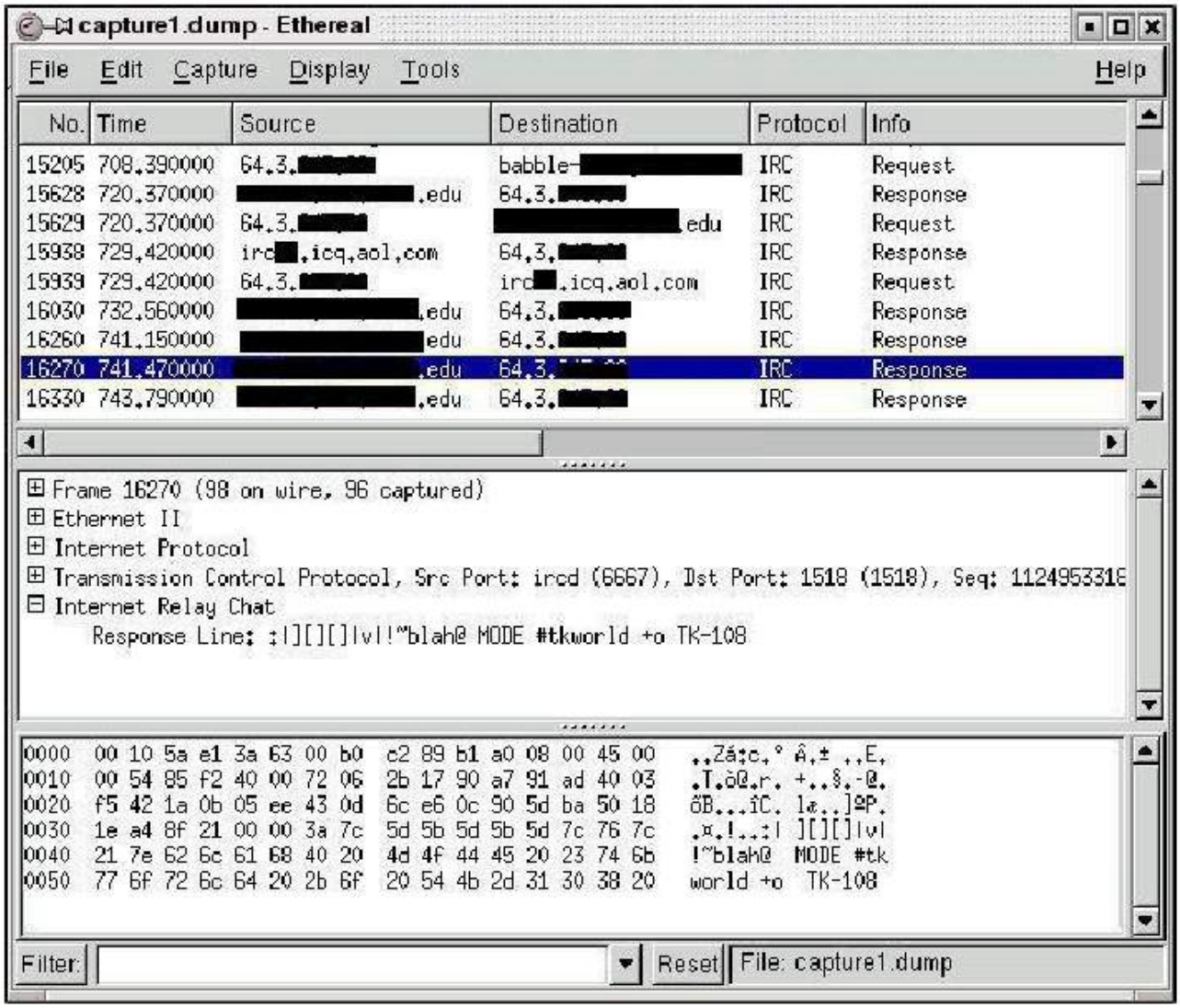
رو در روی انواع هکر

« قسمت آخر »

مترجم : رضا مددی
تاریخ : اول اردیبهشت ۱۳۸۳
نویسندگان : Cyrus Peikari, Seth Fogie

THR34T Krew : روز دوم، شب

بعد از یک بعدازظهر زیبا در کنار خانواده، آماده حمله به فایل توده (فایلی که در سایت از اطلاعات جمع آوری شده بود) شدم. توسط یک فیلتر، فایل را طوری Load کردم که فقط اطلاعاتی را نشان دهد که یا به آدرس IP سرور هک شده رفته و یا از آن برگشته باشند. همینکه فایل Load شد (و این عمل دقایقی به طول انجامید) سریعا ترافیک IRC را مورد نظر قرار دادم. طبق حدسهایی که زده بودم مطمئنا نشستی بین یک سرور IRC و سرور هک شده باز شده بود. همانطور که در شکل ۳ نشان داده شده است، شناخت نام اتاق و نوع عمومی فعالیتی که به نظر، دایمون IRC اسب تروا برای ارسال و دریافت انجام داده بود، براحتی قابل شناخت بودند.



شکل ۳

بسته‌های IRC ضبط شده

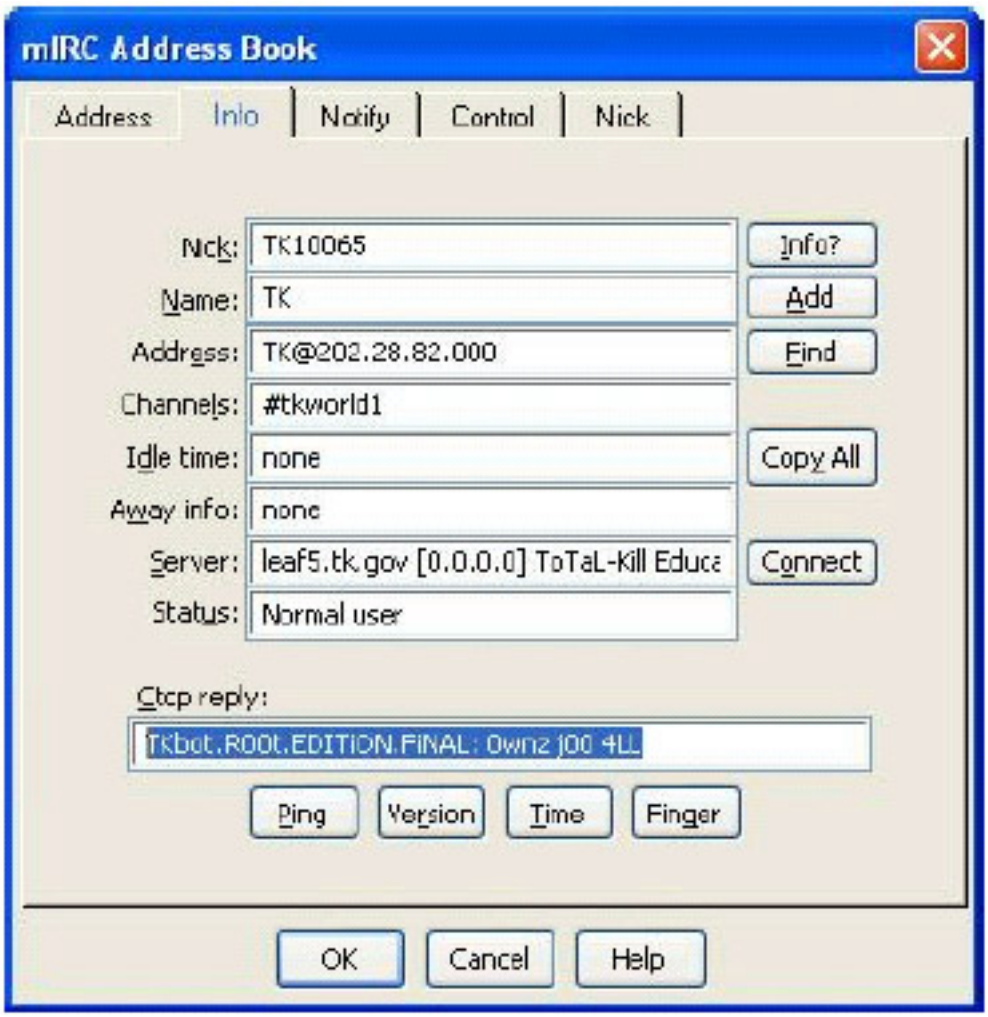
در هنگامی که من امیدوار بودم تا اطلاعات بیشتری از قبیل کلمات شناسه و عبور مورد نیاز برای فعال کردن اسب‌های تروای بر روی سرور بدست آورم، فایل توده‌ای که تهیه کرده بودم، تهی از هرگونه اطلاعات مفید و ارزشمندی شده بود، بنابراین من mIRC را اجرا کرده و آن را طوری تنظیم کردم که به سرور IRC مشکوک متصل شود. هنگامی که اتصال برقرار شد، مشخص شد که این سرور، یک سرور عادی و معمول چت نیست. اولین نظر من این بود که این سرور، یک سرور IRC از نوع warez بوده و در حقیقت به طور معمول به عنوان یک نرم افزار تحت اینترنت برای تعویض اتاق‌ها مورد استفاده قرار می‌گیرد. با استفاده از دستور List/ کانال‌های عمومی را بدست آوردم. فهرست گیری اتاق، نظرم را تایید می‌کرد، اما مانند خیلی چیزها در زندگی، شما نمی‌توانید در مورد کتابی از روی جلد آن نظر دهید!

بـا اسـتفاده از داده‌هـای ضبط شده، اتـــاقی را که به دنبال آن بودم، شناختم (#tkworld) ، بنابرایـن عـبارت /join #tkworld را تایـپ کردم، اما به من گفته شد که به یک کلمه عبور نیاز دارم. چـند کلمـه عـبور واضـح و بدیهی را امتحان کردم، اما درست نبودند. در مرحله بعد سعی کردم تا به #tkworld1 که آنهم در فایل توده نشان داده شده بود، متصل شوم. کار کرد. من داخل شده بودم!

همـانطوری که از شدت هیجان خوشحال بودم و با خودم می‌خندیدم، هنگامی که لیست اعضاء Load شـد، خـنده مـن سـریعا بـه یک آه کوتاه (از روی تعجب) تبدیل شد، چرا که فهمیدم در آن اتاق صدها و صدها نفر از مردم دیگر به همراه من وجود دارند.

بـه تدریـج بـر مـن معلـوم شـده بود که سرور مشتری من تنها یکی از صدها و شاید هزاران کامپـیوتر آلوده‌ای بود که به این اتاق چت متصل شده بودند. شوکه شده بودم. صفحه‌ها یکی پس از دیگـری پـر بـود از شناسه‌های عبور که از مقابل چشمانم عبور می‌کردند. به همراه هر شناسه عبور نامی وجود داشت که با عبارت TK آغاز شده و با یک عبارت ترکیبی افزایشی منظم از حروف و اعداد بـه پایـان رسیده بود. کم کم فهمیدم که سرور هک شده مشتری من احتمالا یکی از اولین قربانیان یک کرم جدید است.

هنگامـی کـه همچـنان در اتاق بودم شروع به نگاه کردن به اطلاعات کاربری کردم تا شاید از آنهـا چـیز جدیـدی بدسـت بیاورم. همانطوری که در شکل ۴ می‌بینید، اطلاعات کاربری بطور اساسی نشـان مـی‌دهـد کـه هـر کسـی که با چنین اسب تروای IRC آلوده شده است، با نامی از Tkbot (یا THR34T Krew's bot که بستگی به چگونگی نگاه شما به آن دارد) آورده شده است.



شکل ۴

اطلاعات مشتری IRC

آخر شب جمعه با (DOOM) |v| [][][][]

هـر چـند کـه موفق شده بودم وارد یک اتاق چت خصوصی شوم، اما عمر این پیروزی بسیار کوتاه بود. بیشتر از پنج دقیقه نگذشته بود که خود را اخراج شده از #tkworld1 دیدم. سعی کردم تا دوباره به داخل اتاق برگردم اما به نظر می‌رسید که اتاق قفل شده است. تلاش خود را برای پیدا کردن راهـی جهـت ورود به اتاق ادامه دادم و درمانده شده بودم، اما ناگهان متوجه شدم که یک اتاق جدید با نـام TK ظاهـر شده است. به سرعت به آن اتاق متصل شده (هیچ کلمه عبوری مورد نیاز نبود) و در آنجـا کاربری را با نامی هکری که آن نام را همچنین در اتاق #tkwprld1 و داخل فایل توده دیده بود، پـیدا کـردم (شـکل شـماره ۳ را ببینـید). بـا این وجود، از آنجایی که اسم، رمزی بود، نتوانستم از آن مطمئـن شوم که این اسم، متعلق به شخصی حقیقی باشد. کمی عامیانه ابتدا پیامی برای اتاق و سپس

بـه طـور مستقیم برای اسم مورد نظر فرستاده و از او پرسیدم که او شخصی حقیقی است یا فقط یک bot دیگر می‌باشد. در کمال تعجب عبارت |v|[[[[[به عنوان پاسخ فرستاده شد.

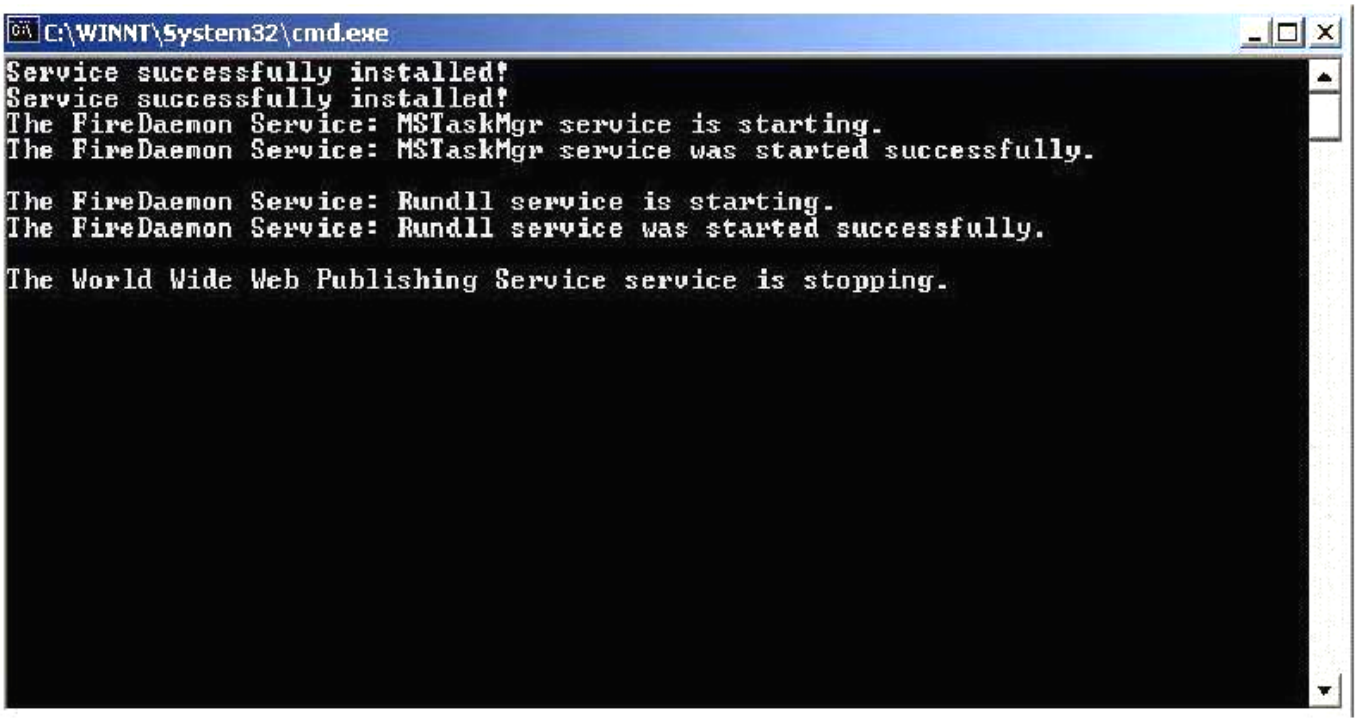
بـرای خلاصـه کـردن ایـن داسـتان طولانی باید بگویم که مکالمه ما در چندین عرصه صورت گرفـت. در ابـتدا DOOM خیلـی کـنجکاو بـود تا بداند که من کیستم، چگونه آنجا هستم و چه چیزی راجـع به #tkworld می‌دانم. من به عنوان پاسخ، نسخه کوتاهی از آنچه تا به حال گفته شده را برای او گفـتم و سپس از او پرسیدم که او چه می‌داند. بدون هیچ تعجبی، او در پاسخ دادن خیلی مبهم بود، اما چندین لقمه چرب و نرم اطلاعاتی جذاب را هدر داد!

- او سرور چت را برای یکی از «دوستان» نصب کرده بود.
- کرم TK به تازگی رها شده و سرور چت فقط به مدت چندین ساعت online بوده است.
- کرم IRC به صورت یک سرویس نصب شده است.
- ساختار کرم با بهره‌گیری ضعفهای IIS باعث گسترش آن می‌شود.
- برنامه IRC او با عنوان THr34t IRC نامگذاری شده است.
- او هنوز در مدرسه درس می‌خواند و در انگلیس زندگی می‌کند (احتمالا دروغ است)

مکالمـه در حـدود نـیم سـاعت بـه همراه بحث بر سر مطالب گوناگون به طول انجامید، اما در نهایـت با سوالی از طرف من به اتمام رسید. سوال من این بود که آیا من می‌توانم یک کپی از فایل‌های اسـب تروا را در اختیار بگیرم و آیا او می‌تواند کلمه عبور اتاق‌های #tkworld را به من بدهد؟ هر دو پاسـخ بطـور مودبانـه‌ای رد شد اما من اطلاعات زیادی بدست آورده بودم و می‌توانستم به کمک آنها جستجو برای بدست آوردن پاسخهایم را شروع کنم. از اتاق Sign Off کرده و رفتم تا کمی بخوابم.

آلوده شده با TKbot : صبح شنبه

در حال حاضر من یک خط سیر داشته و می‌توانم مستقیما آنچه را که اسب تروا انجام می‌دهد، بدسـت آورم. بنابرایـن Windows 2000 را داخـل VMWare بـالا آورده و فـایل tk1.exe را که از طریق سرور Ftp بدست آورده‌ام را بارگذاری می‌کنم. نفس عمیقی کشیده، برنامه‌های ضبط Screen و نظارت بر فایل را آماده کرده و بر روی فایل اسب تروا دوبار کلیک می‌کنم. در ابتدا یک خروج موقت در Windows (شـکل ۵) رخ داده و سـپس صفحه به حالت طبیعی بازمی‌گردد. یک NetStat سریع و بررسی Task List نشان می‌دهد که من در حال حاضر یکی از قربانیان کرم THR34t Krew's IRC می‌باشم.



شکل ۵

نمایش صفحه از نصب فایل TK1.exe

بعد از بررسی سیستم برای پی بردن به تغییرات، متوجه شدم که با یکبار اجرای فایل، فایل مزبور به ۳۰ فایل تبدیل شده و برنامه‌ها، تنظیمات و سرویس‌هایی که با کامپیوتر شروع به کار می‌کنند را در بر گرفته است. این سرویس‌ها یک برنامه mIRC تنظیم شده، یک سرور Ftp و یک اسکریپت پیچیده IRC را شامل می‌شوند. هنگامی که من فایل‌ها را کمی دقیق‌تر در برنامه NotePad بررسی کردم، متوجه شدم که بسیاری از فایل بصورت متن ساده و آشکار نوشته شده‌اند. خوشبختانه در داخل متن‌ها بسرعت چندین کلمه رمز را تشخیص دادم.

مرحله بعدی کارم تست کردن کلمات عبور بود، بنابراین به سرور چت بازگشتم. با خوش‌شانسی، یکی از کمات رمز (خصوصی) کار کرد و من توانستم به اتاق چت وارد شوم. هنگامی که وارد شدم، فورا اسم مستعار خود را تغییر دادم تا شبیه اسمهای دیگر که بر اساس الگوریتم ساخته شده بودند باشد (مانند TK^8376 و TK-=-887). سپس شروع به بررسی اتاق چت و محتویات آن نمودم تا ذره‌ای اطلاعات بدست بیاورم.

پس از چندین دقیقه، متوجه شدم که تلاش‌هایم بیهوده است. با آنکه می‌توانستم سایر handle ها را برای بدست آوردن اطلاعات مورد کنکاش قرار دهم و حتی می‌توانستم آدرس IP آنها را

بـه کمـک اسکن پورت Subnet آنها بر روی پورت 1297 (پورت اسب تروا) به دست آورم، اما قادر به دریافت هیچ پاسخی از اتاق نبودم. گام بعدی بازگشت به سیستم ویندوز ۲۰۰۰ آلوده‌ام برای بررسی فایلهای بیشتری بود .

با فایلی که اسکریپت IRC را دربرگرفته بود و به تصور من bot های IRC را کنترل می‌کرد، شـروع کـردم. اسـکریپت را اسکن کرده و به این نتیجه رسیدم که اسکریپت و یک سرور تقویت‌کننده IRC کـه بـر روی پـورت 1297 باز شده است، متهم اصلی IRC bot می‌باشند. برای اثبات این نظر، بررسـی اسکریپت را با دستوری شروع کردم که می‌توانستم از آن برای تست سایر Tkbot هایی که در اتاق چت محرمانه با من بودند، استفاده کنم. در کمال دلسردی خط زیر را در دستورات پیدا کردم.

```
if ($level($address($nick,9)) != 100) { halt }
```

بـه عـبارت دیگـر تـا زمانـی کـه من اپراتوری از سرور بودم، از قدرت فرمان دادن به bot ها بـرخوردار نـبودم. گـرچه ایـن کمـی بدشانسی برای من بود، اما باید می‌پذیرفتم که این کار تصمیمی عاقلانـه از جانـب نویسـنده اسـکریپت بـوده اسـت. منظورم این است که در نبود چنین دستوری در صورتی که من صاحب ۱۰۰۰ کامپیوتر بودم، می‌توانستم انواع بسیار زیادی از مشکلات را فراهم کنم.

بـا همـه ایـن احـوال، در ادامـه تصـمیم گرفتم تا قدرت اسکریپت را در یک محیط کنترل شده بررسی کنم. برای انجام این کار، اسکریپت را در mIRC بالا آورده، تمام محدودیت‌ها را ویرایش کرده و دسـتورات خـود را جایگزیـن آنهـا کـردم. هنگامی که اسکریپت را اجرا کردم به سرور IRC دیگری متصل شده و اتاق چت شخصی خود را بوجود آوردم.

بعد از چندین دقیقه اشکال زدایی اسکریپت من ایجاد شده بود.

در طـی ایـن کنکاش متوجه شدم که سازنده اسکریپت این اسب تروا، کاری بسیار عالی برای تولید عمده یک برنامه بسیار قدرتمند کنترل از راه دور انجام داده است. با استفاده از دستورات ساده یـک تا چهار حرفی، یک شخص قادر شده است که یک کامپیوتر را برای بدست آوردن اطلاعات آماری، Upload و Download کـردن فـایل‌هـا، اجـرای بـرنامه‌هـا بر روی سرورهای در حال کنترل و حتی فـرمان‌دهـی بـه سـرور برای جستجوی اینترنت جهت پیدا کردن سایر کامپیوترهای آسیب‌پذیر مورد کاوش قرار دهد.

آنچه در ادامه می‌آید دستور و نام مستعاری است که سرعت تخمینی شبکه‌ای را که سرور در آن می‌باشد، بدست می‌آورد:

```
if ($1 == !netspeed) { netspeed }

alias netspeed {
set %nsp $nc
write -c netst.bat netstat -e >stt.tx
run netst.bat
.timer -m 1 9950 once}
```

اولیـن خـط شـامل فیلـتری است که متن وارد شده توسط اپراتور کانال را ضبط می‌کند. اگر اپـراتور کلمه netspeed! را تایپ کند، این خط کد داخل alias netspeed را اجرا می‌کند. این کد شامل کدهایی است که NetStat را اجرا کرده و نتایج را در یک فایل انباشته می‌کنند، سپس فایل را به اتاق چت IRC بازمی‌گردانند.

لیست کارهایی که این دستورات انجام می‌دهند در ادامه آمده است:

- اجرای سیل UDP
- اجرای فایل
- جمع‌آوری اطلاعات آماری Hard Drive
- اجرای یک حمله سیل آسا به Web Site
- ایجاد Server lag
- اجرای دستورات IRC
- نابود کردن سرور
- اجرای یک پرس و جوی پورت باز
- کنترل کردن BNC (اسب تروای نصب شده بر پورت 1297)
- اجرای پویش کامپیوترهای آسیب پذیر
- اجرای دستورات Download و Upload

Th34t : روز سوم، شب

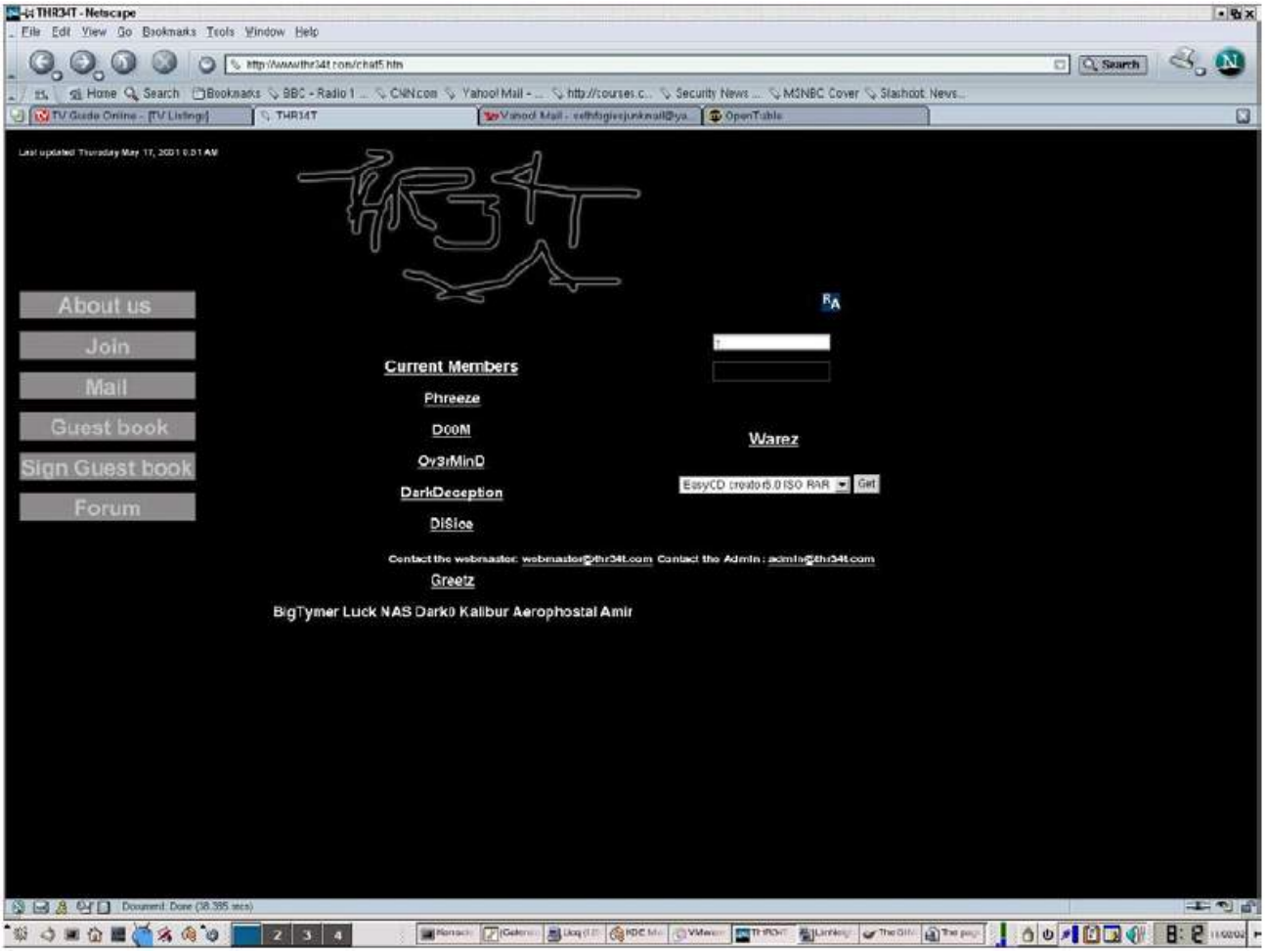
بـیان قـدرت ایـن اسـکریپت IRC فراتـر از هدف و منظور این مقاله می‌باشد. در صورتی که خوانـنده‌هـا بـه مطلب قدرت اسکریپت‌نویسی IRC علاقمند هستند، لطفا آنرا بیان کنند و من احتمالا مقاله‌ای مربوط به آن موضوع تهیه خواهم کرد.

در طـی زمانـی کـه مـن قـدرت اسـکریپت TK را بررسـی و امـتحان می‌کردم، هنوز در کانال #tkworld باقـی بـودم. قصـدم بطور ساده ثبت کردن هرگونه فعالیتی و افرادی که داخل یا وارد آن می‌شوند، بود. در طی زمانی که من متصل بودم، متوجه شدم که بعد از چندین ساعت تعداد Tkbot ها رو بـه کـاهش گذاشـته اسـت. در بین قطع‌ارتباط شده‌ها متوجه فردی با نام DiCise شدم که ارتباط ایجـاد کرده و سپس ارتباط را قطع کرده بود. نکته جالب در مورد این فرد آن بود که در برنامه IRC خود، پیام قطع ارتباط خود را بگونه‌ای تنظیم کرده بود که پیام زیر فرستاده شده بود:

"Can j00 f33l tha THR34T? I g0t th3 p0w3r 0f r3wt"

اولیـن چـیزی کـه در پـیام توجـه من را جلب کرد کلمه بسیار مانوس THR34T بود. همانند ضربه‌ای در تاریکی، سریعا سایت www.google.com را باز کرده و جستجویی را در مورد این کلمه

غـیر مـتعارف انجـام دادم. بعـد از بررسی نتایج بر روی یکی از لینک‌های امیدبخش کلیک کرده و با صفحه زیر روبرو شدم (شکل ۶).



شکل ۶

صفحه وب THR34T security crew's (درحال حاضر دیگر Online نیست)

در اینجا بود که با دیدن سایت، بر اثر خنده شدید از صندلی به زمین افتادم! هیچ چیزی برای انطباق با آنچه مورد نظرم بود وجود نداشت و من کاملا مطمئن بودم که سایت THR34T security crew اطلاعات زیادی در مورد اسب تروای IRC ندارد. احتمالا مذاکره با DOOM که قبلا عنوان شد، بـرنامه IRC کـه او اسـتفاده می‌کرد و پیام good-bye از جانب DiCise کافی نبوده‌اند و من متوجه شدم که باید فایلهای نصب سرور TK Disto Ftp را بدقت بررسی کنم تا شاید شناسه ورودی با نام DOOM وجود داشته باشد. به نظر شما در چه موردی، بدیهیات را ندیده گرفته‌ایم؟

خلاصه

در ایـن مـرحله، تحقـیق و بررسـی دیگـر بـرای مـن تمـام شـده بود. من تمام چیزهایی را که مـی‌خواسـتم پـیدا کنم پیدا کرده بودم. WHOIS چیز با ارزشی برای من بدست نیاورد، log فایلهای سـرور را در اختـیار نداشـتم و THR34T ناپدید شده بود. در هنگامی که به نظر می‌رسید گسترش اسـب تروای از نوع IRC bot هکر مورد نظر، همه جا را در بر بگیرد، این اسب متوقف شد. در آخرین بازدید از سرور هک شده IRC (۲۵ نوامبر ۲۰۰۲)، #tkworld هنوز چند نفر مقیم در خود داشت.

در نهایـت از سرور هک شده ما می‌توان درس بزرگی را آموخت مبنی بر اینکه در صورت عدم نگهـداری صحیح یک کامپیوتر اتفاقات ناخوشایند بسیاری برای آن رخ خواهد داد. مشکل چه ویروس باشد، چه کرم، اسب تروا و یا حتی همه آنها، لازم است که از دارائیتان به شدت مراقبت کنید. وقتی که یکـی از کارهای عمده سروری، تهیه منبع بزرگی از سرگرمی‌ها باشد، باید به مدیر آن سرور در مورد تفکری که درباره امنیت نامه‌های الکترونیکی، داده‌های تجاری و اینگونه موارد دارد، شک کرد.

بـا آنکـه مـن نمـی‌توانم از نقش عملی THR34T در خلق و توزیع این کرم مطمئن باشم، اما بـنظر می‌رسد که آنها چیزهایی درباره آن می‌دانند. متاسفانه تمام ایمیل‌ها به DOOM پس فرستاده شد و وب سایت آنها هم دیگر وجود ندارد، بنابراین فکر می‌کنم که من دیگر درباره آن چیزی ندانم.

در هنگامـی کـه ایـن مقالـه را برای تحویل بازبینی می‌کردم، تصمیم گرفتم تا دوباره یک نگاه زیرچشـمی بـه سرور هک شده IRC داشته باشم. با تعجب دیدم که سایت در جریان می‌باشد. صدها کامپـیوتر شخصـی در آن وارد شده بودند و تعدادی هم دقایقی دیگر وارد می‌شدند. مقداری در سایت درنگ کردم و متوجه شدم که چند شخص حقیقی با من در سرور هستند. بعد از انجام چندین مکالمه و در حالـیکه بـا اطلاعـات بسـیار کـم و نادرستی تغذیه می‌شدم و در نهایت هم با یک حمله DDoS در حـدود ۱۰ سـاعت Offline بـودم، بالاخـره دل یکـی از اعضاء Krew Thr34t به حال من سوخت و مکالمه‌ای خوب با من انجام داد. او همه چیز را درباره Krew، درجه امنیتی که برای حفظ گمنامی خود انجـام داده بودنـد و همچنین درباره قدرت و وسعت شبکه‌شان به من گفت. او همچنین به من گفت که آنها می‌خواستند سرور IRC را به خاطر کاوش‌های من پاک کرده و به سرور دیگری نقل مکان کنند.

به طور خلاصه این شخص ۱۶ ساله و سایر ۱۰ عضو Krew (متعلق به او) اسب تروا / کرمی ساخته بودند که قدرت و وسعتی بسیار بیشتر از بعضی دولت‌ها دارد.

به آینده خوش آمدید، جایی که مالکیت موضوع چشم‌اندازها خواهد بود و قدرت با تعداد کامپیوترها و وسعتی که در کنترل خود دارید، مشخص خواهد شد.

متشکر به خاطر اینکه بالاخره حمله DDoS را متوقف کردید!