چگونه یک بدافزار غیر قابل شناسایی تولید کنیم

روشی عملی برای نوشتن بدافزار در ویندوز

مقدمه

در دنیای امنیت کامپیوتر هر روز روشهای نوینی برای تولید بدافزار توسط Red Team (تیم های مخرب) ابداع و در عرصه های مختلف از شعله ور نمودن یک جنگ سایبری با حملات APT گرفته تا به سرقت بردن اطلاعات اشخاص و یا شاید یک کینه شخصی!

شناخت روشهای تولید بدافزار و دقت در نحوه فعالیت این برنامه های مخرب به تیم های امنیت سایبری (Blue Team) کمک می کند تا در شناسایی گونه های جدیدتر و تکنیک های به کار گرفته شده توسط تولید کننده گان بد افزار آشنایی بیشتر پیدا کنند و بتوانند در خنثی کردن این تهدیدات و یا اطلاع رسانی سریع به خوبی عمل نمایند.

در این مقاله با توجه به اهمیت بی بدیل بحث امنیت در عرصه علوم کامپیوتر برآن شدیم تا شمارا با روشهای تولید یک بدافزار مخرب آشنا نماییم.این مقاله ضمنا" برای متخصصین امنیت در تیم های ضد بدافزار و آنتی ویروس بسیار مفید می باشد. زیرا توانایی شناخت آنها از تهدیدات را افزایش می دهد.

بدافزار نوشته شده در این مقاله طی تست های صورت گرفته در چند آنتی ویروس و سیستم آنتی ویروس ویندوز 10 (جدید ترین آپدیت) غیر قابل شناسایی بوده است.توصیه ما این است برای تست این بدافزار از محیط سندباکس(ویندوز10) و یا یک ماشین مجازی استفاده نمایید تا از آسیب احتمالی در امان باشید.هرچند بخشی از کد که مربوط به تکثیر در شبکه می باشد از کد حذف شده است.ممکن است این بدافزار c&c منجبر به مخاطراتی در سیستم شما یا شبکه ای که در آن فعالیت می نمایید شود.

با تشکر

شروع ماجرا

برای یک متخصص امنیت Read Team دستیابی به روشی برای تولید بدافزار غیرقابل شناسایی توسط آنتی ویروس های مرسوم بسیار وسوسه کننده و فوق العاده است.پیش از این تیم های مخرب با استفاده از ابزار هایی مثل متااسپلویت Veil-Evasion و ابزار تزریق در پروسس ها مثل LoardPE سعی در مخفی نگه داشتن بدافزار خود می کردند که گاها در این مسیر با شکست مواجه می شدند.دلیل عمده این شکست هم این بود که تیم های تحقیق ضد بدافزار و آنتی ویروس هم بیکار ننشسته اند و هر لحظه در حال توسعه مکانیزم خود برای مقابله با بدافزارها می باشند.

دیگر دلیل استفاده نکردن از متااسپلویت هم این بود که ابزارهای متااسپلویت فقط کنترل یک سیستم را میسر می سازند.اما روش توسعه صفر تا صد ما این امکان را به ما میدهد که به هر تعداد سیستم آسیب پذیر دسترسی داشته باشیم.و این مفهومی با نام BotNet را برای مخاطب تداعی خواهد کرد.

بدافزار انتهایی ما یک پنل کنترل بدافزار مانند آنچه در شکل زیر مشاهده می کنید خواهد داشت:

برای نوشتن بدافزار ابتدا باید شما با مکانیزم عملکرد ویندوز آشنا شوید.به عنوان مثال باید بدانید که مثلا یک بازی چگونه عمل می کند.یک بازی را تصور کنید.وقتی کلیدهای جهت و یا هر کلید روی صفحه کلید را فشار میدهید بازی یک عمل خاص انجام می دهد.حالا تصور کنید این کلید های فشرده شده در بازی keystrokes به جای ارسال به بازی از حافظه جمع آوری و داخل یک فایل متنی ذخیره شوند.این یعنی ما توانسته ایم یک keylogger بنویسیم!

تا تمامی کلید های فشرده شده توسط کاربر را برای ما به صورت مخفیانه و در پس زمینه ویندوز ذخیره نماید.

قبل از آغاز توسعه این بدافزار سوالاتی هست که شما باید پاسخ دهید:

الف ) شما میخواهید چه نوع بدافزاری توسعه دهید؟

1. بدافزاری که خودش در شبکه توزیع شود ؟ مثل worm ها؟
2. یک تروجان؟
3. بدافزاری که برخی از فعالیت هایی که شما دوست دارید را در سیستم قربانی به صورت اتوماتیک انجام دهد ؟
4. یک ابزار مخفی از راه دور که فرمانهای شمارا در سیستم قربانی اجرا کند ؟

ب) چه پرتکلی را برای توسعه و ارتباط با بدافزرا مدنظر دارید؟

ج) چه زبانی را برای توشتن بدافزار مناسب می دانید ؟

انتخاب زبان توسعه بدافزار :

در جدول زیر شما برخی از زبانهارا که برای توسعه بدافزار مناسب می باشند می بینید.دراین جدول به معایب و مزایای هر یک اشاره شده است.

با توجه به جدول زیر و اینکه قصد ما از تولید بدافزار پیمودن راههای سخت و طاقت فرسایی مثل نوشتن بدافزار به زبان اسمبلی نیست.ما زبانهای C/C++ و Python3 را انتخاب می کنیم. توصیه می شود برای نوشتن بدافزار از زبانهایی مثل روبی و پایتون استفاده نشود زیرا هم حجم بدافزار افزایش چشم گیری می باید.و هم اینکه برای اجرای آن نیاز به نصب مفسر این زبانها وجود خواهد داشت که در بیشتر مواقع غیرقابل انجام است.



به چه ابزاری نیاز داریم؟

C/C++

1. پوینتر ها : برای ذخیر داده هادر حافظه سیستم سمت قربانی
2. TCP Socket برای دسترسی معکوس(یعنی برقراری ارتباط از سمت سیستم قربانی به سیستم ما که از آن طریق فرمان ما را بر روی سیستم قربانی اجرا نماید.)
3. دستکاری بافرها و هیپ جهت خواندن فایلهای با حجم بالا بر روی هارد دیسک

Python3

1. استفاده از Multi thread ,multi port برای استفاده از چندین bot (قربانی) به صورت همزمان
2. هندل کردن نوع داده ها
3. TCP Socket
4. Event Signal Handling

WIN API : برنامه نویسی سوکت در ویندوز

Mingw-g++ : جهت کم کردن سایز فایل بدافزار

Elastic Search + Kibana : جهت پیاده سازی مکانیزم سرچ و شبیه سازی در بات نت ها و سیستم های قربانی

نیازهای دیگر:

Visual Code: محیط برنامه نویسی مناسب برای c++ و python

ماشین مجازی :جهت اجرا کد تست

سیستم عامل لینوکس برای اجرای اسکریپت پایتون(درویندوز هم امکان پذیر است)

* در صورتی که در لینوکس کد میزنید برای کامپایل کدهای ویندوز در لینوکس پکیج زیر را نصب نمایید:
* **$ apt-get install mingw-w64-common mingw-w64-i686-dev mingw-w64-tools mingw-w64-x86-64-dev**

حالا باید موارد زیر را در بدافزار پیاده سازی کرد.

1. مکانیزم شناخت یوزر whoami
2. مکانیزم شناسایی دایرکتوری جاری pwd
3. قابلیت عملیات روی فایل / فولدر ها
4. دانلود و آپلود فایل
5. قابلیت اجرای دستورات روی کامند ویندوز از راه دور
6. ارسال دستور به چندین Bot
7. مخفی کردن باینری در زمان اجرا