آموزش CEH (هکر کلاه سفید): تروجان‌ها و ویروس‌ها چه کارهای مخربی انجام می‌دهند

اولین کرم شناخته شده‌ای که در اینترنت منتشر شد کرم RTM 1988 بود. این کرم توسط رابرت تی. موریس جونیور توسعه داده شد و تنها یک مدل اثبات مفهومی بود. این کرم سعی می‌کرد گذرواژه‌های ضعیف و آسیب‌پذیری‌های مستتر در برخی سرویس‌های خاص را مورد بهره‌برداری قرار دهد. این برنامه کوچک تقریباً 6000 رایانه متصل به اینترنت را آلوده کرد. انتشار تصادفی این کرم باعث شکل‌گیری این فرضیه شد که کرم‌ها می‌توانند آسیب بزرگی به اینترنت وارد کنند. هزینه خسارت ناشی از آلوده‌سازی توسط کرم‌ها چیزی در حدود 10 تا 100 میلیون دلار تخمین زده شده است. رابرت موریس به جرم نقض قانون کلاهبرداری رایانه و سوءاستفاده به 3 سال حبس مشروط، 400 ساعت خدمات اجتماعی و جریمه 105050 دلاری محکوم شد. ویروس‌ها در دنیای کامپیوترها به روش‌های مختلفی پخش می‌شوند. در ادامه به چند مورد از ویروس‌ها و نحوه انتشار آن‌ها اشاره‌ای خواهیم داشت.

برای مطالعه قسمت قبل آموزش رایگان **دوره CEH I**اینجا کلیک کنید.

از دهه 1980 میلادی به بعد یک سری ویروس‌ها و کرم‌های شناخته شده توسط هکرها تولید شدند. ویروس‌ها به دلایل مختلف نوشته می‌شوند که از آن جمله می‌توان به حذف رقبای سیاسی، بهره‌برداری از آسیب‌پذیری‌های فنی، به‌دست آوردن شهرت، انتقام‌جویی، سرقت اطلاعات یا اخاذی اشاره کرد. درست است که برخی از ویروس‌نویسان شناسایی نمی‌شوند، اما آن‌هایی که به چنگال قانون گرفتار می‌شوند به تحمل حبس و جزای نقدی محکوم می‌شوند. بیشتر ویروس‌نویسان ترجیح می‌دهند تا جایی که امکان دارد ناشناس بمانند. با این حال، آن‌ها معمولاً نام‌های مستعاری برای خود و بدافزارهایشان انتخاب می‌کنند، هرچند شرکت‌های سازنده ضدویروس نام دیگری برای بدافزارها انتخاب می‌کنند و بر مبنای پروتکل‌های خاص اقدام به نام‌گذاری کدهای مخرب می‌کنند. اگرچه این یک فرآیند تصادفی نیست، اما در برخی موارد تاثیرات مخرب باعث نام‌گذاری ویروس‌ها می‌شود.

اولین کرم شناخته شده‌ای که در اینترنت منتشر شد کرم RTM 1988 بود. این کرم توسط رابرت تی. موریس جونیور توسعه داده شد و تنها یک مدل اثبات مفهومی بود. این کرم سعی می‌کرد گذرواژه‌های ضعیف و آسیب‌پذیری‌های مستتر در برخی سرویس‌های خاص را مورد بهره‌برداری قرار دهد. این برنامه کوچک تقریباً 6000 رایانه متصل به اینترنت را آلوده کرد. انتشار تصادفی این کرم باعث شکل‌گیری این فرضیه شد که کرم‌ها می‌توانند آسیب بزرگی به اینترنت وارد کنند. هزینه خسارت ناشی از آلوده‌سازی توسط کرم‌ها چیزی در حدود 10 تا 100 میلیون دلار تخمین زده شده است. رابرت موریس به جرم نقض قانون کلاهبرداری رایانه و سوءاستفاده به 3 سال حبس مشروط، 400 ساعت خدمات اجتماعی و جریمه 105050 دلاری محکوم شد. ویروس‌ها در دنیای کامپیوترها به روش‌های مختلفی پخش می‌شوند. در ادامه به چند مورد از ویروس‌ها و نحوه انتشار آن‌ها اشاره‌ای خواهیم داشت.

■ ملیسا: در اواخر دهه 1990 شایعاتی مبنی بر انتشار شکل جدیدی از ویروس‌ها که به‌نام ویروس ماکرو معروف بودند منتشر شد. کمی بعدتر در سال 1999 شرکت‌های امنیتی خبر از انتشار گسترده ویروسی دادند که ملیسا نام گرفت و تمامی ویژگی‌ها یک کرم ویروسی را داشت. مقامات مربوطه موفق شدند خالق ویروس ملیسا که دیوید اسمیت نام داشت را شناسایی کرده و به جرم انتشار این ویروس به 5 سال زندان محکوم کنند.

Code Red: کرم کد قرمز در سال 2001 ظاهر شد. کد قرمز در زمان شیوع موفق شد به ده‌ها هزار سامانه‌ای که سیستم‌عامل‌های ویندوز NT و ویندوز سرور 2000 روی آن‌ها اجرا می‌شد نفوذ کند. کرم کد قرمز از آسیب‌پذیری سرریز بافر .ida برای نفوذ به سامانه‌ها استفاده می‌کرد. کد قرمز از یک رویکرد حمله منحصر به فرد استفاده می‌کرد و پس از آلوده‌سازی سایر کامپیوترهای هدف می‌رفت.

■ Nimda: در پی حوادث یازده سپتامبر 2001 ، هزاران رایانه در سراسر جهان مورد حمله کرم نیما قرار گرفتند. کرم نیمدا در آن زمان با استفاده از روش‌های منحصر به فردی برای آلوده‌سازی سامانه‌ها استفاده می‌کرد. کرم Nimda وب‌سرورهای وب IIS ویندوز را با بهره‌برداری از اکسپلویت Unicode Web Traversal هدف قرار می‌داد. Nimda از سرویس‌گیرنده ایمیل داخلی خود استفاده می‌کرد. به همین دلیل تشخیص این موضوع که چه کسی ایمیل آلوده را ارسال کرده به سختی امکان‌پذیر می‌شد. Nimda همچنین می‌توانست خود را به فایل‌های اجرایی اضافه کند تا کاربران بیشتری را قربانی کند. نیمدا برای شناسایی سایر سامانه‌ها یک فرآیند پویش آسیب‌پذیری‌ها را به کار می‌گرفت.

■ Slammer: کرم Slammer در سال 2003 شناسایی شد. این کرم موفق شد در کمتر از 3 ساعت صدها هزار رایانه را آلوده کند و به این ترتیب تا پیش از انتشار کرم MyDoom در سال 2004 لقب سریع‌ترین میزان شیوع و آلودگی را از آن خود کند.

■ MyDoom: کرم MyDoom با تلاش برای فریب افراد به منظور باز کردن پیوست‌های آلوده حاوی کرم کاربران مختلف را قربانی می‌کرد. عملکرد کرم فوق به این‌گونه بود که برای قربانی اعلانی ارسال می‌کرد که ارسال ایمیل با موفقیت همراه نبوده و برای مشاهده متن اصلی فایل ضمیمه را باز کند. کرم MyDoom اولین نوع در گونه خود بود که مانع اجرای به‌روزرسانی ویندوز می‌شد.

■ Sasser: کرم Sasser نیز در سال 2004 منتشر شد. کرم Sasser مشکلات امنیتی درون سرویس Local Security Authority Subsystem و lsass.exe را هدف قرار می‌داد. یک جوان 18 ساله به‌نام Sven Jaschan به دلیل ساخت کرم Sasser و ویروس Netsky به 1 سال و 9 ماه حبس مشروط و 30 ساعت خدمت اجتماعی محکوم شد.

■ Storm: کرم storm یک گونه ترکیبی از کرم‌ها و روبات‌ها بود که در حدود سال 2007 شناسایی شد. این کرم ترکیبی قادر به انجام کارهای مختلفی همچون ارسال هرزنامه، جمع‌آوری رمز عبور و سرقت شماره کارت‌های اعتباری بود.

Conficker: Conficker کرم رایانه‌ای دیگری بود که سیستم‌عامل ویندوز مایکروسافت را هدف قرار داد. این کرم اولین بار در نوامبر 2008 کشف شد. Conficker نقص‌های درون سیستم‌عامل ویندوز را برای حمله به سامانه‌های قربانیان به کار می‌گرفت.

■ Ransomware: طی چند سال گذشته، تهدیدات مختلفی گریبان‌گیر سازمان‌ها و کاربران شده است، اما در تمامی موارد ویروس‌ها یا کرم‌های واقعی به کار گرفته نشده‌اند. باج‌افزارها گونه خطرناک دیگری از تکنیک‌های به کار گرفته شده توسط هکرها هستند. باج‌افزارها می‌توانند مانند کرم یا ویروس پخش شده و فایل‌های شخصی روی هارددیسک‌ها را رمزنگاری کنند. این‌کار با هدف دریافت باج از کاربران انجام می‌شود. باج‌افزارها سالیان متمادی است که در فضای سایبری وجود دارند، اما از سال 2012 با شدت بیشتری نسبت به گذشته ظاهر شده‌اند. از مهم‌ترین باج‌افزارها می‌توان به CryptoWall ، CryptoDefense، CryptoLocker ، CryptorBit و Spora اشاره کرد.

حتی اگر نویسندگان ویروس‌ها بتوانند از چنگال قانون فرار کنند، بازهم ویروس‌نویسی یک حرفه سودآور نیست.

ابزارهای ویروسی

سازندگان ویروس تفاوت‌هایی با یکدیگر دارند. در گذشته ویروس‌ها عمدتا توسط دانش‌آموزانی ایجاد می‌شد که تازه مبحث برنامه‌نویسی را یاد گرفته بودند و می‌خواستند توانایی‌های خود را محک بزنند. برخی از ویروس‌نویسان با هدف جلب توجه این‌کار را انجام می‌دهند و برخی دیگر مشتاق هستند تا مهارت‌ها خود را به دیگران نشان دهند. در حالی که سایر ویروس‌نویسان مجرب‌تر با هدف سودآوری اقدام به ساخت ویروس‌های حرفه‌ای می‌کنند. این افراد برای امرار معاش اقدام به انجام این‌کار می‌کنند. ویروس‌هایی که توسط هکرهای مجرب نوشته می‌شود، عمدتا دقیق و روان هستند و بدون مشکل خاصی روی سیستم قربانی اجرا می‌شوند. به همین دلیل این افراد در زمینه برنامه‌نویسی سطح بالایی از مهارت‌ها را در اختیار دارند. ویروس‌های کامپیوتری هیچ تفاوتی با برنامه‌های عادی ندارد. توسعه‌دهنده باید از یک زبان برنامه‌نویسی همچون سی، ویژوال بیسیک، اسمبلی، یک زبان ماکرو یا سایر زبان‌ها برای ساخت ویروس استفاده کند. البته بدون داشتن مهارت برنامه‌نویسی نیز امکان ساخت ویروس‌ها وجود دارد، اما برای این منظور به ابزارهایی نیاز است. نویسندگان ویروس می‌توانند با ایجاد تغییراتی در کدهای مخرب، گونه جدیدی از یک ویروس را تولید کنند. شکل زیر مثالی در این زمینه را نشان می‌دهد.

ابزارهای مختلفی برای ساخت ویروس‌ها و کدهای مخرب وجو دارد که از آن جمله به موارد زیر می‌توان اشاره کرد:

- Sam’s Virus Generator
- JPS Virus Maker
- Andreinicks05’s Virus Maker
- Deadlines Virus Maker
- Sonic Bat Virus Creator
- Internet Work Maker Thing

به‌کارگیری این کیت‌ها ساده است، به این معنی که تقریبا هر کسی می‌تواند به راحتی ویروسی خلق کند. اکثر این برنامه‌ها دارای یک محیط گرافیکی هستند. البته دقت کنید ویروس‌هایی که توسط این ابزارها ساخته می‌شوند همگی متعلق به یک خانواده مشخص خواهند بود که نرم‌افزارهای ضدویروسی قادر به شناسایی آن‌ها هستند. بنابراین، ضدویروس به سادگی آن‌ها را شناسایی کرده و معدوم می‌کنند.

تروجان‌ها

تروجان‌ها برنامه‌هایی هستند که تظاهر می‌کنند زمانی که دانلود می‌شوند قادر به انجام کاری هستند، اما در عمل تنها فعالیت‌های مخرب انجام می‌دهند. تروجان‌ها نام خود را از داستان حماسه هومر به عاریت گرفته‌اند. یک نرم‌افزار تروجان به گونه‌ای طراحی شده که کاربر فکر می‌کند یک فایل بی ضرر را دانلود کرده و اجرای آن خطری ندارد، اما زمانی که فایل اجرا شد، در پشت صحنه فعالیت‌های خرابکارانه خود را انجام می‌دهد. تروجان‌ها به این دلیل قدرت زیادی دارند که کاربر را متقاعد می‌کنند آن‌ها را اجرا کند. این فرآیند ممکن است از طریق باز کردن ضمیمه یک ایمیل یا باز کردن فایل‌های PDF، ورد یا اکسل باشد.

تروجان‌ها برای مخفی کردن هدف اصلی خود به بهترین شکل پیاده‌سازی می‌شوند. به‌طور مثال، کارمندان یک سازمان ممکن است یک نامه الکترونیکی به ظاهر ارسال شده از سوی بخش منابع انسانی دریافت کنند و حتا درون فایل فهرستی از افرادی باشد که قرار است اخراج شوند. اگر مهاجم بتواند قربانی را برای باز کردن پرونده یا کلیک روی پیوست با هدف دانلود متقاعد کند به هدف خود رسیده است. این بارگذاری ممکن است به هکر دسترسی از راه دور به سیستم را ارائه دهد یا کلیدهایی که توسط کاربر برای ورود به سیستم استفاده می‌شود را ضبط کند، یک درب پشتی روی سیستم قربانی ایجاد کند، سیستم قربانی را به شبکه بات‌ها متصل کند یا حتا ضدویروس یا دیوارآتش نرم‌افزاری سیستم قربانی را غیرفعال کند. بر عکس ویروس‌ها یا کرم‌ها، تروجان‌ها نمی توانند خود را گسترش دهند و تنها بر مبنای اعتماد کاربر کار می‌کنند.

انواع تروجان‌ها

موسسه EC-Trojans تروجان‌ها را به انواع مختلفی تقسیم می‌کند تا شناسایی و طبقه‌بندی آن‌ها ساده‌تر شود. از جمله گروه‌های اصلی مهمی که توسط این شورا به رسمیت شناخته شده‌اند به موارد زیر می‌توان اشاره کرد:

command shell Trojans

graphical user interface (GUI) Trojans

HTTP/HTTPS Trojans

document Trojans, defacement Trojans

botnet Trojans

Virtual Network Computing (VNC) Trojans

remote-access Trojans

data-hiding Trojans

banking Trojans

DoS Trojans

FTP Trojans

software-disabling Trojans

covertchannel Trojans

در واقعیت، قرار دادن برخی از تروجان‌ها در یک گروه واحد کار سختی است، زیرا بسیاری از آن‌ها بیش از یک کار مخرب را انجام می‌دهند. برای درک بهتر آنچه تروجان‌ها قادر به انجام آن هستند به موارد زیر دقت کنید:

■ Remote access: تروجان‌های دارای دسترسی از راه دور (RAT) به مهاجم اجازه می‌دهند کنترل کامل سیستم را به دست گیرند. Poison Ivy نمونه‌ای از این نوع تروجان‌ها است. تروجان‌های دسترسی از راه دور معمولاً به

عنوان برنامه‌های کلاینت/ سرور ساخته می‌شوند تا مهاجم بتواند به سیستم آلوده متصل شده و آن‌را از راه دور کنترل کند.

■ Data hiding: ایده ساخت این نوع تروجان‌ها پنهان‌سازی داده‌های کاربری است. این نوع بدافزارها بعضا با عنوان باج‌افزار نیز شناخته می‌شوند. تروجان‌های این گروه دسترسی به سیستم آلوده را محدود می‌کنند و تنها زمانی اجازه دسترسی به سیستم را می‌دهند که کاربر باج مربوطه را پرداخت کند.

■ E-banking: این تروجان‌ها اطلاعات بانکی قربانی را رهگیری کرده و به سوء استفاده از آن‌ها می‌پردازند. Zeus نمونه‌ای از این تروجان‌ها است. به‌طور معمول، این تروجان‌ها به عنوان یک شماره تایید تراکنش (TAN) رفتار می‌کنند و از تکنیک تزریق کدهای HTML به درون سیستم کاربر وارد شده یا به عنوان یک فرم دریافت‌کننده اطلاعات، کاربر را فریب می‌دهند. این نوع تروجان‌ها تنها با هدف کسب منفعت مالی ساخته می‌شوند.

■ Denial of service: این تروجان‌ها برای پیاده‌سازی حملات انکار سرویس طراحی می‌شوند. آن‌ها می‌توانند به گونه‌ای طراحی شوند که یک سرویس خاص را از کار انداخته یا کل سیستم را آفلاین کنند.

■ Proxy: این تروجان‌ها به گونه‌ای طراحی می‌شوند که به عنوان پراکسی کار کنند. این برنامه‌ها می‌توانند به هکرها کمک کنند تا از دید کاربر پنهان شده و فعالیت‌هایی که کاربر در رایانه خود انجام می‌دهد را زیر نظر بگیرند. در حالت کلی هرچه هکر از صحنه جرم دورتر باشد، به سختی شناسایی می‌شود.

■ FTP: این تروجان‌ها به‌طور خاص برای کار روی پورت 21 طراحی شده‌اند. آن‌ها به هکرها اجازه می‌دهند تا فایل‌های مورد نظر را دانلود یا آپلود کرده یا فایل‌هایی را برای دستگاه قربانی ارسال کنند.

■ Security-software disablers: این تروجان‌ها برای حمله و از بین بردن ضدویروس‌ها یا دیوارهای آتش نرم‌افزاری طراحی می‌شوند. هدف از ساخت این تروجان‌ها غیرفعال کردن برنامه‌های امنیتی و کنترل ساده‌تر سیستم کاربر است.

نکته: Sality نوعی نرم‌افزار مخرب ضد امنیتی است. این نرم‌افزار ضد امنیتی اولین بار در سال 2003 شناسایی شد و پس از آن بارها و بارها توسط هکرها به کار گرفته شد. Sality با استفاده از تکنیک‌های چند ریختی و مبهم‌سازی نشانه‌های ورود به سیستم (EPO) اقدام به آلوده کردن سامانه‌های ویندوزی می‌کند. زمانی که نصب شد قادر است ضدویروس و دیوارآتش را غیرفعال کند.

پورت‌های مورد استفاده تروجان‌ها و روش‌های ارتباطی

تروجان‌ها می‌توانند به روش‌های مختلفی با هکرها و سامانه‌های راه دور ارتباط برقرار کنند. برخی از آن‌ها بر مبنای مکانیزم ارتباط آشکار کار می‌کنند. این برنامه‌ها هیچ تلاشی برای پنهان کردن فرآیند انتقال داده‌ها انجام نمی‌دهند یا به‌طور تصادفی سامانه کاربر را راه‌اندازی مجدد یا خاموش نمی‌کنند. در مقابل برخی از آن‌ها سعی می‌کنند از کانال‌های ارتباطی پنهان استفاده کنند. این بدان معنا است که هکر برای پنهان کردن انتقال داده‌ها از دید قربانی از روش‌های خلاقانه‌ای استفاده می‌کند. بسیاری از تروجان‌ها که سعی می‌کنند از کانال‌های پنهان استفاده کنند یک درب پشتی روی سامانه قربانی باز می‌کنند. درب پشتی (Backdoor) به هر نوع برنامه‌ای که به هکرها اجازه می‌دهد بدون انجام مراحل احراز هویت عادی به رایانه قربانی متصل شوند اشاره دارد. اگر هکر بتواند یک برنامه درب پشتی را روی سامانه قربانی بارگذاری کند در ادامه قادر است هر زمان که تمایل داشت به سامانه قربانی نفوذ کرده و انواع مختلفی از فعالیت‌های مخرب را انجام دهد. در نتیجه این احتمال وجود دارد که سامانه یکی از کارمندان سازمان بدون اطلاع او ترافیک مخربی را به سمت سرورها و سایر تجهیزات روانه کند. در این حالت هکر از دید کارشناسان امنیتی پنهان است و قربانی مقصر شناخته می‌شود. البته پیاده‌سازی این مدل حملات به ندرت انجام می‌شود، زیرا بیشتر شرکت‌ها نسبت به آنچه در شبکه داخلی رخ می‌دهد حساسیت زیادی دارند.

نکته: یکی از روش‌هایی که یک هکر قادر است یک تروجان را منتشر کند حمله سیب سمی است. با استفاده از این تکنیک، مهاجم به راحتی می‌تواند یک حافظه فلش را روی میز قربانی یا در کافه تریا شرکت قرار دهد و منتظر شود تا قربانی حافظه فلش را به سیستم خود وصل کند. زمانی که کاربر روی فایل آلوده کلیک کرد کدهای مخرب درون فایل بدون مشکل روی سیستم او اجرا می‌شوند. در این حالت کاربر تنها باید یک کلیک کند (یک گاز به سیب بزند) تا

آسیب وارد شود! جدول زیر فهرستی از رایج‌ترین برنامه‌های تروجان، کانال‌های مخفی و برنامه‌های درب پشتی را نشان می‌دهد. ایده خوبی است که یک دقیقه وقت صرف کرده و درگاه‌ها و پروتکل‌های استفاده شده توسط این برنامه‌ها را حفظ کنید. آگاهی در مورد عاملی که به دنبال آن هستید کمک می‌کند به سرعت ریشه بروز مشکلات در زیرساخت‌های یک سازمان را شناسایی کنید.

Name	Default Ports
Senna Spy	21
Shaft	22
Hackers Paradise	31
Executor	80
Masters Paradise	2129
DeepThroat	6670/6671
Masters Paradise	40421 to 40425
NetBus	12345/12346
EvilFTP	23456
Back Orifice	31337/31339
NetSpy	31339
Fore	50766
SchoolBus	54321
Devil	65000

در شماره آینده مبحث فوق را ادامه می‌دهیم.

برای مطالعه رایگان تمام بخش‌های **دوره CEH** روی لینک زیر کلیک کنید:

آموزش رایگان دوره CEH

تاریخ انتشار:

01 خرداد 1399

نشانی منبع:
https://www.shabakeh-mag.com/security/16877/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D8%AA%D8%B1%D9%88%D8%AC%D8%A7%D9%86%E2%80%8C%D9%87%D8%A7-%D9%88-%D9%88%DB%8C%D8%B1%D9%88%D8%B3%E2%80%8C%D9%87%D8%A7-%DA%86%D9%87-%DA%A9%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-%D9%85%D8%AE%D8%B1%D8%A8%DB%8C-%D8%A7%D9%86%D8%AC%D8%A7%D9%85-%D9%85%DB%8C%E2%80%8C%D8%AF%D9%87%D9%86%D8%AF