معرفی انواع تروجان (۲۰ : (Trojan Horse نوع تروجان که باید بشناسید (نسخه PDF)

معرفی انواع تروجان (۲۰ : (Trojan Horse نوع تروجان که باید بشناسید (نسخه چاپی)

۲۰ اگر مقاله‌های گذشـته در رابطه با تروجان و معرفی آن‌ها را مطالعه کرده باشید، الان وقت آن است تا با ادامه این بحث در خدمت شما باشیم. این قسمت به توضیح انواع مختلف تروجان‌ها از حیث نوع و عملکرد می‌پردازد که به علت گستردگی موضوع، در دوبخش خدمت شما ارائه می‌شود.

شماره ۱ : تروجان‌های Command Shell

تروجان‌های Command Shell، از راه دور کنـترل Command Shell را بر روی سیسـتم قربانی بدست می‌گیرند. تروجان سـرور بر روی سیستم قربانی نصب می‌شد که وظیفه اولش باز کردن پورت‌ها برای اتصال نفوذگر به سیسـتم است. کلاینت بر روی سیستم نفوذگر نصب می‌شود و باعث اتصال Command Shell ای نفوذگر به سیستم قربانی می‌شود.

شماره ۲ : Netcat چیست ؟

نفوذگر با استفاده از Netcat، می‌تواند روی سیستم قربانی یک پورت خاص و یا یک backdoor را ایجاد کند که به او اجازه می‌دهد به DOS shell هدف، telnet بزنـد. با یک کامند ساده مثل C:\>nc –l –p ۵۰۰۰ –t –e cmd.exe، نفوذگر می‌تواند پورت ۵۰۰۰ را برای نفوذ اختصاص دهد. با استفاده از Netcat، کاربر میتواند ارتباط ورودی و خروجی TCP یا UDP را از *به هر پورتی برای خود ایجاد کنـد. این کار چک کامل* Reverse *DNS Forward* را برای کاربر ایجاد می‌کند.

بعلاوه این قابلیت هم در اختیار نفوذگر یا کاربر قرار می‌گیرد که بتوانـد از هر سورس لوکالی اسـتفاده کنـد و قابلیت‌های پیش فرض Port-Scanning در دسترسش قرار گیرد.در ساده‌ترین استفاده از Netcat یعنی nc host port یک ارتباط TCP را برای اختصاص دادن پورت بر روی هدف ایجاد می‌کند. سـپس ورودی استاندارد بسوی هدف فرستاده می‌شود و هرچیزی که بتواند از طریق ارتباط برگشت داده شود، بسوی خروجی ارتبـاط ارسال می‌شود.این عمـل تـا زمانی که یکطرف ارتباط خاموش شود، بصورت پیوسـته ادامه پیـدا می‌کنـد. همچنین Netcat می‌تواند به عنوان یک سرور با قابلیت شنود ارتباطات ورودی بر روی پورت‌های دلخواه عمل کند.

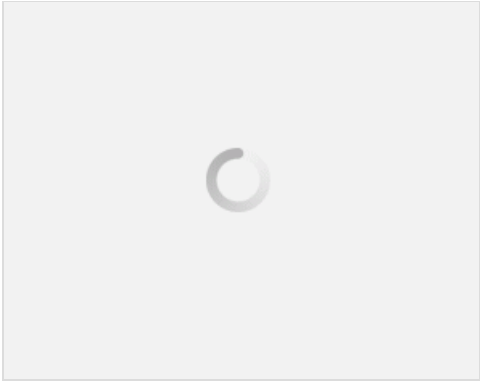
شماره ۳ : GUI Trojans (تروجان‌های گرافیکی)

قابلیت و خاصـیت اصلی این نوع تروجان‌ها گرافیکی بودن ساخت آن‌هاست که توسط نرم‌افزارهای مختلفی صورت می‌پذیرد. از جمله این نرم‌افزارهای می‌توان به Jumper ،MoSucker و Biodox اشاره کرد.

شماره ۴ : Document Trojans یـا تروجان هایی که مسـتندات متصل می شوند

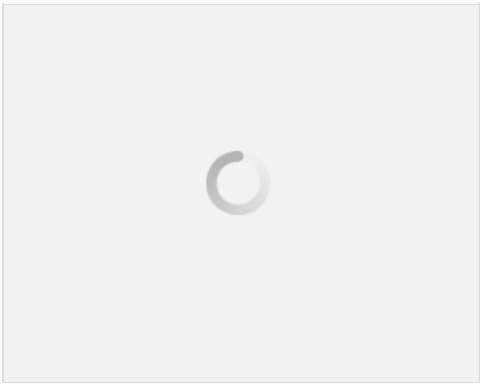
اکثر کاربران علاقه زیادی به آپدیت و آپگرید سیسـتم عامل خود دارند اما این قضیه در مورد نرم‌افزارهای مرتبا انجام نمی‌شود. نفوذگران از

این فرصت استفاده می‌کنند تا Document Trojan ها را نصب کننـد. نفوذگرها معمولا یک تروجان را در قالب یک پوشه جاساز شده کرده و آن را بصورت یـک فایـل پیوست در ایمیلها، پوشـه‌هـای اداری، صـفحات وب یا فایل‌هـای مالتی مـدیا مثل فلش و PDF انتقال می‌دهند. هنگامی که کاربری پوشه حاوی تروجان جاساز شده را باز می‌کند، تروجان بر روی سیستم هدف نصب می‌شود.



شماره ۵ : Emails Trojan یا تروجان های ایمیلی

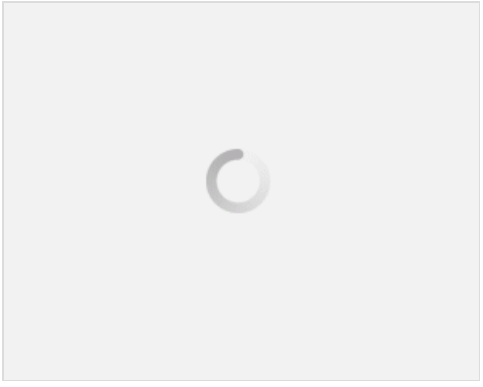
این نوع تروجـان‌هـا از طریق میـل‌هـای گروهی و گسـترده پخش می‌شود. ویروس‌هـای تروجـان از طریق پیوست ایمیـل ارسال می‌شود. هنگامی که کاربر ایمیل را باز می‌کند، ویروس وارد سیستم شده و پس از پخش شدن، سبب ایجاد خسارت‌های زیادی به اطلاعات موجود درسیسـتم می‌شود.همیشه توصـیه شده است که کاربران ایمیل‌هایی که از طرف فرسـتنده‌های ناشـناس دریافت شـده را باز نکنند. گاهی اوقات تروجان‌هـای ایمیلی ممکن است بطور اتوماتیـک تولیـد میل کننـد و به تمام آدرس‌های موجود در لیست مخاطبان سیسـتم قربانی ارسال نماید. بنابراین براحتی توانسته است خود را در بین آدرس‌های مختلف، پخش کند



این تروجان‌ها از طریق نرم‌افزارهای مختلفی قابل تولید هستند که از جمله آن‌ها می‌توان به RemoteByMail اشاره نمود.

شماره ۶ : Defacement Trojans تروجان های تغییر ظاهر

این نوع تروجان‌ها هنگامی که درکل سیستمی پخش می‌شوند، می‌توانند تمام محتوای موجود در دیتابیس را خراب کنند و یا تغیر دهند. این تروجان‌های بـدریخت خطرناکتر هم می‌شوند اگر هدف نفوذگر یک وب‌سایت باشد؛ آن‌ها بصورت سخت‌افزاری تمام فرمت HTML را تغیر می‌دهند و نتیجه آن تغیر فرمت محتوای موجود در وب‌سایت است.



Restorator یکی از نرم‌افزارهایی است که Defacemen Trojan تولد می‌کند.

شماره ۷ : Botnet Trojans تروجان های بات نت

یک بات‌نت مجموعه ای از روبات های نرم‌افزاری (Trojan Horses، Worms و Backdoors) است که بطور اتوماتیک اجرا می شوند. بات نت مجموعه ای از سیستم‌هـای بخطر افتـاده هسـتند که تحت فرمان های مرسوم و ساختاری کنترلی بطور خودکار برنامه‌های خاصی را اجرا می‌کننـد. تولیـد کننده بات نت (نفوذگر) می‌تواند این گروه از سیسـتم‌هـای بخطر افتاده را از راه دور کنترل کنـد. این سیسـتم‌ها که به سیستم‌های زامبی معروف هستند، توسط تروجان‌ها، Wormها آلوده شدند.هدف کنترل کننده بات نت، شبکه های آموزشی، دولتی، نظامی و دیگر شبکه ها می باشد. با کمک بات نت‌ها حملاتی مثل DDoS براحتی انجام می‌پذیرد. این نوع تروجان‌ها بر مبنای دو ساختار کار می کنند:

- Botnet
- Botmaster

چهار نوع توپولوژی که بات‌نت از آن استفاده می‌کند:

- سلسله مراتبی (Hierarchical)
- سرورهای مختلف (Multi Server)
- ستاره‌ای (Star)
- رندوم (Mesh)

شماره ۸ : Proxy Server Trojans یا تروجان های پروکسی سرور

یک Proxy Server تروجان، نوعی از تروجان است که سیسـتم قربانی را طوری تنظیم می‌کنـد که به عنوان یک پروکسـی سـرور عمل کنـد. هنگامی که این تروجان سیسـتم هدف را آلوده کرد، بصورت مخفیانه سیسـتم را تبدیل به یک پروکسـی سرور می‌کند. نفوذگر از این حربه برای اجرای فعالیت‌هـای مجرمانه ماننـد سـرقت اطلاعات کارت بانکی و امثال آن اسـتفاده می‌کنـد و حتی می‌توانـد از طریق آن حملات دیگری را به اهداف مختلف ترتیب دهد.

شماره ۹ : FTP Trojans

یک FTP تروجـان نوعی از تروجان است که طوری طراحی شـده است تا پورت ۲۱ را باز کند و سیسـتم هدف را برای نفوذگر قابل دسترس کند. این تروجان یک FTP سرور را بر روی سیستم هدف نصب کرده و به نفوذگر اجازه می‌دهد تا به اطلاعات حساس دسترسی پیدا کند و فایل‌ها و برنامه‌های موجود در سیستم هدف را با استفاده از پورت ۲۱ و پروتکل FTP، که قبلا باز شده است، منتقل کند.

شماره ۱۰ : VNC Trojans

این نوع تروجـان به نفوذگر اجازه می‌دهد که از سیسـتم هدف به عنوان یک VNC سـرور استفاده کند. این تروجان‌ها بعد از آن‌که اجرایی شدند، توسط آنتی ویروس قابل شناسایی نیستند چرا که VNC سرور خود را به عنوان یک مولفه سودمند نشان می‌دهد.

شماره ۱۱ : HTTP/HTTPS Trojans

تروجان های HTTP/HTTPs، می‌تواننـد از هر فـایروالی رد شونـد و خلاـف جهـتی که یـک تونـل HTTP طی می‌کنـد، عمل کند. آن‌ها از

سخت‌افزارهای وب- بیس و پورت ۸۰ برای عملکرد خود استفاده می‌کنند.

شماره ۱۲ : Shttp Trojan – HTTPS (SSL)

SHTTP یک HTTP سرور کوچک است که براحتی می‌تواند در کنار هر برنامه‌ای خود را جاساز کند. SHTP می‌تواند براحتی خود را در قالب یک فایل Chess.exe کادوپیچ کند و یا بصورت مخفیانه سیستم را تبدیل به یک وب سرور نماید.

- سیستم هدف را با فایل Chess.exe آلوده می‌کند.
- SHTTP در پشت زمینه اجرا می‌شود و روی پورت ۴۴۳ (SSL) شنود می‌کند.
- با استفاده از مرورگر به سیستم هدف وصل می‌شود: Http://۱۰.۰.۰.۵:۴۴۳

پایان بخش اول

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی