به همراه

دنیای زیرزمینی

بدافزارها

و روشهای مقابله

محمدرضا گرمخورانی

نص ناشر تخصصی کتابهای فنی مهندسی کامپیوتر

گرمخورانی، محمدرضا
دنیای زیرزمینی **بدافزارها** [Malwares] و راههای مقابله / مؤلف محمدرضا گرمخورانی.
تهران: نص، ۱۳۸۵.
۲۴۸ ص.: مصور.
ISBN 964-410-082-4 با CD ۲۸۰۰۰ ریال
فهرستنویسی بر اساس اطلاعات فیپا:
۱. ویروسهای کامپیوتری. الف. عنوان.
۴گ ۹ و/QA۷۶/۷۶ ۱۱۵/۸۴
کتابخانه ملی ایران ۷۷۹-۸۵م

موسسه علمی فرهنگی

دنیای زیرزمینی **بدافزارها**
و راههای مقابله
محمدرضا گرمخورانی
چاپ اول: بهار ۸۵
شمارگان: ۳۰۰۰
ناشر: «نص»
چاپ و صحافی: سازمان چاپ و انتشارات وزارت فرهنگ و ارشاد اسلامی
طراحی، آماده سازی: موسسه علمی فرهنگی «نص» قیمت با CD: ۲۸۰۰ تومان

تهران: میدان انقلاب، خیابان اردیبهشت، بن بست مبین، شماره ۲۳۷
تلفکس: ۶۶۴۱۲۳۸۵-۶۶۹۵۳۸۸۳-۶۶۴۶۵۶۷۴ ص.پ. ۸۶۳-۱۳۱۴۵
شابک: ۴-۰۸۲-۴۱۰-۹۶۴ ISBN: 964-410-082-4

مقدمه

بی‌شک فناوری اطلاعات در زمره بزرگترین پیشرفتهای انسانی است که زمینه گسترش و انتشار علوم و اطلاعات را برای عموم فراهم آورده است. دستیابی به آخرین اطلاعات به سادگی چند کلیک تبدیل شده است. این مهم بدون ابزارهایی مانند کامپیوترها، شبکه‌های کامپیوتری و شبکه جهانی اینترنت قابل تصور نیست. در چنین فضای گسترده و پویایی خطراتی نیز در کمین است که همواره کاربران آن را تهدید می‌کند. این تهدید و به عبارتی بدافزارها با بهره‌برداری از ضعفهای امنیتی برنامه‌ها و سیستمهای کامپیوتری و ناآگاهی کاربران و با هدف تخریب و سوءاستفاده از اطلاعات منتشر می‌شوند. در بیانی کوتاه بدافزارها برنامه‌هایی کامپیوتری‌اند (مانند ویروسها، کرمها، تروجانها و...) که برای اهدافی بداندیشانه طراحی و در این فضای ارتباطی رها می‌شوند.

بدین ترتیب هر کاربری لازم است این تهدیدات و ماهیت آنها را شناخته و راه‌های دفاع در برابر آنها را فراگیرد تا بتواند با دیدی کافی مراقب داده‌های خود در مقابل مهاجمان باشد و بدون چنین شناخت و آگاهی حضور در دنیای اطلاعات، جنگ با چشمان بسته خواهد بود.

این کتاب ابتدا با معرفی انواع عمده بدافزارها سعی می‌کند خواننده را با ساختار، ماهیت و اهداف آنها آشنا ساخته، سپس با ارائه روشهایی برای مقابله با این تهدیدات کاربر را آماده دفاع کند.

محمدرضا گرمخورانی
malware@rayaco.ir

فهرست مطالب

فصل اول

بدافزارها..... ۱۰

نمودار تعیین نوع بدافزار..... ۱۰
تکثیر و انتشار..... ۱۰
ویروس‌نویس، مهاجم، قربانی ۱۱
تاریخچه بدافزارها ۱۲
انواع بدافزارها ۱۲
مشخصه‌های بدافزارها..... ۱۶
سیر تحول یک بدافزار عادی..... ۲۲
برنامه‌های سازندهٔ بدافزارها و همسو با آنها .. ۲۴
برنامه‌های مجاز و بدافزارها ۲۶
آنچه بدافزارنویسان رعایت می‌کنند ۲۸

فصل دوم

ویروسها و کرمها..... ۳۲

تولد ویروس..... ۳۲
تعریف ویروس ۳۲
گونه‌های ویروس ۳۳
تکثیر، انتشار، آلودگی..... ۳۳
کرم ۳۴
ماهیت و اهداف کرمها ۳۵
تاریخچه‌ای کوتاه از سرگذشت ویروسها و کرمها ۳۵
انواع ویروسها..... ۳۶
دوره زندگی ویروس..... ۴۷
ساختار ویروس ۴۸
انواع کرمها..... ۵۰
عوامل گسترش سریع کرم ۵۵
نقاط ورودی ویروسها و کرمها و منابع انتشار آنها ۵۶
تکنیکهای استتار ۶۰
فریب‌های ویروسی..... ۶۱
مشکلات ناشی از فریب‌ها..... ۶۲
مقابله با فریب‌ها..... ۶۳
ویروس نویسان..... ۶۳

هدف از ویروس‌نویسی ۶۳
زبانهای ویروس‌نویسی ۶۴

فصل سوم

تروجانها..... ۶۸
شیوه کار تروجان..... ۶۸
انواع تروجانها ۶۹
روشهای ورود تروجان به کامپیوتر..... ۷۴
شیوه‌های پنهان‌سازی تروجانها ۷۷
سایتهای توزیع نرم‌افزار ۸۳
مسمومیت کد برنامه..... ۸۵
روشهای اجرای خودکار تروجانها..... ۸۵
کشنده آشکارسازها ۸۷

فصل چهارم

تولد جاسوس‌افزارها..... ۹۰
جاسوس‌افزار..... ۹۰
انواع جاسوس‌افزارها ۹۰
علائم و اثرات جاسوس‌افزارها..... ۹۷
روشهای نصب جاسوس‌افزارها..... ۹۸
درهای پشتی..... ۹۹
خطر در حال گسترش..... ۹۹

فصل پنجم

روشهای دفاعی در برابر ویروسها و کرمها. ۱۰۲
برنامه‌های ضدویروس ۱۰۲
دیوار آتش..... ۱۰۶
نشانه‌های آلودگی به ویروس..... ۱۰۷
نشانه‌های آلودگی به کرم ۱۰۸
اقدامات و توصیه‌های حفاظتی ۱۰۸
مرور وب و تبادل ایمیل به صورت ایمن.... ۱۱۱
برنامه‌های ضدویروس ۱۱۳
برنامه‌های دیوار آتش..... ۱۱۹
اطلاعات ویروسها ۱۲۰
اطلاعاتی از دنیای ضدویروسها..... ۱۲۰

فصل ششم

روشهای دفاعی در برابر تروجانها..... ۱۲٤
روشهای آلودگی به تروجانها..... ۱۲۴
روشهای حفاظتی در برابر تروجانها..... ۱۲۵
برنامه‌های ضدویروس، برنامه‌های ضد تروجان..... ۱۲۶
برنامه‌های آلوده اینترنتی..... ۱۲۶
معرفی برنامه‌های ضد تروجان ۱۲۶

فصل هفتم

روشهای دفاعی در برابر جاسوس‌افزارها. ۱۳۰
جلوگیری از ورود جاسوس‌افزارها..... ۱۳۰
برنامه‌های ضد جاسوس‌افزار..... ۱۳۱
دیوارهای آتش و جاسوس‌افزارها..... ۱۳۳
نصب برنامه‌هایی عاری از تبلیغ‌افزار ۱۳۴
نصب مسدودکننده پنجره‌های خودبازشو... ۱۳۴
حین مرور اینترنت برنامه‌ای نصب نکنید.... ۱۳۴
حذف تبلیغ‌افزارها ۱۳۵
کشف پردازشهای جاسوس‌افزاری..... ۱۳۵
جاسوس‌افزارها و روشهای اجرای خودکار . ۱۳۶
حذف سارقان مرورگر..... ۱۳۶
حذف BHO های بداندیش ۱۳۸
جلوگیری از فعالیت تبلیغ‌افزارها با فایل HOSTS..... ۱۳۸
برنامه‌های اشتراک‌گذاری و جاسوس افزارها..... ۱۴۰
کوکی‌ها و مقابله با خطرات آنها..... ۱۴۱
کنترل‌های ActiveX و جاسوس‌افزارها..... ۱۴۳

پیوست الف ۱۴۵
ویروس AntiEXE ۱۴۶
ویروس Bablas.A ۱۴۶
ویروس Chernobyl ۱۴۷
ویروس Cybernet ۱۴۷
ویروس Jeefo ۱۴۸
ویروس Melissa.A ۱۴۹
ویروس Melissa.AU ۱۴۹
ویروس Michelangelo ۱۵۰
ویروس PolyBoot.B ۱۵۱
ویروس Pri.Q ۱۵۱
ویروس Rahack.B ۱۵۳
ویروس Resume.a@m ۱۵۴
ویروس Satan Bug.C ۱۵۴
ویروس Thus.T ۱۵۴
ویروس Trivial.88.D ۱۵۵
ویروس Tuareg ۱۵۵
ویروس Venus ۱۵۶
ویروس Y2k ۱۵۶
ویروس Zori.a ۱۵۸
کرم Acebot ۱۵۸
کرم Assiral.A ۱۵۹
کرم Bagle.BN ۱۵۹
کرم Bagle.E ۱۶۰
کرم ـ درپشتی Bereb.C ۱۶۱
کرم Blaster ۱۶۲
کرم Blaster.E ۱۶۳
کرم Bubble Boy ۱۶۳
کرم تروجان Bugbear.B ۱۶۴
کرم CodeRed.F ۱۶۵
کرم Evaman.C ۱۶۶
کرم ـ تروجان Explorer ۱۶۶
کرم Explorer Zip ۱۶۷
کرم Fatso.A ۱۶۸
کرم Fizzer ۱۶۸
کرم Gaobot.CYX ۱۶۹
کرم Gibe.C ۱۷۰
کرم Hai ۱۷۲
کرم Happy ۱۷۲
کرم Hybris.Wsock ۱۷۳
کرم kakworm ۱۷۴
کرم Korgo.D ۱۷۵
کرم Loveletter.CN ۱۷۶
کرم Mapson ۱۷۶
کرم Meve ۱۷۷
کرم Mimail.I ۱۷۸
کرم Mydoom.AM ۱۷۹
کرم Mydoom.G ۱۷۹
کرم Nachi.A ۱۸۰
کرم Navidad.A ۱۸۱
کرم Netlog.A ۱۸۲
کرم Netsky.P ۱۸۲
کرم Netsky.Y ۱۸۳
کرم Newbiwo.A ۱۸۴
کرم Newlove ۱۸۴
کرم Nimda.D ۱۸۵
کرم Padobot.m ۱۸۶
کرم Randex.AA ۱۸۶
کرم Redlof.A ۱۸۷
کرم Sasser.E ۱۸۷
کرم Sober.D ۱۸۹
کرم Stator ۱۹۰
کرم Sumom.A ۱۹۱
کرم Tam.A ۱۹۲
کرم ـ ویروس Trile ۱۹۲
کرم VB.e ۱۹۳
تروجان Beliu.A ۱۹۴
تروجان Bionet.318 ..... ۱۹۴

تروجان Brador.A ۱۹۵
تروجان Cabrotor.10.A ۱۹۵
تروجان Death.18 ..... ۱۹۶
تروجان DoS.Ras.11 ..... ۱۹۷
تروجان Haxdoor.O ۱۹۸
تروجان HLLW.Gool.B ۱۹۹
تروجان IRC.Sx2 ..... ۱۹۹
تروجان Katien.a ۲۰۰
تروجان Keenval.f ۲۰۰
تروجان KeyLogger.aa ۲۰۱
تروجان Kraimer ۲۰۱
تروجان Lopin ۲۰۱
تروجان Mitglieder.CG ۲۰۲
تروجان Mitglieder.S ۲۰۳
تروجان Montp.L ۲۰۳
تروجان NetBuie.b ۲۰۴
تروجان Netbus.160 ..... ۲۰۴
تروجان Orifice2k.sfx ۲۰۶
تروجان Padodor.W ۲۰۶
تروجان PNGBO ۲۰۸
تروجان ـ کرم Pretty Park ۲۰۸
تروجان Qhost.a ۲۰۹
تروجان Rbot.gen ۲۰۹
تروجان Runner.B ۲۱۰
تروجان Shinwow.E ۲۱۰
تروجان Sikou.A ۲۱۱
تروجان Small.hg ۲۱۲
تروجان Sub7.21.Gold ۲۱۲
تروجان Sub7.213 ..... ۲۱۲
تروجان Surila.k ۲۱۴
تروجان Throd.a ۲۱۵
تروجان Tofger.AT ۲۱۵
تروجان Trifor ۲۱۶
تروجان Webber.h ۲۱۶
شماره‌گیر Dialer.DU ۲۱۷
جاسوس‌افزار ـ تبلیغ‌افزار Dyfuca ۲۱۷
جاسوس‌افزار ـ تبلیغ‌افزار Gator ۲۱۸
جاسوس‌افزار ISTbar ۲۱۹
جاسوس‌افزار ـ تبلیغ‌افزار Lop ۲۲۰
جاسوس‌افزار ـ تبلیغ‌افزار nCase ۲۲۰
جاسوس‌افزار New.net ۲۲۱
جاسوس‌افزار ـ تبلیغ‌افزار PurtyScan ۲۲۲
جاسوس‌افزار ـ تبلیغ‌افزار SaveNow ۲۲۳
جاسوس‌افزار ـ تبلیغ‌افزار Searchmeup ۲۲۳
جاسوس‌افزار ـ تبلیغ‌افزار WUpd ۲۲۴

پیوست ب ۲۲۷

منابع و مأخذ ۲۴۵

فصل اول

بدافزارها

اهداف فصل

۱. معرفی بدافزارها
۲. بررسی انواع عمده بدافزارها و دسته بندی آنها
۳. بررسی مشخصه‌های بدافزاری
۴. آشنایی با آسیب‌های ناشی از بدافزارها

کلمات کلیدی :

بدافزار

هر برنامه یا کد کامپیوتری که هدف مخرب و بداندیشانه‌ای داشته باشد.

ویروس

کد کامپیوتری با هدف بداندیشانه که خود را تکثیر کرده و داخل فایلها قرار می‌گیرد.

کرم

بدافزاری که در فایل مجزایی قرار می‌گیرد و توانایی تکثیر و انتشار خود را دارد.

تروجان

بدافزاری که با نفوذ در کامپیوترها اهداف مهاجم را تأمین می‌کند.

جاسوس‌افزار

بدافزاری که در پی جمع آوری اطلاعات مهم کاربر و ارسال آن به مهاجم است.

میزبان

هر فایل و کامپیوتر و به طور کلی سیستمی که پذیرای یک بدافزار باشد.

قربانی

کاربر یا سیستمی که مورد حمله یک بدافزار یا مهاجم است.

حمله

اقدام یک مهاجم علیه دیگر کاربران

بدافزارها

بدافزار (Malware) که مخفف **نرم‌افزار بداندیش** (Malicious software) است، اصطلاحی برای برنامه‌های کامپیوتری با اهداف بداندیشانه و مخرب مانند ویروسها، کرمها و تروجانهاست. به عبارت دیگر بدافزارها برنامه‌های کامپیوتری نامطلوبی هستند که به صورت مخفیانه و یا بدون مجوز با فعالیت ناخواسته و یا با ناپایداری سیستم و یا با استفاده از منابع پردازنده و حافظه باعث می‌شوند کامپیوتر قادر به عملکرد عادی خود نباشد.

بعضی منابع تنها ویروس، کرم و تروجان را بدافزار می‌دانند ولی هر نرم‌افزاری که هدفش غیرمجاز، ناخواسته و ضربه‌زدن به کامپیوتر باشد و حتی برنامه مجازی که در موردی کاربرد نادرستی داشته باشد، در تعریف بدافزار می‌گنجد. البته در این میان اشکالات (Bugs) نرم‌افزاری برنامه‌ها که ناشی از اشتباهات برنامه‌نویسی است و به کامپیوتر و سیستم‌ها آسیب وارد می‌کنند، جزو بدافزارها به شمار نمی‌آید.

بدافزارها را گاهی **کد بداندیش** (Malicious code) و **تهدیدات برنامه‌نویسی شده**(Programmed threats)نیز می‌نامند.

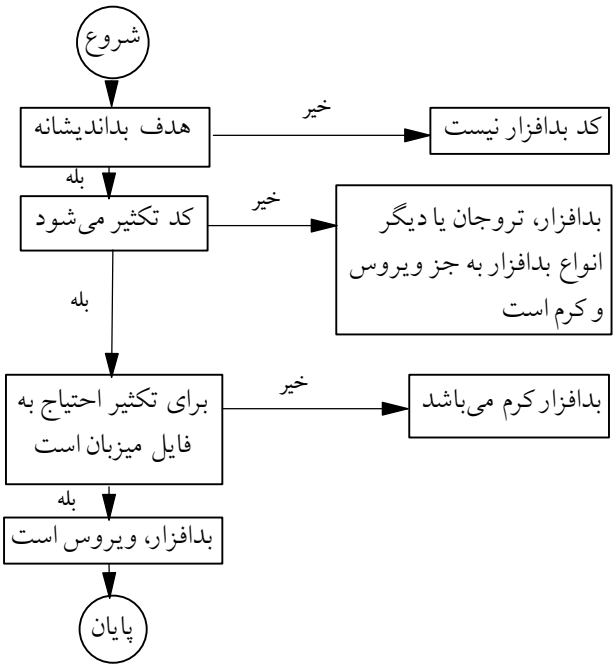
بدافزارها را می‌توان به دو دسته عمده تقسیم کرد: بدافزارهای مستقل و بدافزارهای نیازمند میزبان. بدافزارهای مستقل بدون نیاز به برنامه دیگری توسط سیستم عامل اجرا می‌شود (مانند کرمها و تروجانها). در مقابل، بدافزارهای نیازمند میزبان به تنهایی نمی‌توانند وجود داشته باشند، بلکه باید به برنامه دیگری بچسبند و همراه آنها اجرا شوند (مانند ویروسها). به‌علاوه باید بین برنامه‌های بداندیشی که تکثیر می‌شوند و آنهایی که چنین قابلیتی ندارند، تفاوت قائل شد. تکثیر پردازشی است که طی آن کد بداندیش نمونه‌ای از خودش را دوباره تولید می‌کند. برنامه بداندیش نیازمند میزبان هنگامی فعال می‌شود که برنامه میزبان اجرا شده و یا عملکرد خاصی داشته باشد، در این زمان است که بدافزار فرصت تکثیر را به دست می‌آورد ولی برنامه بداندیش مستقل پس از ورود به سیستم می‌تواند فعال شده و خود را در همان سیستم یا سیستم دیگری تکثیر کند.

نمودار تعیین نوع بدافزار

به کمک شکل ۱-۱ بر اساس عملکرد بدافزارها می‌توان نوع آنها را مشخص کرد.

تکثیر و انتشار

اصطلاح تکثیر و انتشار که به دفعات در مباحث استفاده خواهد شد، دارای مفاهیم متفاوتی هستند. **تکثیر** (Replication) عملی است که طی آن ویروس یا کرم نمونه جدیدی از خود تولید می‌کند. ولی **انتشار** (Spread) به شیوع و پراکندگی بدافزار بر روی کامپیوترها اطلاق می‌شود. منظور از انتشار بدافزار، وجود آن در محیطی خاص است. میزان انتشار بدافزار محدوده آلوده‌سازی آن را نشان می‌دهد. تکثیر یکی از عوامل انتشار بدافزارهاست که تنها ویروسها و کرمها قادر به انجام آن هستند.



شکل ۱-۱ نمودار تعیین نوع بدافزار

ویروس‌نویس، مهاجم، قربانی

افرادی که مبادرت به تولید و انتشار بدافزارها می‌کنند با عنوان کلاسیک **ویروس‌نویس** (Virus writer) یا **بدافزارنویس** (Malware writer) نامیده می‌شوند. این دو عنوان را می‌توان معادل یکدیگر دانست. ویروس‌نویسان علاوه بر ویروسهای کامپیوتری، دیگر انواع بدافزارها (مانند کرمها و تروجانها) را نیز برنامه‌نویسی می‌کنند.

هنگامی که ویروس‌نویس یا هر شخص دیگری از بدافزار ساخته شده علیه فرد یا سیستم دیگری استفاده می‌کند، تبدیل به یک **مهاجم** (Attacker) می‌شود و عمل وی را **تهاجم** یا **حمله** (Attack) می‌نامیم. در مقابل کامپیوتر یا کاربری را که مورد حمله قرار می‌گیرد، کامپیوتر یا کاربر **قربانی** (Victim) یا **هدف** (Target) می‌خوانیم. کامپیوتر یا سیستم کامپیوتری قربانی که پذیرنده بدافزار شده و بدافزار بر روی آن و یا علیه دیگر کامپیوترها فعالیت می‌کند، **میزبان** (Host) بدافزار نامیده می‌شود.

عنوان دیگری که اغلب برای شخص مهاجم به کار می‌رود **هکر** (Hacker) است ولی **هک** (Hacking) کامپیوتری اعمالی را شامل می‌شود که مهاجم سیستم مورد حمله خود را به خوبی می‌شناسد و فعالیتش دارای هدف مشخصی است و ممکن است برای فعالیت خود از بدافزاری استفاده نکند بلکه با بهره‌برداری از آسیب‌پذیری‌های کامپیوترها به آنها نفوذ نماید. در حالی که اغلب پس از انتشار بدافزارهایی مانند ویروسها و کرمها، هیچ کنترلی از طرف ویروس‌نویس بر روی آنها اعمال نمی‌شود و در اکثر موارد ویروس‌نویس

سیستم خاصی را مورد هدف قرار نمی‌دهد بلکه قصدش آلوده‌سازی هر چه بیشتر و تخریب عمومی است. از این رو مهاجم اصطلاحی جامع‌تر و کلی‌تر است و در مطالب از این عنوان استفاده خواهد شد.

تاریخچه بدافزارها

بدافزارها مبحث نسبتاً جدید در دنیای کامپیوتر و فناوری اطلاعات به نظر می‌رسد و کاربران به‌ویژه در دهه اخیر صدمات عمده‌ای از ویروسها، کرمها و تروجانها دیده‌اند. در این میان وسایل ارتباطی کامپیوتری (مانند شبکه‌ها و اینترنت) نقش تعیین‌کننده‌ای در گسترش بدافزارها ایفا می‌کنند. بدافزارها به واقع موضوع جدیدی نیستند، بلکه تا دو دهه اخیر زمینه ظهور گسترده برای آنها فراهم نشده بود. اگرچه کامپیوترهای اولیه مورد حمله ویروسها نبودند، ولی این به معنای عدم آسیب‌پذیری آنها نیست. پیش از گسترش فناوری اطلاعات، افراد اندکی با سیستم‌های کامپیوتری سر و کار داشتند و به همان نسبت سوءاستفاده از این سیستم‌ها اندک بود.

با انقلاب فناوری اطلاعات و ارتباطات و همه‌گیر شدن کامپیوترها، مشکلات آغاز شد. ویروسها در شبکه‌های اختصاصی مانند ARPANET در دهه 1970 ظاهر شدند. با دسترسی عموم افراد به سیستم‌های کامپیوتری در دهه 1980 و آشنایی به نحوه کار کامپیوتر و آسیب‌پذیری‌های آنها، زمینه ظهور ویروس و دیگر بدافزارها در دنیای واقعی و خارج از آزمایشگاه‌ها فراهم شد.

ویروسهایی که در دهه 1980 به وجود آمدند، انواع سیستم‌های عامل و شبکه‌ها را هدف قرار می‌دادند ولی بدافزارهای امروزی اغلب در پی بهره‌برداری از آسیب‌پذیری‌های پراستفاده‌ترین سیستم عامل یعنی **ویندوز مایکروسافت** (Microsoft WINDOWS) هستند. تعداد زیاد این آسیب‌پذیری‌ها فرصت و روشهای مناسبی برای ویروس‌نویسان و مهاجمان فراهم می‌کند.

اولین نسل‌های بدافزارها بیشتر برای اثبات امکان وجود چنین برنامه‌هایی و نشان دادن آسیب‌پذیری سیستم‌ها نوشته می‌شدند. ولی اکنون عمده‌ترین اهداف بدافزارها تخریب وسیع منابع کامپیوتری یا شبکه‌ای و یا دستیابی به اطلاعات مهم و کنترل سیستم‌هاست.

از این روست که امروزه بدافزارها تبدیل به تجارت بزرگی شده‌اند و از سرقت اطلاعات بانکی گرفته تا نمایش آگهی‌های تبلیغاتی و دستیابی غیر مجاز به سیستم‌های حساس، به کمک انواع بدافزارها انجام می‌شود.

انواع بدافزارها

بدافزارها گستره وسیعی از برنامه‌های مخرب را شامل می‌شوند. بدافزارها را می‌توان بر اساس عوامل مختلفی دسته‌بندی کرد از جمله روش مورد استفاده برای حمله یا اجرا، هدف و کارکرد برنامه، شیوه تکثیر یا انتشار، سیستم‌های نرم‌افزاری مورد حمله و...

فهرست زیر چند نوع معروف و رایج از بدافزارها را به صورت مختصری تعریف می‌کند. لازم به ذکر است بعضی از این بدافزارها در تعاریف دقیق‌تر زیر گروه یک یا چند نوع دیگر هستند که همراه معرفی کامل این بدافزارها در فصول بعدی مشخص خواهند شد.

۱. ویروس
۲. کرم
۳. تروجان
٤. درپشتی
۵. کیت ریشه
۶. جاسوس‌افزار
۷. تبلیغ افزار
۸. دستیار مرورگر
۹. سارق مرورگر
۱۰. شماره‌گیر
۱۱. بمب منطقی
۱۲. بهره‌بردار
۱۳. عکس افزار
۱٤. کلید نگار

ویروس (Virus)

ویروس برنامه نرم‌افزاری بداندیشی است که خود را به صورت خودکار با آلوده‌سازی دیگر فایلهای کامپیوتری منتشر می‌کند. ویروس احتیاج به فایل میزبان دارد تا خود را به آن بچسباند. مثلاً یک ویروس بوت، کد خود را در رکورد بوت یا رکورد بوت اصلی دیسک وارد می‌کند، سپس هنگام بوت شدن کامپیوتر از روی دیسک، کد ویروس اجرا می‌شود. یک ویروس فایل، کد خود را داخل فایلهای اجرایی وارد کرده و هنگام اجرای فایل آلوده، ویروس نیز اجرا می‌شود. ویروس ماکرو خود را به مستنداتی مانند فایلهای برنامه Word یا Excel می‌چسباند.

کرم (Worm)

کرم برنامه‌ای مشابه ویروس است که به صورت خودکار از کامپیوتری به کامپیوتر دیگر منتشر می‌شود. کرم با ارسال خود از طریق ایمیل یا هر وسیله دیگری انتشار می‌یابد. کرمها برای انتشار نیاز به فایل میزبان ندارند. کرمها همانند ویروسها توانایی تکثیر خود را دارند و از کامپیوتری به کامپیوتر دیگر منتقل می‌شوند. اولین هدف کرمها و ویروسها انتشار است. عمده‌ترین تفاوت بین کرمها و ویروسها این است که کرمها ممکن است خود را جایگزین فایلهای کامپیوتری کنند ولی کد خود را وارد فایلی نمی‌نمایند. در مقابل ویروسها، کد خود را وارد فایلها می‌کنند و هرگز به صورت فایلهای جداگانه‌ای ظاهر نمی‌شوند.

تروجان (Trojan)

تروجان برنامه‌ای است که به مهاجم امکان کنترل و فعالیت بر روی کامپیوتر آلوده را می‌دهد. تروجانها ابزارهایی هستند که به تناوب توسط مهاجمان به کار می‌رود. زمانی که تروجان اجرا می‌شود،

مجموعه‌ای از کارها را انجام می‌دهد مانند حذف کردن فایلها، اجرای برنامه‌های دیگر و یا نصب یک درپشتی برای دستیابی مهاجم به کامپیوتر آلوده.

درپشتی (Backdoor)

درپشتی برنامه‌ای است که امکان دستیابی مهاجم به کامپیوتر آلوده را با دور زدن روال‌های اعتبارسنجی معمول فراهم می‌آورد. بر اساس نحوه عمل و انتشار، درهای پشتی به دو گروه عمده تقسیم می‌شوند. اولین گروه بسیار شبیه دیگر تروجانها هستند، یعنی داخل برنامه‌های دیگری قرار می‌گیرند و با اجرای برنامه میزبان فعال می‌شوند. دومین گروه مشابه کرمها عمل می‌کنند و به عنوان بخشی از پردازش بوت اجرا می‌شوند و معمولاً همراه کرمهایی که آنها را به عنوان **بار هدف** (Payload) همراه دارند، دیگر کامپیوترها را نیز آلوده می‌کنند.

کیت ریشه (Rootkit)

کیت ریشه برنامه‌ای است که پس از دستیابی مهاجم به کامپیوتر مورد حمله بر روی آن نصب می‌شود. کیت‌های ریشه اغلب حاوی توابعی برای پنهان کردن ردپای حمله مانند پاک کردن یا تغییر **فایلهای ثبت وقایع** (Log files) می‌باشند. کیت‌های ریشه ممکن است شامل درپشتی نیز باشند که به مهاجم اجازه دستیابی مجدد به کامپیوتر مورد حمله را می‌دهد؛ و یا حاوی برنامه‌های بهره‌بردار برای حمله به دیگر کامپیوترها باشد.

جاسوس‌افزار (Spyware)

جاسوس‌افزارها نرم‌افزارهایی هستند که داده‌ها و اطلاعات کاربر را بدون اطلاع وی جمع‌آوری و در اختیار مهاجم قرار می‌دهند. این اطلاعات هر چیزی می‌تواند باشد؛ عادات اینترنتی کاربر، صفحات اینترنتی بازدیده شده، اطلاعات حساب بانکی، کلمات عبور و....

تبلیغ‌افزار (Adware)

تبلیغ افزارها برنامه‌هایی برای نمایش آگهی‌های تبلیغاتی بر روی کامپیوتر هستند. این برنامه‌ها حاوی کدهایی برای دریافت و نمایش تبلیغات در **پنجره‌های خودبازشو** (Pop-up windows) و یا به صورت لینکهای متنی و یا نتایج جستجو هستند. تبلیغ‌افزار توانایی ردگیری فعالیتهای کاربر را دارد.

دستیار مرورگر (Browser Helper Object)

برنامه **دستیار مرورگر** در اصل هدف مخربی ندارد بلکه قابلیت‌های مرورگر اینترنت را افزایش می‌دهد. با این حال برنامه‌های دستیار مرورگر می‌توانند داده های کاربر را بدون اطلاع وی به سازنده خود یا مهاجم ارسال کنند و یا بر روی هدف کاربر از جستجو تأثیر بگذارند.

سارق مرورگر (Browser Hijacker)

برنامه **سارق مرورگر** بعضی امکانات و توانمندی‌های کامپیوتر را به سرقت می‌برد و تغییراتی در تنظیمات مرورگر وب انجام می‌دهد مانند تغییر **صفحه اصلی** (Home Page) مرورگر.

از دیگر اثرات برنامه‌های سارق مرورگر می‌توان به تعویض صفحه جستجوی مرورگر برای هدایت جستجوها به سایتهای جستجوی مشخص، ارسال آدرسهای اینترنتی بازدید شده به مهاجم، باز کردن پنجره‌های تبلیغاتی خودبازشو و ارسال داده‌ها و اطلاعات کاربر به مهاجم اشاره کرد.

شماره‌گیر (Dialer)

شماره‌گیر برنامه‌ای است که اغلب به صورت مخفیانه با تغییر تنظیمات **اتصال تلفنی** (Dial-up connection) به اینترنت، باعث می‌شود کامپیوتر هنگام اتصال به اینترنت به جای تماس با فراهم‌کننده سرویس اینترنت (ISP) محلی کاربر، یک شماره بین‌المللی را گرفته و موجب صورت حسابهای مخابراتی سنگین شود. شماره‌گیرها را بیشتر سایتهای مستهجن بر روی کامپیوترها نصب می‌کنند.

بمب منطقی (Lagic bomb)

بمب منطقی کدی است که داخل برنامه مجازی قرار می‌گیرد و هنگامی که رویدادهای از پیش تعریف شده‌ای رخ دهد، اجرا می‌شود. کد بمب منطقی با وارد شدن به داخل برنامه‌های کاربردی (Applications) یا سیستم عامل باعث می‌شود در شرایطی خاص، بمب فعالیتهای تخریبی یا ضد امنیتی خود را شروع کند.

یک بمب منطقی ممکن است مهاجم را از اتصال کاربر قربانی به اینترنت یا استفاده از برنامه کاربردی خاصی مطلع کند تا مهاجم از آماده بودن کامپیوتر مورد هدف برای حمله آگاه شود.

وجود یا عدم وجود فایلی مشخص، روز یا ساعتی معین یا باز کردن برنامه‌ای خاص می‌تواند نمونه‌هایی از شرایط اجرای بمب منطقی باشد. بمب فعال شده ممکن است فایلی را حذف یا تعویض کرده و یا باعث آسیب‌های دیگری شود.

بهره‌برداری (Exploit)

بهره‌بردار برنامه‌ای است که به آسیب‌پذیری امنیتی خاصی حمله می‌کند. بهره‌بردارها الزاماً بدافزار نیستند، زیرا بسیاری مواقع به عنوان ابزاری جهت تحقیقات امنیتی درباره وجود آسیب‌پذیری‌های کامپیوتری بکار می‌روند. با این حال جزء مشترک و لازم بعضی بدافزارها مانند کرمها هستند.

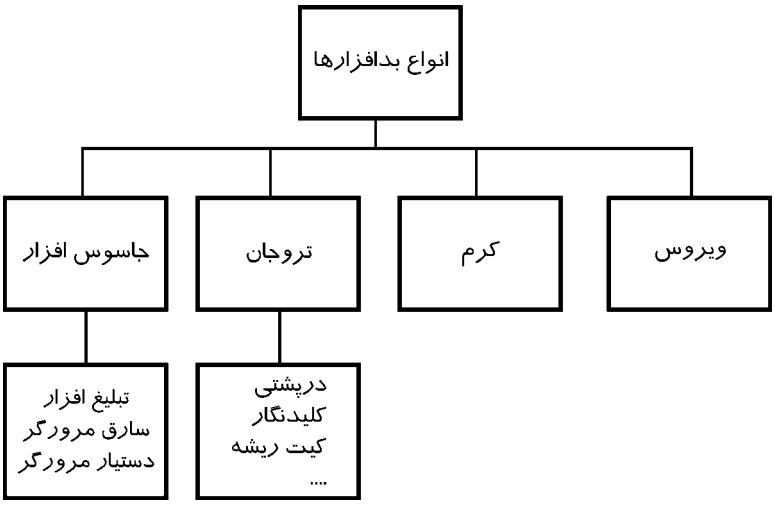
عکس‌افزار (Betrayalware)

عکس‌افزار برنامه‌ای است که دقیقاً عکس کار مورد ادعایش را انجام می‌دهد. مثلاً ممکن است برنامه‌ای که برای حذف جاسوس‌افزارها استفاده می‌شود، خود اقدام به نصب جاسوس‌افزار بر روی کامپیوتر کند.

کلید نگار (Keylogger)

کلید نگار برنامه‌ای است که کلیدهای فشرده شده توسط کاربر را در فایلی ذخیره کرده و می‌تواند فایل حاصل را به مهاجم بفرستد. بسیاری از کلیدنگارها تنها هنگام اتصال به وب‌سایتهای امن مانند سایتهای بانکی فعال می‌شوند. کلیدنگارها مهاجم را برای یافتن اطلاعات حساس مانند نامهای کاربری، کلمات عبور و... کمک می‌کند.

در شکل ۱-۲ دسته بندی کلی بدافزارها را مشاهده می‌کنید.



شکل ۱-۲ دسته بندی بدافزارها

مشخصه‌های بدافزارها

بسیاری از مشخصه‌ها بین انواع و گروه‌های مختلف بدافزارها مشابه و مشترک است به عنوان مثال ویروس و کرم هر دو می‌توانند شبکه را وسیله‌ای برای انتقال خود قرار دهند، اما ویروس برای انتشار، فایلها را آلوده می‌کند ولی کرم تنها خود را تکثیر می‌کند.

در ادامه مشخصه‌های معمول بدافزارها را بررسی می‌کنیم.

محیط‌های هدف

بدافزار تلاش می‌کند به یک سیستم میزبان حمله کند و پیش از انجام حمله وجود برخی اجزای خاص در سیستم هدف ضروری است. چند نمونه از اجزای مورد نیاز برای حمله به یک سیستم میزبان عبارتست از:

۱. **وسایل** (Devices) – بعضی از بدافزارها نوع خاصی از وسایل را هدف قرار می‌دهند مانند کامپیوترهای شخصی، کامپیوتر **مکینتاش** (Macintosh) یا حتی **کامپیوترهای جیبی** (Packet computer).

۲. **سیستم‌های عامل** – ممکن است بدافزار برای اجرای خود به سیستم عاملی خاص یا ویرایش مشخصی از یک نوع سیستم عامل نیاز داشته باشد. برای مثال ویروس CIH که در اواخر دهه 1990 ظاهر شد تنها به کامپیوترهای ویندوز 95/98 حمله می‌کند.
۳. **برنامه‌های کاربردی** (Software applications) – ممکن است بدافزار به برنامه کاربردی نصب شده خاصی بر روی کامپیوتر هدف برای اجرا یا تکثیر خود نیاز داشته باشد. مثلاً ویروس LFM.926 تنها در صورتی می‌تواند به کامپیوتر حمله کند که امکان اجرای فایلهایی با پسوند SWF (فایلهای مربوط به برنامه Shockwave Flash) وجود داشته باشد.

میزبانها

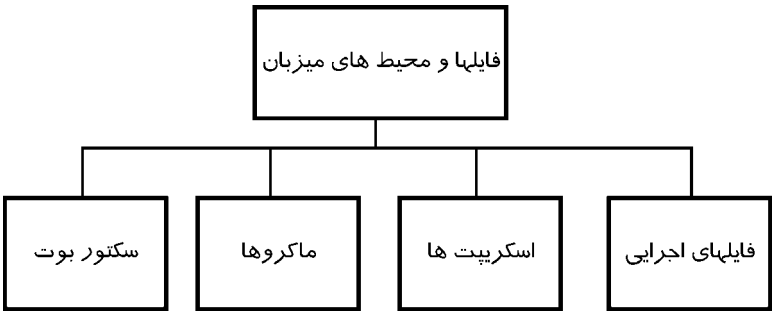
اگر بدافزار یک ویروس باشد، تلاش می‌کند **میزبانها** (Hosts) را برای آلوده‌سازی مورد هدف قرار دهد. تعداد و نوع میزبانها برای بدافزارها بسیار گسترده است. دیگر بدافزارها (به غیر از ویروس) نیز گاهی برای اجرا در داخل فایلهای دیگر قرار می‌گیرند. چند نمونه از میزبانهای رایج بدافزارها عبارتند از:

۱. **فایلهای اجرایی** (Executable Files) – فایلهای اجرایی هدف کلاسیکی برای ویروسها به شمار می‌آید که سعی می‌کنند خود را وارد کد این فایلها کرده و همراه آن اجرا شوند. علاوه بر فایلهایی که پسوند exe. دارند، فایلهای اجرایی ممکن است دارای پسوندهای دیگری مانند com، sys، dll، ovl، ocx و prg. باشند.
۲. **اسکریپت‌ها** (Scripts) – اسکریپت‌ها تکه کدهایی هستند که داخل دیگر فایلها قرار می‌گیرند تا هنگام باز شدن آنها اجرا شوند. حملاتی که اسکریپت‌ها را فایل میزبان خود قرار می‌دهند از یک زبان اسکریپت‌نویسی مانند VBA، JavaScript، Apple Script یا Perl استفاده می‌کنند. پسوند فایلهای اسکریپت زبانهای مذکور عبارتند از vbs.، js.، whs.، و prl.
۳. **ماکروها** (Macros)ـ ماکروها فایلهایی هستند که با یک زبان اسکریپت نویسی ماکرو برای استفاده در برنامه کاربردی خاصی مانند ویرایشگرهای متن نوشته می‌شود. ماکروها حاوی مجموعه‌ای از دستورات اجرایی هستند. مثلاً ویروسها می‌توانند از زبانهای ماکرو نویسی برنامه Word و AmiPro Lotus برای ساخت ماکروهای مخرب استفاده کنند.
۴. **سکتور بوت** (Boot sector) – ممکن است فضاهای خاصی از دیسکهای کامپیوتر مانند رکورد بوت اصلی (MBR) یا رکورد بوت داس (Dos boot record) میزبان ویروس باشند. زیرا امکان اجرای کد بداندیش در آنها وجود دارد. چنانچه از یک دیسک آلوده به ویروس سکتور بوت در کامپیوتر دیگری استفاده شود، باعث آلودگی آن کامپیوتر نیز می‌شود.

شکل ۱–۳ فایلها و محیط‌های میزبان بدافزارها را نمایش می‌دهد.

بار هدف

بدافزار به محض ورود به کامپیوتر میزبان و یا تحت شرایطی پس از ورود، فعالیت خود را شروع می‌کند. این فعالیت **بار هدف** (Payload) آن بدافزار نامیده می‌شود. بار هدف چند گونه مختلف دارد، که رایج‌ترین آنها عبارتند از:



شکل ۱-۳ فایلها و محیط‌های میزبان ویروس

۱. **درپشتی** – این نوع بار هدف دستیابی راه دور غیر مجازی برای مهاجم فراهم می‌کند. درپشتی را اغلب زیر مجموعه‌ای از تروجانها می‌دانند. مهاجم به کمک درپشتی می‌تواند همانند کاربر مجاز ولی از راه دور با کامپیوتر آلوده کار کند.

۲. **خرابی یا حذف داده‌ها** – یکی از معمولترین انواع بار هدف، خراب کردن و یا حذف داده‌ها و غیر قابل استفاده نمودن آنهاست. بدافزارنویسان در این موارد دو انتخاب دارند: بار هدف را برای اجرای سریع طراحی کنند که این نوع عملکرد بالقوه فاجعه‌آمیز است و پیش از کشف و حذف اثرات مخربی به دنبال خواهد داشت ولی طراحی خاص آن باعث شناسایی سریع‌تر و نتیجتاً محدودتر شدن شانس انتشار آن می‌شود. گزینه دیگر نگهداشتن بار هدف در کامپیوتر آلوده (به شکل تروجان) برای مدت مشخصی است. بدین ترتیب بدافزار پیش از اینکه بخواهد بار هدف خود را اجرا کند، فرصت کافی برای انتشار خواهد داشت.

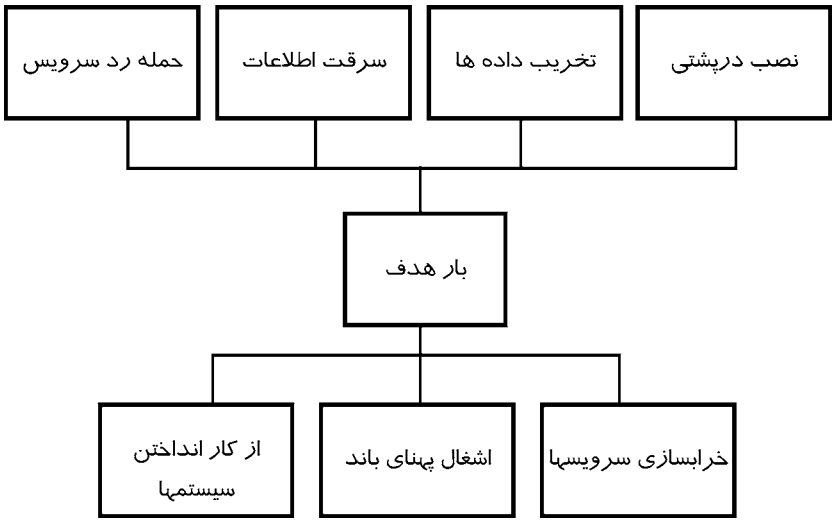
۳. **سرقت اطلاعات** – یکی از انواع نگران‌کننده بار هدف بدافزارها، طراحی آنها برای سرقت اطلاعات و تحویل آن به مهاجم است. اگر بار هدف از سیستم امنیتی کامپیوتر میزبان عبور کند آنگاه می‌تواند وسیله‌ای برای رساندن اطلاعات به مهاجم باشد. سرقت اطلاعات به چند روش میسر است. مثلاً بدافزار می‌تواند فایلهای کامپیوتر هدف را برای مهاجم ارسال کند و یا کلیدهایی را که کاربر فشرده (برای به دست آوردن نام کاربری، کلمه عبور و دیگر اطلاعات حساس) ذخیره و در اختیار مهاجم قرار دهد.
روش دیگر فراهم کردن محیطی بر روی کامپیوتر میزبان است که مهاجم بتواند آن را کنترل و مستقیماً به فایلها دسترسی پیدا کند.

۴. **رد سرویس** – یکی از ساده‌ترین انواع بار هدف حمله **رد سرویس** (Denial of Service)است. حمله رد سرویس تهاجمی کامپیوتری است که باعث اعمال بار اضافی به کامپیوتر میزبان شبکه می‌شود و می‌تواند سرویس‌های شبکه مانند سرور وب یا سرور فایل را از کار بیاندازد. حمله رد سرویس، سرویس‌های خاصی را برای مدتی غیر قابل استفاده می‌کند.
نوعی از حمله رد سرویس به نام **رد سرویس توزیع شده** (Distributed DoS) معمولاً از تعداد بسیار زیادی سرویس گیرنده‌های آلوده استفاده می‌کند که اغلب از نقش خود در حمله آگاه نیستند. حمله رد سرویس توزیع شده نوعی حمله رد سرویس است که از روی چندین کامپیوتر که بدافزار بر روی آنها

نصب شده، به هدف یکسانی شروع می‌شود. مهاجم پیش از حمله بدافزار خود را به روشهای مختلفی منتشر می‌کند. هر کامپیوتر آلوده به این بدافزار، در زمان حمله نقش یک مهاجم را خواهد داشت.
نوعی دیگر از حمله رد سرویس علیه منابع کامپیوتر سعی می‌کند به جای حمله به سیستم‌های میزبان شبکه به منابع کامپیوتر میزبان خود، بار اضافی تحمیل کرده و منابعی مانند ریزپردازنده و ظرفیت حافظه را با درخواست‌هایی بی مورد اشغال و ترافیک پردازشی ناخواسته ایجاد نماید. این نوع حمله باعث کاهش سرعت پردازشی کامپیوتر و ایجاد اختلال در عملکرد آن می‌شود.

۵. **اشغال پهنای باند** – بسیاری از سرویس‌های اینترنتی از طریق اتصالات با پهنای باند محدود به سرویس گیرنده‌ها ارائه می‌شود. اگر بدافزاری بتواند این پهنای باند کم را با ترافیکی بی‌مصرف و ساختگی پر کند، ممکن است به سادگی یک حمله رد سرویس ایجاد کرده و مانع از دستیابی سرویس گیرنده‌ها به سرورها شود.
۶. **ازکار انداختن سیستم** – اگر بدافزار توانایی خاموش کردن یا ازکار انداختن سیستمی را داشته باشد می‌تواند باعث اختلال در سرویس‌دهی یا سرویس‌گیری آن شود. برای حمله به سرویس میزبان نیاز است بدافزار ضعفی در یک برنامه کاربردی یا سیستم عامل پیدا کند که به وسیله آن بتوان سیستم را از کار انداخت.
۷ **خراب‌سازی سرویس** – این نوع بار هدف نیز می‌تواند باعث حمله رد سرویس شود. برای مثال اگر مهاجمی سرور DNS را غیرفعال کند، با انباشته شدن ترافیک و عدم پاسخ‌دهی، شبکه مورد حمله رد سرویس قرار می‌گیرد. به علاوه سرویس‌های سیستم نیز ممکن است بلااستفاده باقی بمانند.

در شکل ۱-۴ انواع معمول بار هدف را مشاهده می‌کنید.



شکل ۱-٤ انواع معمول بار هدف

مکانیزم‌های آغازگر

مکانیزم‌های آغازگر (Trigger Mechanisms) یکی از مشخصه‌های بدافزارهاست که برای شروع تکثیر

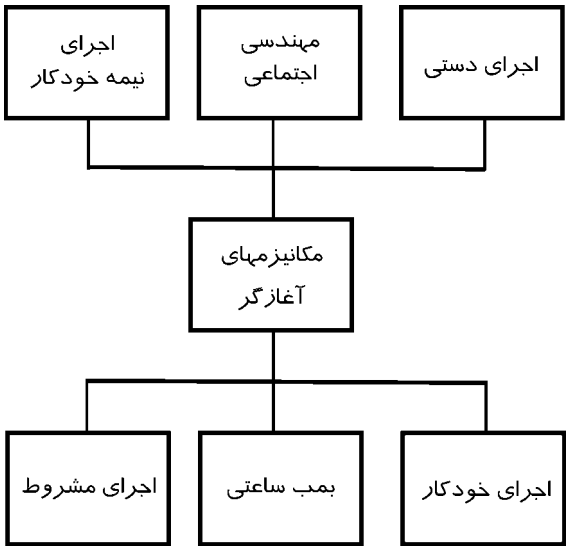
یا رهاسازی بار هدف به کار می‌رود. مکانیزم‌های آغازگر معمول عبارتند از:

۱. **اجرای دستی** – این نوع از مکانیزم آغازگر عبارتست از اجرای بدافزار مستقیماً توسط کاربر قربانی. به عبارت دیگر بدافزار برای شروع فعالیت خود وابسته به دخالت مستقیم کاربر است.
۲. **مهندسی اجتماعی** (Social engineering) – بدافزارها اغلب برای اجرا شدن از بعضی اشکال مهندسی اجتماعی استفاده می‌کنند تا کاربر را فریب دهند. در دنیای بدافزارها هدف مهندسی اجتماعی فریب کاربر و تشویق وی به انجام کار مورد نظر مهاجم است. یک نمونه نسبتاً رایج این روش در کرمهای ایمیلی به کار می‌رود. در پیغام این ایمیل‌ها، متن‌ها و عبارتها به گونه‌ای انتخاب می‌شوند تا کاربر را به خواندن مطلب و باز کردن پیوست ایمیل ترغیب کنند. به علاوه نویسندگان بدافزار ممکن است با ارسال ایمیل‌های جعلی، سعی کنند کاربر را به گونه‌ای فریب دهند که تصور شود پیغام از طرف منبع مورد اعتمادی است. به عنوان مثال کرم Dumaru فیلد From ایمیل آلوده را به گونه‌ای مقداردهی می‌کند که به نظر می‌رسد پیغام از security@microsoft.com آمده است.
۳. **اجرای نیمه خودکار** – در این نوع مکانیزم آغازگر ابتدا با مداخله اندکی از طرف کاربر قربانی فعالیت بدافزار شروع شده سپس اجرا به صورت خودکار ادامه می‌یابد.
۴. **اجرای خودکار** – این نوع مکانیزم آغازگر، نیازی به اجرای دستی ندارد. بدافزاری که از مکانیزم اجرای خودکار استفاده می‌کند، حمله خود را بدون نیاز به اجرای برنامه‌ای از طرف قربانی انجام می‌دهد.
۵. **بمب ساعتی** (Time bomb) – این نوع مکانیزم آغازگر، پس از مدت زمان معینی فعالیتی را انجام می‌دهد. این مدت زمان ممکن است پس از اولین اجرای برنامه‌ای از پیش تعیین شده، تاریخی مشخص و یا بازه زمانی معینی پس از ورود به سیستم باشد. برای مثال کرم MyDoom.B حملات خود را علیه وب‌سایت *www.microsoft.com* در سوم فوریه 2004 و علیه وب‌سایت گروه SCO در اول فوریه 2004 شروع کرد. بعد از آن از اول مارس 2004 از تکثیر خودداری نمود. با این حال درپشتی آن همچنان فعال است.
۶. **اجرای مشروط** – در این نوع مکانیزم آغازگر، حمله تحت شرایطی از پیش تعیین شده شروع می‌شود. برای مثال این شرایط ممکن است تغییر نام یک فایل، مجموعه‌ای از کلیدهای فشرده شده یا اجرای برنامه‌ای خاص باشد. بدافزارهایی که از این نوع مکانیزم آغازگر استفاده می‌کنند گاهی بمب منطقی نامیده می‌شوند (شکل ۱–۵).

مکانیزم‌های دفاعی

بسیاری از بدافزارها از مکانیزم‌هایی استفاده می‌کنند که آنها را از دید برنامه‌های ضدویروس و امنیتی پنهان و حذفشان را مشکل می‌نماید. چند نمونه از این روشها عبارتند از:

۱. **زرهی** (Armor) – روش دفاعی زرهی چند روش برای جلوگیری از شناسایی و تجزیه و تحلیل کد بدافزار و به شکست کشاندن چنین تلاش‌هایی به کار می‌برد. این روش هنگامی که متوجه شد برنامه اشکال‌زدایی (Debugger) در حال اجراست، سعی می‌کند مانع عملکرد صحیح آن شود و یا مقداری کد بیهوده برای مشکل ساختن شناسایی هدف کد بدافزار به آن اضافه می‌کند.



شکل ۱-۵ مکانیزم‌های آغازگر اجرای بدافزارها

۲. **پنهان‌کاری** (Stealth) – بدافزاری که از این روش استفاده می‌کند برای مخفی کردن خود، پنهانی به درخواست‌های انجام شده برای دریافت اطلاعات گوش می‌دهد و داده نادرست به پردازش درخواست‌کننده برمی‌گرداند. برای مثال ممکن است ویروس نمونه‌ای از سکتور بوت غیر آلوده ذخیره کرده باشد و هنگامی که تلاش می‌شود سکتور بوت آلوده بررسی شود، نمونه غیر آلوده را نمایش می‌دهد. یکی از قدیمی‌ترین ویروسهای کامپیوتری به نام Brain (سال 1986) از این روش استفاده می‌کرد.

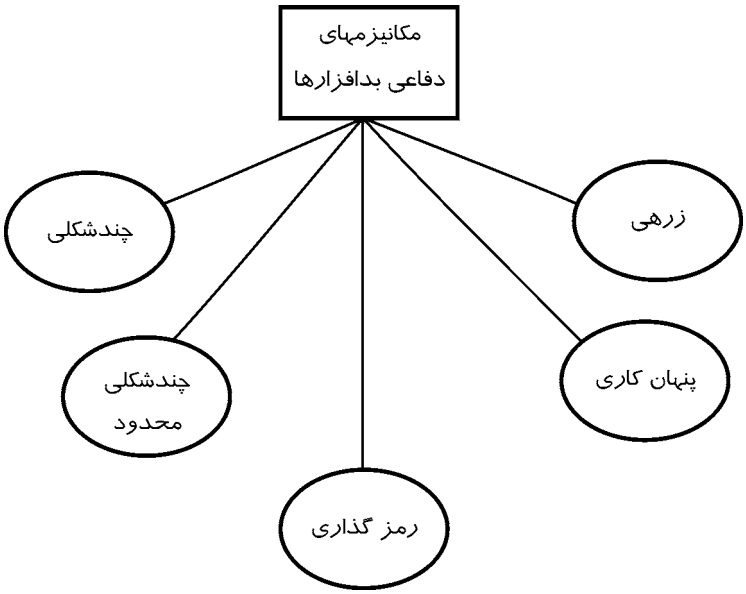
۳. **رمزگذاری** (Encrypting) – بدافزارهایی که از این روش استفاده می‌کنند، خود یا بار هدف خود را رمزگذاری می‌کنند تا از کشف یا بازیابی داده جلوگیری نمایند. بدافزار رمزگذاری شده حاوی یک رویه رمزگشایی ثابت، کلید رمزگذاری و کد بداندیش رمزگذاری شده است و زمانی که بدافزار اجرا می‌شود از رویه رمزگشایی و کلید برای خارج کردن کد بداندیش از حالت رمز استفاده می‌کند. سپس بدافزار یک کپی از کد خود و کلید رمزگذاری جدیدی می‌سازد. با استفاده از کلید جدید، برنامه بدافزار مجدداً رمزگذاری شده و کلید جدید و رویه رمزگشایی به ابتدای بدافزار اضافه می‌شود.

بر خلاف بدافزارهای چندشکلی (که در ادامه توضیح داده می‌شود)، بدافزارهای رمزگذاری شده همواره از رویه رمزگشایی یکسانی استفاده می‌کنند و تنها کلید رمزگذاری در هر بار آلوده‌سازی تغییر می‌کند. برنامه‌های ضدویروس برای کشف بدافزارهایی که از این روش دفاعی استفاده می‌کنند به جستجوی رویه رمزگشایی آنها می‌پردازند.

۴. **چندشکلی محدود** (Oligomorphic) – بدافزارهایی که از این روش دفاعی استفاده می‌کنند، خود را رمزگذاری می‌نمایند و می‌توانند چندین بار مشخص رویه رمزگذاری خود را تغییر دهند. برای مثال ویروسی که بتواند دو رویه رمزگشایی مختلف بسازد در این گروه قرار می‌گیرد.

۵. **چندشکلی** (Polymorphic) – بدافزارهایی که از این روش بهره می‌برند، از شیوه رمزگذاری خاص

خود برای جلوگیری از کشف استفاده می‌کنند و در هر بار رمزگذاری علاوه بر کلید رمزگذاری جدید از رویه رمزگذاری تازه‌ای نیز استفاده می‌نمایند (برخلاف روش رمزگذاری). با هر بار انتشار بدافزار، بخشی از رویه رمزگشایی آن تغییر می‌کند. بسته به کد بدافزار، بار هدف یا دیگر بخش‌ها ممکن است رمزگذاری شوند یا نشوند. معمولاً در بدافزارهای چندشکلی یک موتور تبدیل (mutation engine) وجود دارد که داخل بدافزار قرار می‌گیرد و رویه‌های رمزگذاری تصادفی تولید می‌کند. این موتور و بدافزار هر دو رمزگذاری می‌شوند و کلید رمزگشایی جدیدی به آنها اضافه می‌شود (شکل ۱-۶).



شکل ۱-۶ مکانیزم‌های دفاعی بدافزارها

سیر تحول یک بدافزار عادی

مراحل مختلف تکامل و تحول حملات بدافزاری جدید را می‌توان با الگویی نشان داد. مرور این الگو می‌تواند برای درک دوره زندگی بدافزارها، روند شکل‌گیری و مقابله با آنها مفید باشد.

سیر تحولی جدید زمانی شروع می‌شود که بدافزاری برای اولین بار توسعه می‌یابد و زمانی پایان می‌پذیرد که همه اثرات آن از کامپیوترها و شبکه‌ها حذف و یا تحت کنترل درآید. این مراحل به صورت زیر تعریف می‌شوند:

۱. **طرح‌ریزی** (Conceive) – اغلب توسعه بدافزار از زمانی آغاز می‌شود، که روش حمله یا بهره‌برداری جدیدی پیشنهاد شده و مهاجمان از آن آگاه می‌شوند. با مرور زمان این روشها مورد بحث و بررسی قرار می‌گیرد تا راه مناسبی برای کاربرد آنها در حملات واقعی کشف شود.
۲. **توسعه** (Develop) – ساخت بدافزار نیاز به آشنایی صحیح و کامل از برنامه‌نویسی کامپیوتری و عملکرد

سیستم مورد حمله دارد. با این حال ابزارهای کمکی و تبادل اطلاعات از طریق اینترنت، تولید بدافزار را تسریع می‌بخشد.

۳. **تکثیر** (Replication) – پس از توسعه بدافزار جدید و رهاسازی آن در دنیای واقعی، معمولاً یکی از اهداف عمده، انتشار بر روی میزبانهای مستعد است تا میزان آلودگی بالاتر رود. لازم به یادآوری است که از میان انواع بدافزارها تنها ویروسها و کرمها توانایی تکثیر دارند.

نکته: اگر چه هزاران برنامه بدافزاری شناخته شده ولی در هر زمان تنها تعداد کمی از آنها فعال است این‌گونه بدافزارها را با عنوان "In the wild" می‌نامند. در مقابل بخشی اعظمی از بدافزارها هرگز در فضای عمومی رها نمی‌شوند. این نوع بدافزارها به **ویروس باغ وحش** (Zoo virus) معروفند.

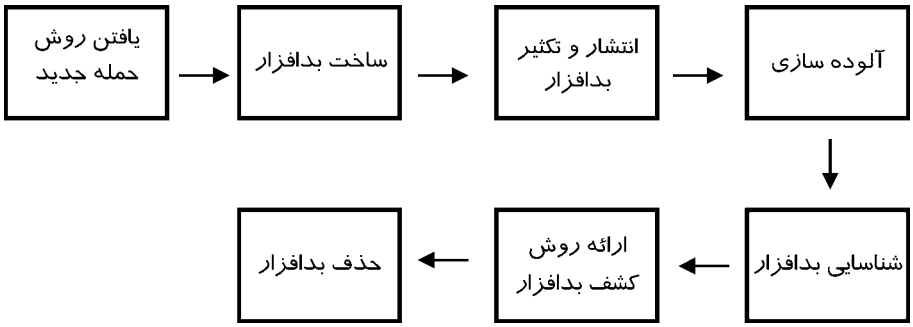
۴. **واگذاری بار هدف** (Deliver payload) – بعد از این که بدافزار توانست با موفقیت میزبان را آلوده کند، می‌تواند بار هدف خود را وارد میزبان نماید. اگر کد بدافزار دارای آغازگر شرطی برای بار هدف خود باشد، این مرحله مهمی است که هنگام برآورده شدن شرط(ها) بار هدف فعال می‌شود. برای مثال بار هدف بعضی بدافزارها زمانی شروع به کار می‌کند که کاربر عمل معینی را انجام دهد و یا ساعت سیستم به زمان خاصی برسد. اگر آغازگر بدافزار به روش اقدام مستقیم (Direct action) عمل کند، این مرحله تنها زمانی فرا می‌رسد که آلوده‌سازی کامل شده باشد.

۵. **شناسایی** (Identify) – در این مرحله از زندگی بدافزار، برنامه‌های ضدویروس و امنیتی قادر به شناسایی آن هستند. در بسیاری از مواقع این مرحله قبل از مرحله ۴ و حتی گاهی قبل از مرحله ۳ رخ می‌دهد ولی همواره این‌گونه نیست.

۶. **کشف** (Detect) – بعد از شناسایی بدافزار، لازم است ارائه‌کنندگان برنامه‌های ضدویروس کد آن را برای دستیابی به یک روش کشف قابل اطمینان، تجزیه و تحلیل کنند. به محض یافتن راه حل مناسب، **فایلهای نشانه** (Signature Files) برنامه ضدویروس به‌روز رسانی می‌شود تا ضدویروس بتواند بدافزار جدید را کشف کند (فایلهای نشانه حاوی اطلاعات و علائم خاص هر بدافزار شناخته شده هستند). مدت زمانی که در این مرحله سپری می‌شود، برای جلوگیری از شیوع بدافزار حیاتی است. به عبارت دیگر هر چه سریع‌تر بتوان روشی برای کشف بدافزار ارائه کرد، میزان شیوع آن کمتر خواهد بود.

۷. **حذف** (Removal) – بعد از این که امکان به‌روز رسانی ضدویروس برای عموم فراهم شد، این وظیفه کاربران است که برنامه ضدویروس خود را برای محافظت از کامپیوترهایشان در مقابل حملات به‌روز کنند.

اگر چه این سیر تحول برای هر حمله بدافزاری جدید تکرار می‌شود ولی برای همه حملات صادق نیست. بسیاری از حملات صرفاً بخشی از کد بدافزار اصلی را تغییر می‌دهند و ویرایش‌های جدیدی از آن می‌سازند. از این رو کد مبنا و روش عمل یکسان است ولی تغییراتی کوچک به مخفی ماندن حمله و نتیجتاً عدم حذف آن کمک می‌کند. معمولاً حمله بدافزاری موفق، تعدادی ویرایش و گونه جدید از خود طی هفته‌ها و ماه‌ها به وجود می‌آورد. این روش باعث می‌شود کشف و حذف بدافزار مشکل شود (شکل ۱–۷). گذشته از بدافزارها، برنامه‌هایی وجود دارد که مستقیماً کامپیوترها را تهدید نمی‌کنند ولی برای ساخت ویروسها یا تروجانها و دیگر بدافزارها و یا برای انجام فعالیتهای غیر مجازی مانند حملات رد سرویس (DoS) و ورود به دیگر کامپیوترها استفاده می‌شوند. این ابزارها عبارتند از:



شکل ۱-۷ سیر تحول بدافزار

برنامه‌های سازندهٔ بدافزارها و همسو با آنها

۱. برنامه‌های حمله رد سرویس (DoS) و حمله رد سرویس توزیع شده (DDoS)
۲. برنامه‌های هک و بهره‌برداری از سیستم‌ها (Exploiting and hacking tools)
۳. ابزارهای ساخت ترافیک سیل‌آسا (Flooders)
٤. ابزارهای ویروس‌ساز (Virtools)
۵. برنامه‌های رمزگذاری فایل و رمزگذاری چندشکلی (Filecryptors and PolyCryptors)
۶. ابزارهای کشنده (Nukers)

برنامه‌های حمله DoS و DDoS

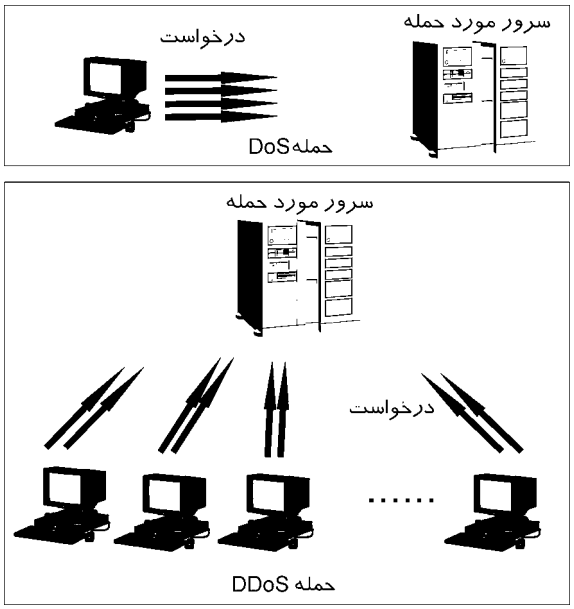
این برنامه‌ها با ارسال تعداد بسیار زیادی درخواست به سرورهای اینترنتی آنها را مورد حمله قرار می‌دهند و اغلب باعث اختلال در عملکرد سرور و از کار افتادن آن می‌شوند. اگر سرور دارای منابع پشتیبان نباشد، در صورت حمله رد سرویس، قادر به پردازش درخواست نخواهد بود.

برنامه‌های حمله DoS حملات را از یک کامپیوتر و با دستور مهاجم انجام می‌دهند. حملات DDoS از تعداد زیادی کامپیوتر آلوده بدون اطلاع و موافقت کاربران آنها برای حمله به سرور مورد نظر خود استفاده می‌کند. برنامه‌های DDoS به روشهای مختلفی قابل انتقال به کامپیوترهای قربانی (و مورد استفاده برای حمله) است. سپس حمله در زمان تعیین شده در کد برنامه و یا با دستور مهاجم شروع می‌شود. کرمها می‌توانند یک رویه DoS را به عنوان بخشی از بار هدف خود منتقل کنند. برای مثال در بیستم آگوست 2001 کرم CodeRed حمله موفقی علیه وب‌سایت ریاست جمهوری ایالات متحده به روش مذکور انجام داد. نمونه دیگر کرم Mydoom.a که حاوی کدی برای حمله DDoS است، به سایت شرکت SCO حمله کرد. این سایت در اول فوریه 2004 اندکی پس از آغاز حمله بسته شد و به آدرس دیگری منتقل گردید (شکل ۱-۸).

برنامه‌های هک و بهره‌برداری از سیستم‌ها

این برنامه‌ها برای نفوذ به کامپیوتر راه دور طراحی شده‌اند تا به کمک درهای پشتی از این کامپیوترها برای

حملات DoS و انتشار بدافزارها به دیگر کامپیوترها استفاده شود. **ابزارهای بهره‌برداری** (Exploits) نیز با استفاده از آسیب‌پذیری‌های سیستم‌های عامل و برنامه‌های کاربردی، در صدد رسیدن به اهداف مشابهی هستند.



شکل ۱-۸ حملات DoS و DDoS

ابزارهای ساخت ترافیک سیل‌آسا

این برنامه‌ها برای ساخت و ارسال سیل‌آسای اطلاعات و پرکردن کانالهای داده‌ای با بسته‌ها و ایمیل‌های بی‌مصرف به کار می‌رود. هدف این برنامه‌ها ایجاد اختلال یا اتلاف منابع و زمان است.

ابزارهای ویروس‌ساز

ویروس‌نویسان از برنامه‌های ویروس‌ساز برای ساخت برنامه‌های بداندیش و تروجانهای جدید استفاده می‌کنند. ویروس سازها برای ساخت انواع ویروسها به ویژه ویروسهای ماکرو برای محیط ویندوز به کار می‌روند. این برنامه‌ها می‌توانند کد منبع ویروس و فایلهای آلوده را تولید و در اختیار ویروس‌نویس قرار دهند. بعضی از ویروس‌سازها دارای رابط گرافیکی کاربری هستند که امکان انتخاب نوع ویروس، میزبانهای مورد حمله، گزینه‌های رمزگذاری، روش حفاظت در مقابل اشکال زداها (Debuggers)، رشته‌های متنی، تأثیرات چند رسانه‌ای و... را از طریق منوهایی فراهم می‌کنند. ویروس سازهایی که طراحی ساده‌تری دارند، بدون رابط گرافیکی کاربری هستند و با دریافت اطلاعاتی درباره نوع ویروس با استفاده از فایلهای پیکربندی اقدام به ساخت ویروس می‌کنند.

به علاوه از این ابزارها می‌توان برای تجزیه و تحلیل ویروس استفاده کرد تا چگونگی عملکرد آن را در حملات هکری مشاهده نمود.

برنامه‌های رمزگذاری و رمزگذاری چندشکلی

برنامه‌های رمزگذاری و برنامه‌های رمزگذاری چندشکلی، برنامه‌هایی هستند که ویروس‌نویسان برای رمزگذاری بدافزارهای خود استفاده می‌کنند تا نرم‌افزارهای ضدویروس قادر به شناسایی آنها نباشند.

برنامه‌های کشنده

مهاجمان با استفاده از کشنده‌ها درخواست‌های کد شده خاصی را به طرف کامپیوتر مورد حمله می‌فرستند تا آن را از کار بیاندازند. این درخواست‌ها با بهره‌برداری از آسیب‌پذیری‌های برنامه‌های کاربردی و سیستم‌های عامل باعث خطاهای جدی و مهلکی می‌شوند.

برنامه‌های مجاز و بدافزارها

مهاجمان از برخی نرم‌افزارهای مجاز و قانونی نیز برای اهداف بداندیشانه و نفوذ به کامپیوترها بهره می‌برند. درباره این که چه نرم‌افزارهایی شامل این مبحث می‌شوند، هیچ اظهار نظر قطعی نمی‌توان ارائه کرد و این موضوع کاملاً به شرایط و دیگر ابزارها بستگی دارد. به محض این که مهاجم استفاده از نرم‌افزاری را برای حمله مفید تشخیص دهد، آن را بدون اطلاع و موافقت کاربر به کامپیوتر مورد هدف منتقل کرده و کنترل کامپیوتر را بدون مواجه شدن با برنامه‌های ضدویروس و امنیتی در دست می‌گیرد. اگر نرم‌افزاری مجاز با مهارت کافی برای اهداف غیر مجاز استفاده شود، شناسایی منشأ حمله بسیار مشکل خواهد شد.

در زیر چند نمونه از نرم‌افزارهای مجاز که ممکن است وسیله‌ای برای حمله باشند، فهرست شده است:

۱. دانلودکننده‌ها (Downloaders)
۲. سرورهای FTP
۳. سرورهای پروکسی (Proxy Servers)
٤. سرورهای Telnet
۵. سرورهای وب (Web Server)
۶. سرویس گیرنده‌های IRC
۷. مونیتورها (Monitors)
۸. ابزارهای کلمه عبور (PWD Tools)
۹. ابزارهای مدیریت راه دور (Remote administration tools)
۱۰. قفل شکن‌ها (Crackers)
۱۱. پیغام فریب (Hoaxes)

دانلود کننده‌ها

حتی برنامه‌های دانلود مجاز نیز ممکن است خطرناک باشند، زیرا این برنامه‌ها معمولاً به گونه‌ای برنامه‌نویسی می‌شوند که در پشت پرده و بدون مداخله مستقیم کاربر عمل کنند و این فرصت خوبی برای

مهاجمان است تا با جایگزینی لینکهایی به منابع آلوده به جای سایتهای دانلود معتبر، بدافزارهای موردنظر خود را بدون اطلاع کاربر به کامپیوتر وی هدایت کنند.

سرورهای FTP

برنامه‌هایی وجود دارد، که برای دستیابی به فایلهای راه دور به کار می‌رود. به محض این که مهاجم چنین برنامه‌ای را روی کامپیوتر کاربر نصب کند، امکان گرفتن فایلهای کامپیوتر قربانی برای وی فراهم می‌شود. به علاوه مهاجم می‌تواند فعالیتهای کامپیوتر آلوده را ردگیری کند.

سرورهای پروکسی

سرورهای پروکسی برنامه‌هایی هستند که در اصل برای ایمن نمودن ارتباطات شبکه‌ای به وسیله جداسازی آدرس داخلی از کاربران خارجی ارائه می‌شوند. ولی مهاجمان از این سرورها برای اتصال به اینترنت به صورت ناشناس استفاده می‌کنند. به این ترتیب که آدرس سرور پروکسی جایگزین آدرس واقعی مهاجم می‌شود.

سرورهای Telnet

این برنامه‌ها برای دستیابی راه دور به منابع کامپیوتری به کار می‌رود. مهاجمان از این برنامه‌ها برای دستیابی کامل به کامپیوتر قربانی استفاده می‌کنند.

سرورهای وب

سرورهای وب برنامه‌هایی هستند که امکان دستیابی به صفحات وب واقع در فضای تعریف شده‌ای از سیستم فایل را فراهم می‌آورند. مهاجمان از این برنامه‌ها برای دستیابی به سیستم فایل قربانی استفاده می‌کنند.

سرویس گیرنده‌های IRC

این برنامه‌ها دستیابی به کانالهای IRC را ممکن می‌سازند. بسیاری از سرویس گیرنده‌های IRC به خصوص mIRC شامل زبانهای اسکریپت‌نویسی قدرتمندی هستند که عملکرد سرویس گیرنده IRC را خودکار می‌کند و اغلب نیازی به مداخله کاربر نیست. این ویژگی ممکن است برای نوشتن تروجانها و کرمهای IRC مورد بهره‌برداری قرار گیرد. هنگامی که مهاجم یک برنامه تروجان IRC روی کامپیوتر قربانی نصب می‌کند، به احتمال قریب به یقین یک سرویس گیرنده IRC نیز نصب خواهد کرد.

مونیتورها

مونیتورها برنامه‌های مجازی هستند که کامپیوتر و فعالیت کاربر را تحت نظر گرفته و اتفاقات را ثبت می‌کنند. معمولاً اطلاعات مربوط به فعالیت کاربر در دیسک کامپیوتر ذخیره و یا به آدرس ایمیل خاصی

ارسال می‌شود. برنامه‌های مونیتور تنها تفاوتشان با برنامه‌های جاسوسی این است که حضور خود را در سیستم پنهان نمی‌کنند و امکان حذف آنها وجود دارد. این برنامه‌ها مشابه برنامه‌های مونیتور شبکه عمل می‌نمایند.

ابزارهای کلمه عبور

این برنامه‌ها کلمات عبور از بین رفته را بازیابی می‌کنند. اطلاعات به دست آمده درباره کلمات عبور یا در صفحه نمایش ارائه و یا در دیسک ذخیره می‌شود. زمانی که مهاجم از این برنامه‌ها استفاده می‌کند، اطلاعات مذکور قابل ارسال به آدرس وی است.

ابزارهای مدیریت راه دور

ابزارهای مدیریت راه دور به مهاجمان امکان کنترل کامل کامپیوتر قربانی را می‌دهد. این برنامه‌های مجاز توسط مدیران شبکه‌ها و برای کنترل از راه دور کامپیوترهای تحت مدیریت‌شان به کار می‌رود.

قفل‌شکن‌ها

برنامه‌های قفل‌شکن نه ویروس هستند نه تروجان، ولی مهاجمان برای شکستن قفل انواع نرم‌افزارها از آنها استفاده می‌کنند. این برنامه‌ها معمولاً به فایلها و نرم‌افزارهای نصب شده آسیبی نمی‌رسانند و تنها حفاظت نرم‌افزارها را در مقابل کپی شدن و یا شماره سریال رفع می‌کنند.

پیغام‌های فریب

این گروه شامل پیغام‌های ایمیلی است که هیچ آسیب مستقیمی به کامپیوترها نمی‌رسانند اما اخطارهایی درباره بدافزاری غیر واقعی به کاربر می‌دهند. این پیغام‌ها ممکن است به کاربر هشدار دهند که به علت وجود ویروس درایوها فرمت خواهد شد و یا علائمی از آلودگی کامپیوتر کشف شده است.

این نوع برنامه‌ها را می‌توان حاصل حس طنز ویروس‌نویسان دانست.

آنچه بدافزارنویسان رعایت می‌کنند

بدافزارنویسان یا همان ویروس‌نویسان بر اساس هدف خود، ممکن است اصول و قواعد برنامه‌نویسی و فنی خاصی را در برنامه‌های تولیدی خود رعایت کنند تا آنها را به نتیجه مطلوبشان برساند. با این حال اغلب بدافزارها برای افزایش گستره شیوع و خسارات خود دو هدف عمده دارند: انتشار هر چه بیشتر و پنهان ماندن از دید کاربر و برنامه‌های امنیتی. بر این اساس چند اصل مهم که اکثر بدافزارنویسان سعی می‌کنند برای نیل به اهداف مذکور آنها را رعایت کنند، در ادامه بررسی می‌شود:

۱. **قابلیت انتقال** (Portability) – ویروسها و کرمها بایستی مستقل از معماری سیستم‌های کامپیوتری باشند و بتوانند بر روی سیستم‌های عامل مختلفی کار کنند. هدف ویروس‌نویسان انتشار بیشتر

بدافزارهایشان است. به همین دلیل همواره سعی می‌کنند رویه آلوده‌سازی و انتشار را به گونه‌ای طراحی کنند که بدافزار بتواند با بهره‌برداری از آسیب‌پذیری‌های مشترک بر روی تعداد بیشتری سیستم عامل و ویرایش‌های مختلف هر سیستم عامل قابل اجرا باشد.

۲. **نامرئی بودن** (Invisibility) – نامرئی بودن بدافزار معادل شکست‌ناپذیری آن است. هنر پنهان ماندن از دید دیگران کشف و شناسایی بدافزار را مشکل‌تر می‌سازد. عمده‌ترین روش برای پنهان کردن فعالیت بدافزار شبیه‌سازی پردازشهای مجاز است تا باعث شک نشود.

۳. **تغییر ظاهر** (Masquerading) – اکثر بدافزارها برای گمراه کردن کاربر و برنامه‌های ضدویروس، پردازشهای خود را با نامهای مشابه پردازشهای سیستم عامل و برنامه‌های امنیتی اجرا می‌کنند. بدین ترتیب تمایز بین پردازش بدافزار و پردازش مجاز مشکل می‌شود.

۴. **تغییرات چرخه‌ای** (Cyclic changes) – تغییرات چرخه‌ای عبارتست از روشهایی برای پنهان نگهداشتن پردازشها. این روشها اغلب مدت کوتاهی دوام دارند و توسط ویروسها و کرمهایی به کار می‌رود که قصدشان رسیدن سریع به هدف مورد نظر است. بعد از این مرحله روشهای پنهان‌سازی دیگری استفاده می‌شود.

نامرئی شدن شیوه‌ای است که بیشتر در بدافزارهای سیستم عامل داس به کار می‌رود و تغییرات چرخه‌ای در سیستم‌های ویندوز.

۵. **استقلال و یادگیری** (Independence and Learning) – فعالیت بسیاری از انواع بدافزارها به گونه‌ای به مداخله کاربر وابسته است مانند اجرای فایلها، باز کردن پیوستها و...

هدف ایده‌آل ویروس‌نویسان نوشتن بدافزارهایی است که بدون نیاز به دخالت کاربر و بر اساس اطلاعاتی از آسیب‌پذیری سیستم‌ها که در داخل بدافزار تعبیه شده، منتشر شود.

۶. **استقلال از محیط و سیستم‌ها** – یکی از اهداف عمده ویروسها و کرمها انتشار هر چه بیشتر است. برای این منظور لازم است که بدافزار مستقل از محیط هدف باشد. محیط هدف را می‌توان سیستم عامل، منابع سخت‌افزاری و نرم‌افزاری آن دانست. به عنوان مثال کرمی که بر روی تمام ویرایش‌های سیستم عامل ویندوز منتشر و اجرا می‌شود احتمال انتشار بیشتری نسبت به کرمی دارد که تنها بر روی بعضی ویرایش‌های ویندوز قابل انتشار و اجراست.

۷. **چندشکلی** (Polymorphism) – امروزه اکثر ویروس‌نویسان از فناوری چندشکلی برای کدهای خود استفاده می‌کنند. بدافزارهای چندشکلی در هر بار اجرا مجدداً رمزگذاری شده و شکل ظاهری آنها تغییر می‌کند. بدین ترتیب شناسایی آنها بسیار مشکل می‌شود.