بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

به‌روزرسانی ماژول انتشار جدید "Nworm" توسط هکرهای توسعه‌دهنده TrickBot

اخبار بروزرسانی

هکرهای توسعه‌دهنده بدافزار TrickBot، ماژول انتشار جدید خود را تحت عنوان "Nworm"، به‌روزرسانی کردند. عموم مردم با بدافزار TrickBot آشنایی دارند، اما این بار این بدافزار با ماژول انتشار جدیدی ظاهر می‌شود.

شاید فکر کنید این ماژول انتشار چه تفاوتی دارد؟ این ماژول، یک ماژول انتشار است که بطور کلی برای سرقت اطلاعات حساس که به دسترسی به درب‌پشتی کمک می‌کند، استفاده می‌شد که بعدا توسط چند گروه غیرقانونی برای انتشار بدافزارهای مختلف مورد استفاده قرار گرفت.

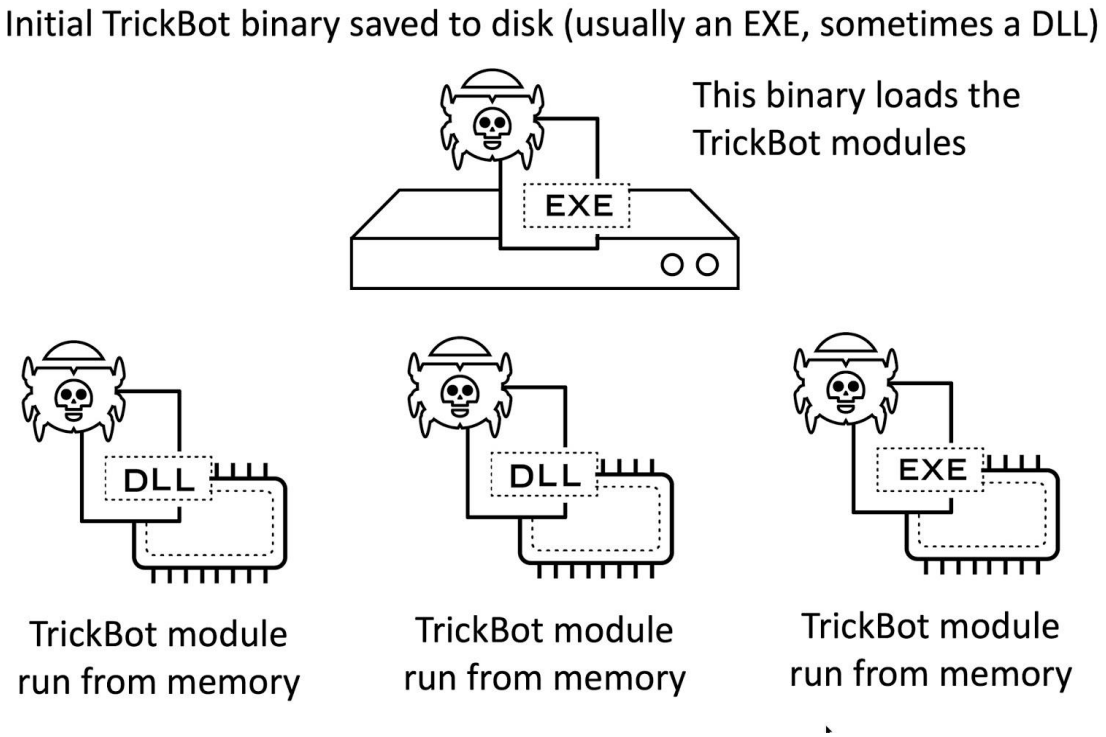
GBHackers چند فعالیت TrickBot را گزارش کرده‌است که ابتدا در سال ۲۰۱۶ دیده شدند و بطور معمول با دسترسی پیدا کردن به مواردی که اخیرا توسط کاربر در پس‌زمینه اجرا شده‌اند، شروع می‌شود.

زمانی که راهی برای ورود به رایانه بیابد، به تدریج ماژول‌های مختلفی را برای اجرای امور مخرب ابتدا در رایانه و سپس در شبکه، بارگیری می‌کند.

۱ ماژول‌های TrickBot و ماژول‌های مورد استفاده برای گسترش

این ماژول یک ماژول انتشار است که به‌شکل ویژه با هدف سرقت داده‌های حساس با اجرای اعمال مخرب خود، توسعه یافت. TrickBot با سایر بدافزارها متفاوت است، زیرا این بدافزار در طول عمل خود از فایل‌های باینری مختلف برای اجرای امور مخرب متفاوتی استفاده می‌کند.

TrickBot ابتدا فایل‌های اجرایی ویندوز(EXE) مخرب را بر روی دیسک ذخیره می‌کند که این مرحله به‌عنوان "TrickBot Loader" شناخته می‌شود. برای درک بهتر، در ادامه مثال‌هایی از ویندوز۱۰ و ویندوز۷ آورده شده‌است.



اگر ویندوز۱۰ آلوده شود، ماژول‌های TrickBot را فقط در حافظه می‌توان پیدا کرد. درحالیکه اگر ویندوز۷ آلوده شود، علاوه‌بر مورد گفته‌شده برای ویندوز ۱۰، کاربران می‌توانند محصولاتی را ببینند که به ماژول‌ها مرتبط‌اند و در دیسک ذخیره شده‌اند.

اخیرا گردانندگان TrickBot و باج‌افزارهای دیگر به‌هم ملحق شده‌اند تا با دسترسی پیدا کردن به شبکه‌ای توافق شده، به‌سادگی از این باج‌افزار استفاده کنند.

پالو آلتو،محقق حوزه امنیت، بیان‌کرد "شواهدی که در ویندوز۷ نشان داده می‌شوند، فایل‌های باینری رمزگذاری شده هستند که بعدا در طول عملیات، رمزگشایی می‌شوند و در حافظه‌ی سیستم به عنوان ماژول‌های TrickBot اجرا می‌شوند"

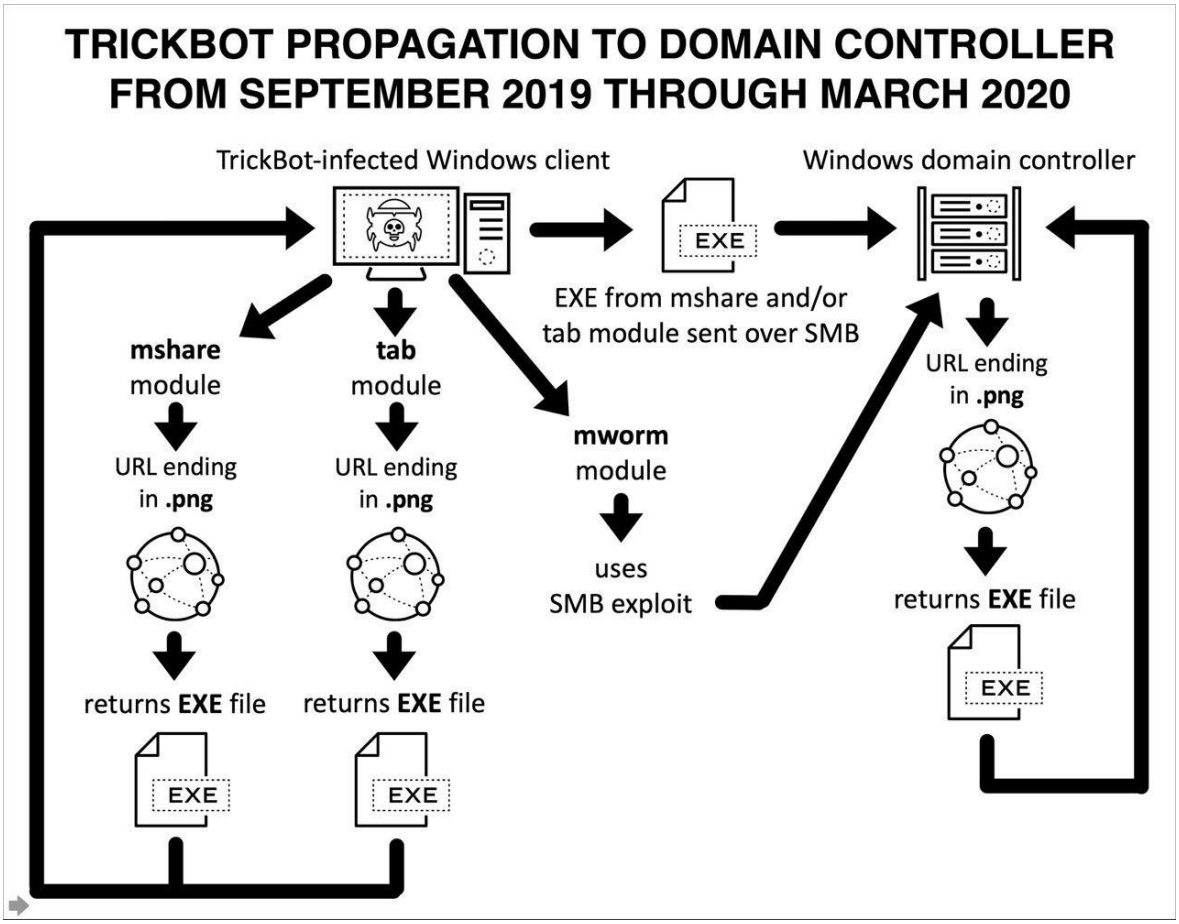
ماژول‌های مورداستفاده‌ی TrickBot:

- ماژول Mshare

- ماژول Tab

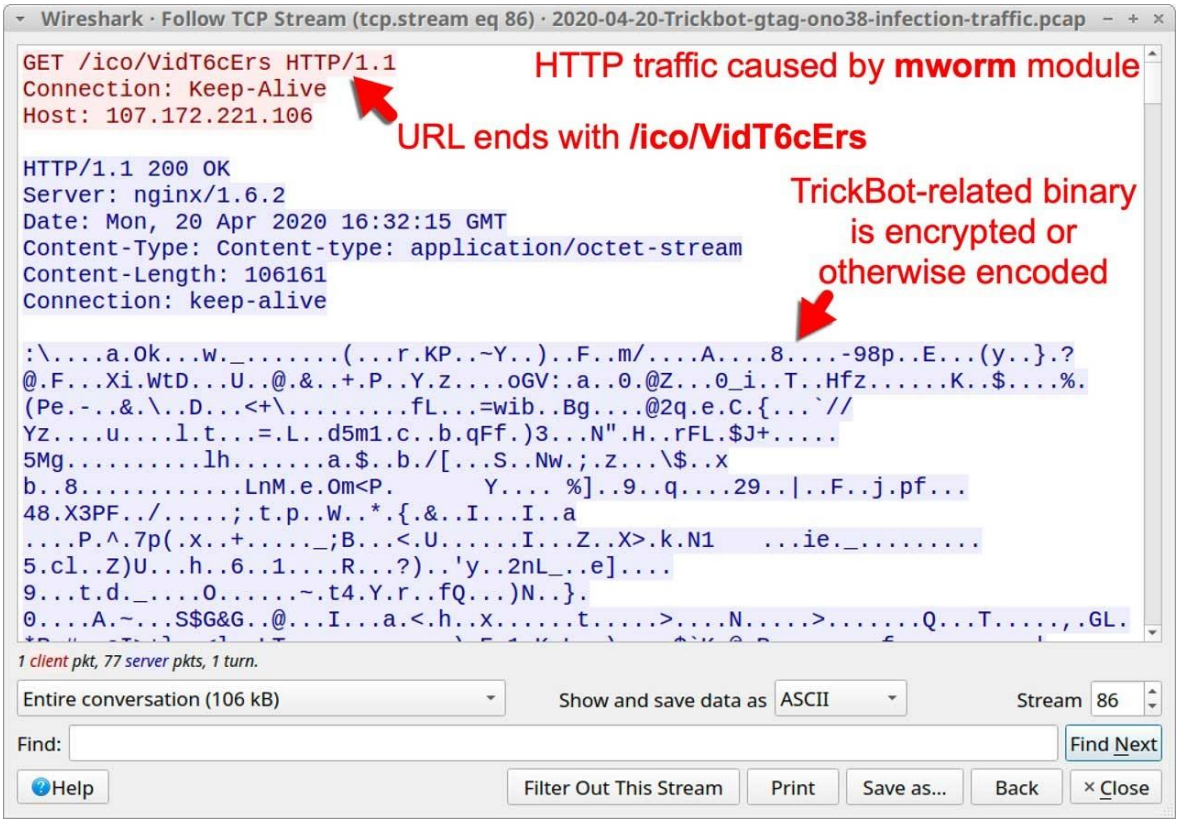
ماژول Mworm

این ماژول برای بهره‌برداری از آسیب‌پذیری SMB در کنترل‌کننده‌ی دامنه استفاده می‌شود. نمودار موردنظر ما در زیر ذکر شده است که در آن می‌توان جریان پخش ناشی از ماژول‌های TrickBot فوق را مشاهده کرد.



۲ خداحافظ "Mworm"، سلام "Nworm"

ماژول Nworm جدید، با هدف مبهم‌سازی، پیچیده‌سازی و غیرقابل تشخیص شدن، حافظه‌ی کنترل‌کننده‌ی دامنه را آلوده می‌کند تا بتواند به‌راحتی اجرا شود.



می‌دانیم TrickBot ماژول انتشار جدید "Nworm" را درحالی معرفی کرده‌است که در اوایل سال ۲۰۲۰ استفاده از ماژول "Mworm" را در یکی از محیط‌های آزمایشگاهی متوقف کرد. هنگامی که TrickBot استفاده از Mworm را متوقف کرد، گردانندگان آن محصول جدیدی را به نام "Nworm" معرفی کردند که در ابتدا در یکی از سیستم‌ها با ویندوز۷ آلوده ظاهر شد.

منبع:

https://gbhackers.com/nwrom/