید فایل پیکربندی، مجرمین هر دو فایل اجرایی و پیکربندی که با استفاده از ابزار Zues Builder تولید کرده‌اند را بر روی یک کارگزار وب قرار می‌دهند. زئوس این قابلیت را دارد که هر دو فایل اجرایی و پیکربندی بر روی یک کارگزار و یا بر روی دو کارگزار مختلف قرار گیرند. پس از آنکه سیستم یک قربانی به بدافزار Zeus آلوده شد، بدافزار آخرین نسخه از فایل پیکربندی را دریافت کرده و با اعمال آن، شروع به سرقت اطلاعات حساس کاربر می‌نماید. در نتیجه مجرمین به سادگی و تنها پس از چند کلیک می‌توانند یک شبکه‌ی بات حرفه‌ای و آماده راه‌اندازی کنند. کارگزار زئوس نیز به سادگی قابل نصب و راه‌اندازی است. مجرم به سادگی فایل‌های کارگزار وب را بر روی سیستم خود کپی کرده و صفحه‌ی نصب را با استفاده از مرورگر خود مرور می‌نماید که در این صفحه نیز صرفاً اعمال برخی تنظیمات ساده و کلی نیاز است.

شکل 4- صفحه‌ی نصب کارگزار زئوس

پس از راه‌اندازی، کارگزار تمامی اطلاعات دزدیده شده توسط بات‌های زئوس را دریافت می‌کند. این کارگزار قابلیت‌های دیگری از جمله نگهداری تعداد کاربران آلوده (بر حسب سیستم‌عامل، موقعیت جغرافیایی و ...) و اجرای اسکریپت دلخواه بر روی ماشین‌های آلوده را نیز دارا می‌باشد.

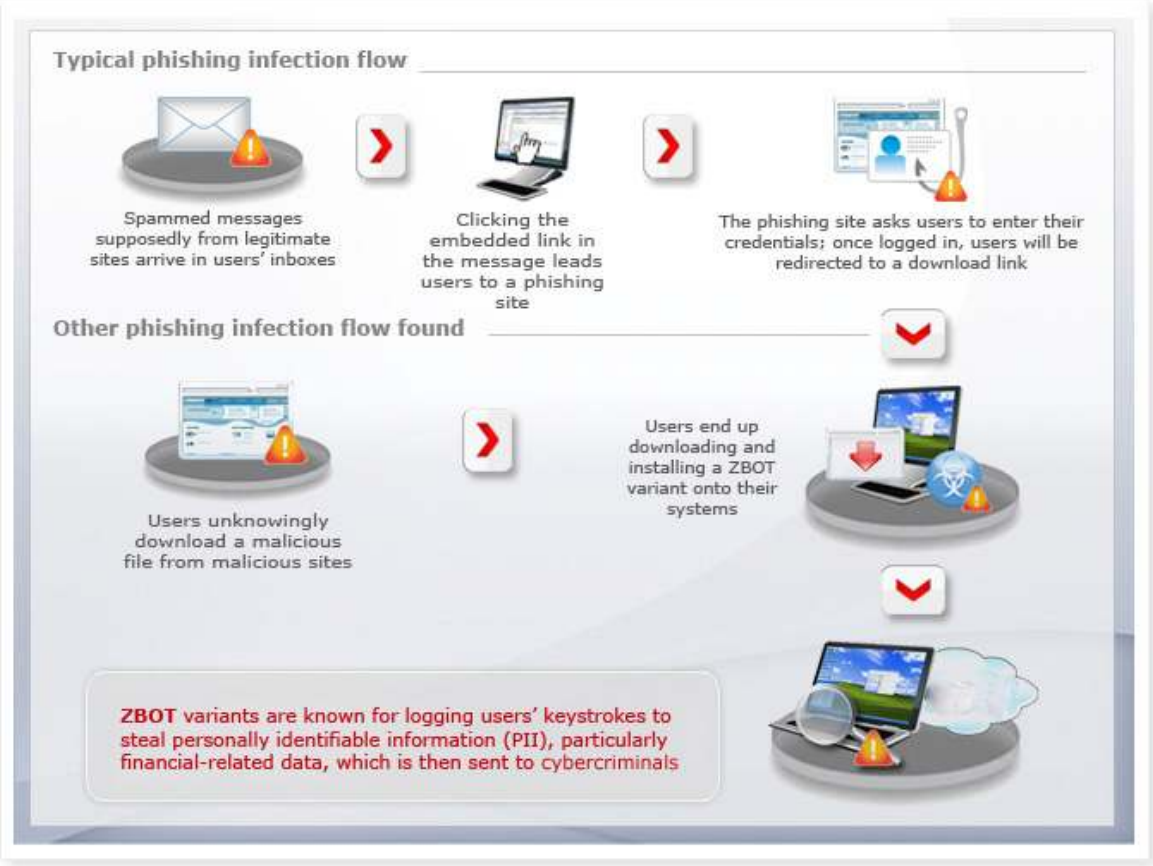


شکل 5- نمایی از برخی دیگر از ویژگی‌های کارگزار زئوس

Zeus Builder و کارگزار زئوس عوامل اصلی شناسایی زئوس به عنوان ابزار استاندارد و ملزم برای مجرمین سایبری هستند. این ابزارها سبب شده‌اند که افرادی با کمترین دانش فنی نیز بتوانند به سادگی و در عرض کمتر از ۵ دقیقه یک شبکه بات بسیار حرفه‌ای و کارآمد ایجاد کنند. سادگی استفاده از زئوس عامل اصلی فروش بسیار زیاد است و همین موضوع نیز سبب شده که پیش‌بینی‌ها از عدم از بین رفتن شبکه‌های بات زئوس در آینده نزدیک حکایت داشته باشد.

فرآیند آلوده شدن به بدافزار زئوس

شکل زیر فرآیند معمول آلودگی به زئوس را نشان می‌دهد.



شکل 6- فرآیند معمول آلودگی به زئوس

همانطور که در تصویر فوق نیز قابل مشاهده است، آلودگی به زئوس معمولاً از طریق اسپم انجام می‌گیرد. در این حالت کاربر با دریافت یک ایمیل مشکوک و باز کردن فایل الصاق شده که یک فایل آلوده به بدفزار زئوس است، سبب آلوده شدن رایانه خود به بدافزار زئوس می‌گردد. در نسخه‌های جدیدتر بدافزار زئوس، روش‌های دیگری مانند آلودگی با استفاده از بدافزارهای فیس‌بوکی، Drive-by-download و غیره نیز مشاهده شده است.

شکل 7- هرزنامه فیس‌بوکی برای آلوده‌سازی زئوس

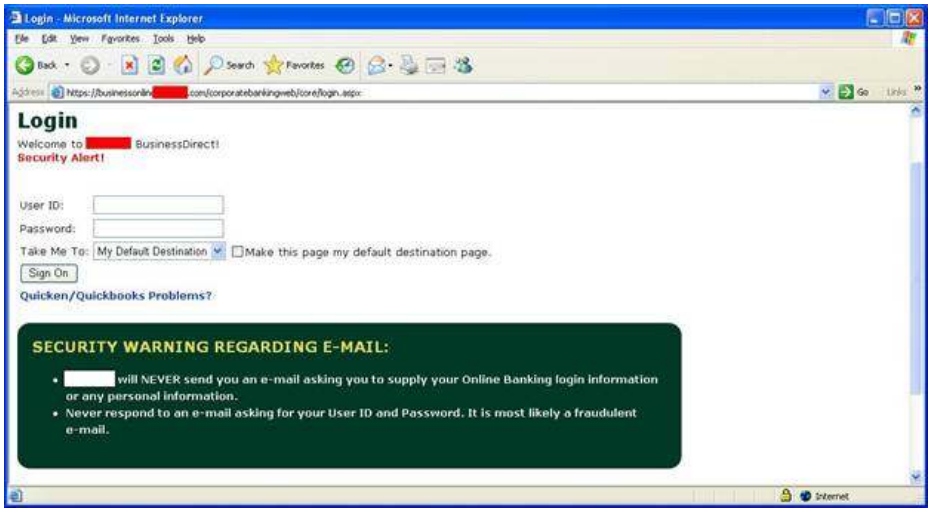
شکل 8 صفحه‌ی قلابی فیس‌بوک برای انتشار زئوس با استفاده از شبکه‌ی بات Avalanche

عملکرد بدافزار زئوس

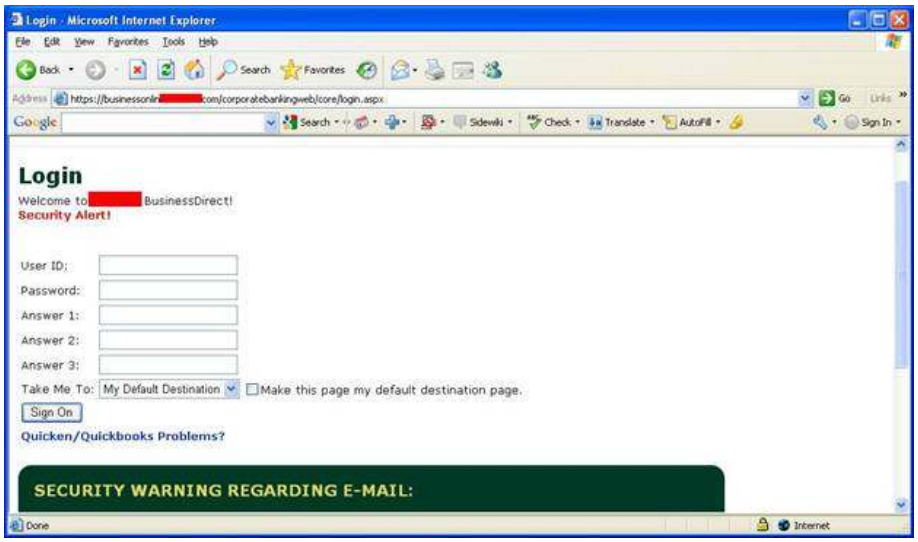
کارکرد اصلی زئوس در دو بخش اصلی خلاصه می‌شود که عبارتند از:

1. سرقت اطلاعات و ارسال آن‌ها به محل تخلیه
2. اجرای فرامین دریافتی از کارگزار کنترل و فرمان

الگوریتم رمزنگاری استفاده شده توسط زئوس، الگوریتم RC4 بوده که کلید رمزنگاری در داخل کد بدافزار قرار داده شده است. هرچند که هدف اصلی این بدافزار سرقت اطلاعات بانکی است اما ماهیت کلی این بدافزار به گونه‌ای است که توانایی سرقت هرگونه اطلاعاتی را دارد و در نتیجه خطری بزرگ برای تمامی شرکت‌ها و افراد محسوب می‌شود. هرچند که این بدافزار امکان سرقت هرگونه اطلاعات را دارد اما گردانندگان شبکه‌های بات معمولاً سامانه‌های بانکداری خاصی را مدنظر دارند و تلاش دارند مشتریان این سامانه‌ها را هدف قرار داده و به سرقت پول از آن‌ها بپردازند. بسیاری از اعمالی که توسط بدافزار زئوس انجام می‌گیرد بر حسب تقاضای گرداننده‌ی شبکه‌ی بات و با استفاده از واسط وب کارگزار زئوس در قالب اسکریپت‌های خاصی به بات‌ها ارسال شده و توسط آن‌ها اجرا می‌گردد.



شکل 9- صفحه‌ی ورود یک سایت مالی



شکل 10- صفحه‌ی ورود به همان سایت بر روی یک سیستم آلوده به زئوس. به سه فیلد اضافی افزوده شده توسط زئوس دقت شود.

هنگامی که فایل بدافزار زئوس بر روی یک سیستم اجرا می‌شود یک سری مراحل برای نصب و پیکربندی بدافزار بر روی سیستم طی می‌شوند که عبارتند از:

1. تابع نصب، به دنبال پروسه‌ی Winlogon.exe می‌گردد و پس از یافتن آن، مقداری از فضای حافظه‌ی این پروسه را به خود اختصاص داده و کد اجرایی اصلی خود را رمزگشایی کرده و در این حافظه می‌نویسد.
2. فایل اجرایی برنامه بر روی هارد دیسک در مسیر C:\WINDOWS\system32\sdra64.exe کپی می‌شود (نسخه‌های جدید بدافزار از اسامی تصادفی برای فایل استفاده می‌کنند).
3. مسیر C:\WINDOWS\system32\lowsec\ می‌شود (در نسخه‌های جدید این مسیر تصادفی است). این مسیر در Windows Explorer قابل رویت نیست اما از طریق cmd قابل رویت است. این مسیر حاوی فایل‌های زیر است:
   a) Local.ds: که شامل جدیدترین نسخه فایل پیکربندی بارگزاری شده است.
   b) User.ds: شامل اطلاعات جمع‌آوری شده است.
   c) User.ds.iii: در صورتی که انتقال اطلاعات به کارگزار با خطا مواجه شود به صورت موقت ایجاد می‌شود.

4. مسیر فایل اجرایی بات به مقدار کلید رجیستری فایل Winlogon (در مسیر HKLM/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/Winlogon) الحاق می‌شود. این موضوع سبب می‌شود که بات در هر بار بوت ویندوز اجرا شود.
5. فایروال ویندوز XP غیر فعال می‌شود.
6. بات، یک دستور M-SEARCH را به صورت همه پخشی بر روی شبکه ارسال می‌کند تا دستگاه‌های UPnP موجود در شبکه را شناسایی کند.
7. بات، یک درخواست HTTP GET به کارگزار زئوس ارسال می‌کند تا آخرین فایل پیکربندی را دریافت کند.
8. بات شروع به جمع‌آوری اطلاعات از کامپیوتر قربانی می‌کند.
9. بات، دو درخواست HTTP POST برای کارگزار ارسال می‌کند تا فایل user.ds و نیز اطلاعات آماری جمع‌آوری شده را برای آن ارسال کند.

اطلاعات هدف قرار گرفته توسط زئوس برای سرقت

اطلاعاتی که از هر قربانی سرقت می‌شود، بر روی کارگزار در یک فولدر جداگانه ذخیره سازی می‌شود:

شکل 11- اطلاعات سرقت شده از هر قربانی در یک فولدر جداگانه بر روی کارگزار ذخیره سازی می‌شود.

شکل زیر نمونه‌ای از اطلاعات جمع‌آوری شده از یک قربانی که با یک شبکه اجتماعی مرتبط است را نشان می‌دهد.

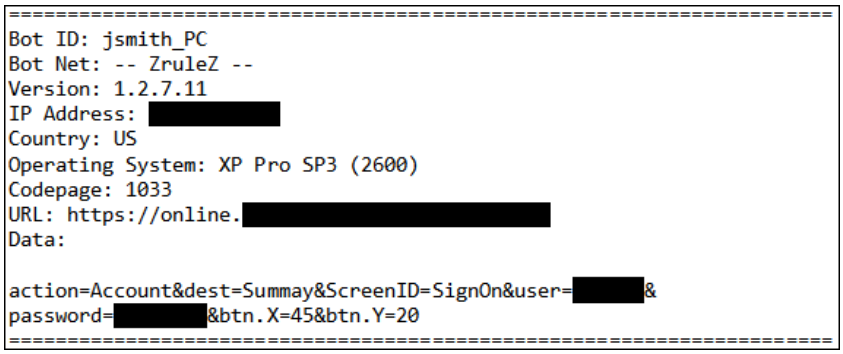
```
==========================================================================
Bot ID: jsmith_PC
Bot Net: -- ZruleZ --
Version: 1.2.7.11
IP Address: [redacted]
Country: US
Operating System: XP Pro SP3 (2600)
Codepage: 1033
URL: https://login.[redacted]
Data:

locale=en_US&email=[redacted]&pass=[redacted]
==========================================================================
```

شکل 12- نمونه‌ای از اطلاعات جمع‌آوری شده از یک سیستم آلوده برای وب‌سایت یک شبکه اجتماعی

این اطلاعات شامل موارد زیر است:

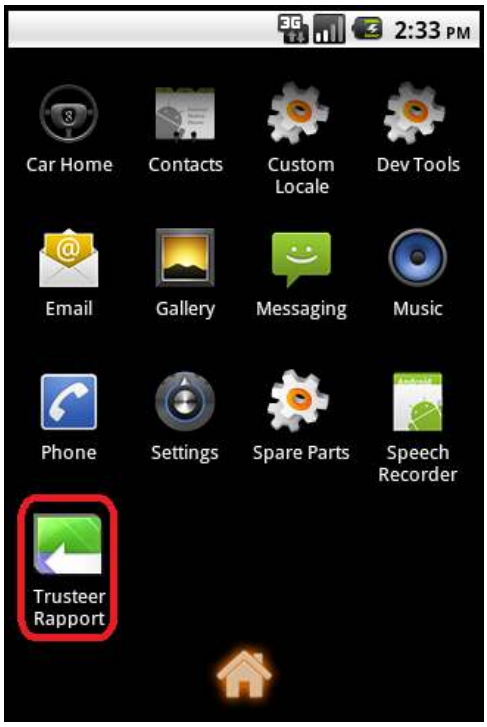
- لیست با Bot ID شروع می‌شود که معمولاً نام کامپیوتر آلوده شده است.
- بعد از آن نام شبکه‌ی بات و نیز نسخه‌ی بدافزار نصب شده ارسال می‌گردد.
- بعد از آن آدرس IP سیستم آلوده و نیز نام کشوری که سیستم به آن تعلق دارد ارسال می‌شود.
- بعد از آن نام سیستم عامل قربانی ارسال می‌شود.
- بعد از آن آدرس سایت بازدید شده و نیز مشخصات ارسال شده به سایت جمع‌آوری شده و ارسال می‌شود.



شکل 13- نمونه‌ای از اطلاعات بانکی استخراج شده از سیستم قربانی

زئوس در تلفن همراه

بدافزار زئوس نسخه‌ای مخصوص سیستم عامل‌های مختلف موبایل (مانند ویندوز موبایل، سیمبین و اندروید) نیز دارد که برای دزدی اطلاعات از تلفن همراه قربانی (به خصوص اطلاعات تراکنش که توسط بانک در قالب پیامک برای قربانی ارسال می‌شود)، مورد استفاده قرار می‌گیرد. این ویژگی به زئوس امکان می‌دهد که سیستم‌های احراز اصالت دو فاکتوری رایج که بر مبنای ارسال پیامک کار می‌کنند را نیز دور بزند. نسخه‌ی اندروید بدافزار موبایل ZitMo نامیده می‌شود.



شکل 14- آیکون اجرای نسخه‌ی اندروید بدافزار ZitMo

مقابله با زئوس

برای مقابله با بدافزار زئوس دو راه وجود دارد. اولین راه حذف بدافزار به صورت دستی و راه دوم حذف بدافزار با استفاده از ابزارهای موجود است. برای حذف بدافزار به صورت دستی بایستی فایل‌های زیر را از سیستم آلوده حذف نمود:

در صورتی که میزان دسترسی شما در سیستم در حد مدیر است:

%systemroot%\system32\sdra64.exe (malware)
%systemroot%\system32\lowsec
%systemroot%\system32\lowsec\user.ds (encrypted stolen data file)
%systemroot%\system32\lowsec\user.ds.lll (temporary file for stolen data)
%systemroot%\system32\lowsec\local.ds (encrypted configuration file)

در غیر این صورت:

%appdata%\sdra64.exe
%appdata%\lowsec
%appdata%\lowsec\user.ds

%appdata%\lowsec\user.ds.lll
%appdata%\lowsec\local.ds

کلیدهای زیر نیز بایستی در رجیستری ویندوز تغییر یابند:

در صورتی که میزان دسترسی شما در سیستم در حد مدیر است:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
From: "Userinit" = "C:\WINDOWS\system32\userinit.exe"
To: "Userinit" = "C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe"

در غیر این صورت:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Add:
"Userinit" = "C:\Documents and Settings\<user>\Application Data\sdra64.exe"

از ابزارهای زیر نیز می‌توان برای حذف خودکار بدافزار زئوس استفاده کرد:

http://download.avg.com/filedir/util/avgrem/avg_remover_zbot.exe

http://www.symantec.com/security_response/writeup.jsp?docid=2014-052915-1402-99

http://kb.eset.com/esetkb/index?page=content&id=SOLN3170