امنیت شبکه

جلسه دهم: بدافزارها

تهیه و تنظیم: دکتر آرش حبیبی لشکری

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

اولین نسخه: دی 1393
بروزرسانی: دی 1393

فهرست:

بدافزارها

تعريف: يك برنامه‌ای که به صورت پنهاني براي نابود كردن اطلاعات و داده‌ها و يا فعال نمودن برنامه هاي مخرب و غير مطلوب، در يك برنامه ديگر نفوذ مي كند و يا در حالتهاي ديگر محرمانگي و يكپارچگی داده‌ها، دستورالعمل‌ها و كاركرد سيستم و محرمانه و قابل حصول بودن آنها را به مخاطره مي اندازد.

يك ديدگاه مفيد برای دسته بندی بدافزارها بررسی بر مبنای روشهاي سرايت به هدف يا نحوه تكثير وانتشار در آن و سپس بر مبنای عملكردشان يا بارگذاري انواع محتوي پيامها يا واكنشی كه در هنگام رسيدن به هدف بروز مي‌دهند، است.

ديدگاه ديگر دسته بندی براساس ويژگيهای آنهاست *. سه ويژگی بدافزارها :

1. بدافزارهای *همانندزا*: فعالانه تلاش می‌کنند تا با ایجاد کپی‌های جدید یا مشابه خود، تولید مثل کنند.

2. *رشد جمعیت* بدافزار، نشان‌دهنده‌ی این است که تعداد کل همانندهای به وجود آمده از بدافزار در نتیجه‌ی تولید مثل در حال تغییر است. (بدون تولید مثل یعنی رشد جمعیت صفر - ولی رشد جمعیت صفرممکن است همانندزا باشد).

3. بدافزارهای *انگلی*، به کدهای اجرایی دیگری برای زنده ماندن احتیاج دارند (از قبیل کد بلاک بوت روی هارددیسک، کد باینری نرم‌افزارها و کدهای تفسیری).

* منبع : ویروسها و بدافزارهای کامپیوتری – دکتر بابک بشری راد و دکتر آرش حبیبی لشکری

لیست بدافزارها

بمب منطقی

تولید مثل : خیر

رشد جمعیت: صفر

انگلی: ممکن است

یک بمب منطقی کدی است که حاوی دو بخش است:

- تخریبگر ، که عملی برای اجرا شدن است. تخریبگر می‌تواند هر چیزی باشد، اما معمولاً دلالت بر یک عمل خرابکارانه دارد.

- راه‌انداز ، که عبارتست از یک شرط منطقی که ارزیابی می‌شود و کنترل می‌کند که چه زمانی تخریبگر اجرا شود. شرط راه‌اندازی می‌تواند بر مبنای شرایط محلی یا موضعی، مثل تاریخ، کاربری که وارد سیستم شده است، یا نسخه‌ی سیستم عامل تنظیم شده باشد.

بمب‌های منطقی، هم می‌توانند درون یک کد موجود قرار بگیرند، هم به صورت مستقل باشند.

اسب تروآ (تروجان)

تولید مثل: خیر

رشد جمعیت: صفر

انگلی: بله

برنامه‌ای است که به ظاهر، قصد انجام یک کار بی‌خطر و موجه را دارد، اما به طور مخفیانه کارهای اضافی مخربی را نیز انجام می‌دهد. یک مثال قدیمی، برنامه‌های login برای سرقت رمز عبور هستند که یک درخواست به نظر موجه برای نام کاربری و رمز عبور نمایش می‌دهند و منتظر می‌مانند تا کاربر اطلاعات را وارد کند. سپس، برنامه‌ی سرقت‌کننده‌ی رمز عبور، اطلاعات را در جایی برای سازنده آن مخفی می‌کنند و یک پیغام خطای «رمز عبور اشتباه» را نمایش می‌دهند و پس از آن برنامه‌ی *واقعی* login اجرا می‌شود.

بدافزار اسب تروا (تروجان) در يكي از سه مدل زير جاي مي‌گيرد:

- دنبال كردن اجراي ماموريت برنامه اصلي و انجام دادن فعاليت بدافزاري مخرب جداگانه
- دنبال كردن اجراي ماموريت برنامه اصلي ولي تغيير در ماموريت براي انجام دادن فعاليت مخرب
- اجراي عمليات بدافزار مخرب كه بطور كامل جايگزين عمليات برنامه اصلي مي‌شوند

درب پشتی

تولید مثل: خیر

رشد جمعیت: صفر

انگلی: ممکن است

به هر مکانیسمی اطلاق می‌شود که از یک بازرسی امنیتی معمولی فرار می‌کند و اصطلاحاً آن را دور می‌زند. برنامه‌نویس‌ها برخی مواقع درب‌های پشتی را به دلایلی قانونی ایجاد می‌کنند، مثلاً برای جلوگیری از اتلاف وقتِ پروسه‌ی کنترل و تأیید کاربر و رمز عبور، در هنگام دیباگ‌کردن یک سرور شبکه.

همانند بمب‌های منطقی، درب پشتی‌ها نیز می‌توانند هم درون یک کد قانونی و موجه قرار بگیرند و هم به صورت برنامه‌های مستقل باشند.

یک نوع خاص از درب پشتی، *ابزار راهبری از راه دور* یا *تروجان دسترسی از راه دور* است (بسته به اینکه چه کسی درخواست کرده است)، که به طور اختصاری *RAT* نامیده می‌شود. این برنامه ها به یک کامپیوتر اجازه می‌دهند که از راه دور بازرسی و کنترل شوند. (Remote (Remote Access Trojan - Administration Tool

ویروس

تولید مثل: بله

رشد جمعیت: مثبت

انگلی: بله

ویروس، یک نوع از بدافزار است که وقتی اجرا می‌شود، تلاش می‌کند خودش را در یک کد اجرایی دیگر کپی‌کند. وقتی موفق به انجام این کار شد، کد جدید، *آلوده* نامیده می‌شود. کد آلوده، وقتی اجرا شود، به نوبه‌ی خود کد دیگری را می‌تواند آلوده کند. این عمل تولید مثل یا کپی‌سازی از خود بر روی یک کد اجرایی موجود، ویژگی کلیدی در تعریف یک ویروس است.

در جمع کلمه‌ی **virus** توافقی وجود ندارد و دو کلمه‌ی **viruses** و**virii** استفاده میشوند.

اولین تحقیق واقعی علمی و آکادمیک بر روی ویروس‌ها توسط فرد کوهن در سال 1983، با نام ویروس که توسط لِن آدلمن ابداع شده بود، انجام شد. بعضاً از کوهن به عنوان «پدر ویروس‌های کامپیوتری» نام برده می‌شود، اما واقعاً ویروس‌هایی بودند که قبل از شروع تحقیقات او تولید شده بودند. (نوشته شده توسط ریچ اسکرنتا و ویروسهای جو دلینگر بین سالهای 81 تا 83 روی پلتفرمهای Apple II)

کرم

تولید مثل: بله

رشد جمعیت: مثبت

انگلی: خیر

کرم در برخی از خصوصیات با ویروس مشترک است. مهمترین ویژگی مشترک آن‌ها این است که کرم‌ها نیز خود- همانندساز هستند، اما تولید مثل آن‌ها از دو جهت متفاوت است. اول اینکه، کرم‌ها مستقل و متکی به خود هستند، و محتاج به کد اجرایی دیگری نیستند. دوم، کرم‌ها از طریق شبکه‌ها، از ماشینی به ماشین دیگر منتقل و توزیع می‌شوند.

واژه‌ی worm برای اولین بار در سال 1975 توسط جان برونر در داستان علمی تخیلی‌اش به نام *The Shockwave Rider* استفاده شد.

آزمایشات بر روی کرم‌هایی که محاسباتِ (غیرمخرب) توزیع‌شده انجام می‌دهند، حدود سال 1980 در Xerox PARC انجام شد، اما نمونه‌های قدیمی‌تری نیز وجود داشتند.

در حدود 1970 کرمی که creeper نامیده می‌شد و درون Arpanet می‌خزید نیز وجود داشت که بعدها توسط کرم دیگری به نام Reaper تعقیب شد که creeper ها را شکار و نابود می‌کرد.

خرگوش

تولید مثل: بله

رشد جمعیت: صفر

انگلی: خیر

واژه‌ی *خرگوش* برای توصیف بدافزارهایی به کار می‌رود که به سرعت تکثیر می‌شوند. به همین دلیل خرگوش‌ها، با نام *باکتری* نیز نامیده می‌شوند.

به طور واقعی، دو نوع خرگوش وجود دارد:

اولی، برنامه‌ای است که برخی از منابع سیستم، مثلاً فضای دیسک، را به طور کامل مصرف کند. یک «بمب خوشه‌ای»، برنامه‌ای که فرآیندهای جدید، در یک حلقه‌ی بی‌نهایت می‌سازد، مثالی قدیمی از این نوع خرگوش‌هاست.

نوع دوم از خرگوش‌ها، که خصوصیات بالا توصیف می‌کنند، یک حالت خاص از کرم‌ها هستند. این نوع از خرگوش‌ها، برنامه‌های مستقلی هستند که خودشان را از طریق یک شبکه از یک ماشین به ماشین دیگر تکثیر می‌کنند، اما نسخه‌ی اصلی خود را پس از تولید مثل پاک می‌کنند.

جاسوس‌افزار

تولید مثل: خیر

رشد جمعیت: صفر

انگلی: خیر

نرم‌افزاری است که اطلاعات را از یک کامپیوتر جمع‌آوری می‌کند و آن را برای شخص دیگری ارسال می‌کند. (برای نخستین بار این واژه در سال 1995، در یک پست برای شوخی و کنایه‌زدن به مدل رقابت تجاری مایکروسافت استفاده شد)

اطلاعات با ارزش جاسوس افزارها میتواند شامل:

- نام‌های کاربری و رمزهای عبور
- آدرس‌های ایمیل
- شماره حساب‌های بانکی و شماره کارت‌های اعتباری
- کلیدهای فعال‌سازی نرم‌افزارها

آگهی‌افزار

تولید مثل: خیر

رشد جمعیت: صفر

انگلی: خیر

آگهی‌افزار شباهتهایی با جاسوس‌افزار دارد از این جهت که هر دوی آن‌ها اطلاعاتی را در مورد کاربران و رفتارهایشان جمع‌آوری می‌کنند. آگهی‌افزار، بیشتر بازار- محور است و پنجره‌های تبلیغاتی باز می‌کند یا مرورگر وبِ کاربر را به قصد فروش برخی کالاها به وب‌سایتهای خاصی هدایت می‌کند.

البته، آگهی‌افزار ممکن است اطلاعاتی راجع به کاربر را جمع‌آوری و ارسال کند که می‌تواند برای مقاصد تبلیغاتی و تجاری مورد استفاده قرار بگیرد.

هیبرید ها ، dropper ها ، و تهدیدهای مختلط

طبیعت نرم‌افزار باعث می‌شود که ساختن بدافزارهای ترکیبی یا هیبرید که ویژگیهای انواع مختلف را دارا باشند، آسان باشد.

یک مثال قدیمی از هیبرید، توسط کن تامپسون در سخنرانی جایزه تورینگ ***ACM***اش، ارائه شده بود. او یک کامپایلر اجرایی خاص برای ***C*** ساخته بود که علاوه بر کامپایل‌کردن کدهای ***C*** ، دو ویژگی اضافه داشت:

اول اینکه هنگام کامپایل کد سورس، کامپایلر او یک درب‌پشتی برای دور زدن تأییدیه رمز عبور نیز در آن جای می‌داد. دوم آنکه هنگام کامپایل‌کردن کد سورس کامپایلر، یک کد اجرایی کامپایل‌گر با همین خاصیت تولید می‌کرد. بدین ترتیب، در واقع این کامپایلر خاص او، یک تروجان بود که همانند یک ویروس می‌توانست تولید مثل کند و یک درب‌پشتی نیز ایجاد می‌کرد.

یک ***dropper*** ، نوعی بدافزار است که بدافزارهای دیگری را پشت سر خود، در محل رها می‌کند، یا اصطلاحاً *پیاده* می‌کند. به عنوان مثال، یک کرم می‌تواند همچنانکه خودش را پخش می‌کند، بر روی همه‌ی کامپیوترهایی که با آن‌ها برخورد می‌کند یک تروجان، بر جای بگذارد؛ یا یک ویروس ممکن است یک درب‌پشتی از خودش باقی بگذارد.

تهدید مختلط، ویروسی است که علاوه بر نمایش خصوصیات معمول خود، از یک ضعف و آسیب‌پذیری فنی برای انتشار خود بهره‌برداری می‌کند (کرمهای اینترنتی).

زامبی ها

کامپیوترهایی که از لحاظ استاندارد ایمنی، در سطح پایین‌تری هستند می‌توانند توسط یک مهاجم برای انواع مقاصد مختلف مورد استفاده قرار بگیرد. کامپیوترهایی که به این شکل، بدون آگاهی صاحب واقعی آن‌ها، مورد بهره‌برداری قرار می‌گیرند، *زامبی* نامیده می‌شوند.

معمول‌ترین کاربردهای زامبی‌ها عبارتند از ارسال هرزنامه و شرکت در حملات هماهنگ و در مقیاس بالا از نوع از کار انداختن سرویس.

حمله‌ی از کار انداختن سرویس عبارتست از سرریز کردن شبکه‌ی قربانی با ایجاد ترافیک بالا یا تحت فشار گذاشتن یک سرویس عادی شبکه قربانی با ارسال درخواستهای فراوان.

نوعی حمله‌ی از کار انداختن سرویس که از روی تعداد زیادی از ماشین‌ها به راه می‌افتد، حمله‌ی *از کار انداختن سرویس توزیع شده* یا *DDoS* نامیده می‌شود.

ویروس

ويروسها

بخشي از يك نرم‌افزار كه مي‌تواند برنامه‌هاي ديگر، يا در واقع هر متن اجرائي را آلوده نموده و محتويات آنها را تغيير دهد.

اين تغيير شامل تزريق يک روال در برنامه اصلی است که بتواند کدهاي ويروسي را کپی نموده و بنوبه خود مي‌تواند ساير محتويات را نيز آلوده سازند.

ويروس كامپيوتري در ساختمان خود حامل دستورالعملی براي كپي كردن كامل از خود مي-باشد. اين ويروس، بطور مشابه خود را در يك برنامه يا متن اجرائي كامپيوتری تعبيه مي-نمايد.

در مرحله بعد هر زمان كه اين كامپيوتر آلوده شده، بخواهد با كد آلوده نشده‌اي كار نمايد، يك كپي تازه از ويروس مزبور به آن كد جديد وارد مي‌گردد و بهمين علت آلودگي مي‌تواند از كامپيوتري به كامپيوتر ديگر سرايت كند.

بخشهای یک ویروس

یک ویروس کامپیوتري و معمولا بیشتر بدافزارهاي جدید متشکل از يك يا چند بخش مختلف ذیل مي‌باشند:

* **مکانیزم آلوده‌کردن:** با استفاده از این مکانیزم يك ویروس پخش یا منتشر شده و قادر به تکرار خود خواهد بود. این مکانیزم بنام بردار سرایت نیز معروف است.

* **فعال‌سازی:** رخداد یا شرایطي که مشخص کننده زماني است که بارگذاري مخرب فعال گشته یا به کامپیوتر وارد شده است. برخي اوقات بنام بمب منطقی نیز شناخته مي‌شود.

* **بارگذاري مخرب یا تخریبگر:** آنچه که ویروس اضافه بر پخش شدن انجام مي‌دهد، این عمل ممکن است شامل ایجاد آسیب یا يك عمل بي‌خطر ولي قابل ملاحظه باشد.

فازهای ویروس

يك ويروس، در خلال عمر خود، ممكن است در يكي از چهار فاز زير باشد:

* **فاز تاخير :** در اين حالت ويروس غيرفعال است. ويروس در نهايت بدليل برخي پيشامدها مانند: تاريخ اجراء، حضور يك برنامه يا فايل و يا پرشدن ظرفيت ديسك بيشتر از يك حد معين فعال خواهد شد. البته همه ويروسها اين مرحله را ندارند.

* **حالت انتشار:** در اين حالت ويروس يك نسخه از خود را در يك برنامه ديگر يا در جاي مشخصي از فضاي سيستم كپي مي‌كند. اين نسخه ممكن است همانند نسخه اصلي نباشد، چون معمولا ويروسها از شناخته شدن طفره مي‌روند. هر برنامه آلوده شده بنوبه خود حاوي ويروس همگني است كه خود بطور مستقل وارد حالت انتشار خواهد شد.

* **فاز فعال‌سازی :**در اين حالت ويروس براي انجام دادن وظيفه در نظر گرفته شده، فعال مي-گردد. حالت فعال شدن، بمانند فاز تاخير، ممكن است بعلت رخدادهاي مختلف در سيستم از قبيل شماركافي از تعداد نسخه‌هائي كه اين ويروس از خود كپي نموده، بروز نمايد.

* **فاز اجرايي:** در اين حالت عمليات و توابع انجام می‌شوند. اين ماموريت ممكن است مانند ايجاد يك پيغام بر روي صفحه مانيتور مضر نبوده و يا مانند خرابكاري در برنامه‌ها و فايلهاي داده مضر باشد.

ساختمان ويروسهاي اجرائي

كد ويروس سنتي قابل اجراء در كامپيوتر مي‌تواند در همان ابتداء يا بعدا به برخي از برنامه-هاي اجرائي متصل شود و يا مي‌تواند بطريق ديگر به برنامه وارد شود. اصل عمل ويروس اينست كه وقتي برنامه اجرائي آلوده شده براي انجام دادن كاري به خدمت گرفته مي‌شود، ابتداء كد آلوده و در مرحله بعد كد اصلي به اجراء در خواهد آمد.

يـک ترسـيم عمـومی از سـاختمان ويروس در شـكل روبـرو نشـان داده شـده اسـت. در ايـن حالـت كـد ويـروس، V، در همـان ابتـداء جهـت آلوده كردن برنامه ها اضافه می‌شود و اين گونه فرض شده است كـه اولـين نقطه ورود ويروس به برنامه در زمانی كه به خدمت گرفته مـی‌شـود، اولـين خط برنامه باشد.

```
program V
1234567;

procedure attach-to-program;
begin
    repeat
        file := get-random-program;
    until first-program-line ≠ 1234567;
    prepend V to file;
end;

procedure execute-payload;
begin
    (* perform payload actions *)
end;

procedure trigger-condition;
begin
    (* return true if trigger condition is true *)
end;

begin (* main action block *)
    attach-to-program;
    if trigger-condition then execute-payload;
    goto main;
end;
```

الف: يک ويروس ساده

```
program CV
1234567;

procedure attach-to-program;
begin
    repeat
        file := get-random-program;
    until first-program-line ≠ 1234567;
    compress file;  (* t1 *)
    prepend CV to file;  (* t2 *)
end;

procedure (* main action block *)
    if ask-permission then attach-to-program;
    uncompress rest of this file into tempfile;  (* t3 *)
    execute tempfile;  (* t4 *)
end;
```

ب: يک ويروس فشرده

دسته بندي ويروسها

ويروسها را بر مبناي دو محور متعامد دسته‌بندي می شوند:

يکی نوع هدفي که ويروس قصد آلوده کردن آنرا دارد و ديگری روشهاي مورد استفاده جهت مخفي شدن بمنظور جلوگيري از شناسائي توسط آنتی ويروس ها.

دسته بندی براساس هدف:

* **آلوده کننده سکتور راه اندازی:** اين ويروس اطلاعات راه اندازي اصلي سيستم را آلوده ساخته و هنگام روشن شدن کامپيوتر از محل آلوده شده در سيستم پخش مي‌شود.

* **آلوده کننده فايلها:** اين ويروس فايلهائي را آلوده مي‌سازد که طبق فرمانها و اصول کارکرد سيستم در زمره فايلهاي اجرائي به حساب مي‌آيند.

* **ويروس ماکرو:** اين ويروس فايلهائي را آلوده مي‌سازد که حاوي ماکرو يا کدهاي فرمان مورد استفاده در برنامه‌هاي کاربردي سيستم باشد.

* **ويروس چند جزئي:** اين ويروس فايلها را به چندين طريق مختلف آلوده مي‌سازد. ويروس چند جزئي قادر است که انواع فايلهاي مضاعف را نيز آلوده سازد، بنابراين، بطوراساسي اين ويروس بايد با تمام حوزه‌هاي آلوده‌سازي ممکن، تعامل داشته باشد.

دسته بندي ويروسها

دسته بندی براساس روش مخفی سازی:

* **ويروس رمز گذاري شده:** رويكرد كلي از اين قرار است كه بخشي از ويروس يك كد رمزگذاري تصادفي خلق مي‌كند و تمام ويروس را رمزگذاري مي‌كند. كد رمزگذاري در نزد خود ويروس نگهداري مي‌شود. هنگامي كه يك برنامه كه قبلا آلوده شده توسط كاربر مورد استفاده قرار مي‌گيرد، ويروس آن كد را براي باز كردن رمز مورد استفاده قرار مي‌دهد. زماني كه ويروس خود را كپی مي‌كند يك كد رمزگذاري تصادفي ديگر اختيار مي‌نمايد. بدليل اينكه ساختمان ويروس با كدهاي مختلف در هر مرحله رمزگذاري شده است، بنابراين هيچگونه روند ثابتي براي دنبال كردن آن وجود ندارد.

* **ويروس پنهانكار:** نوعي از ويروس كه بطور خاص براي پنهان شدن از شناسائي توسط نرم افزارهاي ضد ويروس طراحي شده است. بنابراين نه فقط عمليات انتشار پيامهاي مخرب بلكه كل ويروس مخفي است. اين ويروس ممكن است براي رسيدن به اين هدف علاوه بر كد جهش يا تغيير ناگهاني مثل فشرده-سازي از تكنيك روتكيت نيز استفاده نمايد.

* **ويروس چندريختی:** يك نوع ويروس كه با هر بار آلودگي تغيير مي‌يابد و بهمين علت رديابي آن با استفاده از اثرش تقريبا غيرممكن است.

* **ويروس دگرريخت:** مانند ويروس چند ريختی، اين ويروس هم با ايجاد هر آلودگي تغيير مي‌يابد. ولي با اين تفاوت كه ويروس دگرريخت بعد از هر تكرار خود را بطور كلي بازنويسي مي‌كند و شناسائي خود را مشكلتر مي‌سازد. ويروسهاي دگرريخت ممكن است رفتار خود را به همان خوبي تغيير دهند كه ظاهرشان را عوض مي‌كنند.

ويروسهاي ماكرو و اسكريپت

ويروس ماكرو در اصل كدهای اسكريپتی كه وظيفه پشتيباني از محتويات بسياري از اسناد كاربران را دارند، را آلوده مي‌سازد. علل اهميت ويروسهای ماكرو:

- يک ويروس ماكرو در اصل مستقل از پلتفرم است.
- ويروس‌های ماكرو اسناد نوشتاري مربوط به بخش‌هاي غير اجرائي كدها را آلوده مي-سازند.
- ويروسهاي ماكرو بسهولت پخش مي‌شوند، زيرا از اسنادي كه براي استفاده عادي به اشتراك گذاشته شده، بهره مي‌گيرند. نمونه خيلي رايج و معمول آن سوء استفاده از پستهای الكترونيكی است.
- ويروسهاي ماكرو اسناد كاربران را بيشتر از برنامه‌هاي سيستمي آلوده مي‌سازند، زيرا فرض بر اين است كه اين اسناد بطور مداوم توسط كاربران اصلاح مي‌شوند.

کرم

كرمها

همانطور كه پيشتر نيز گفته شد كرم برنامه اي است كه بطور فعال بدنبال يافتن و آلوده‌كردن سيستم‌هاي ديگر مي‌باشد و سپس هر كدام از سيستم‌هاي آلوده شده بمانند يك سكوي پرتاب خودكار جهت آلوده‌كردن سيستم‌هاي ديگر وارد عمل مي‌شوند.

كرمها از نرم‌افزارهاي آسيب پذير در برنامه‌هاي كاربر يا سرويس‌دهنده، براي بدست آوردن راه دسترسي به هر سيستم جديد، بهره برداري مي‌كنند.

كرمها مي‌توانند:

- جهت تكثير از يك سيستم به سيستم ديگر از ارتباطات شبكه‌اي استفاده نمايند.
- از اطلاعات و داده‌هاي به اشتراك گذاشته شده در وسايلي مانند USB يا CD و DVD جهت تكثير استفاده كنند.
- و يا كرمهاي پست الكترونيكی می توانند با استفاده از برنامه‌هاي ماكرو يا كدهاي نوشتاري موجود در اسناد ضميمه پست الكترونيكی يا فايلهاي آني مورد استفاده در انتقال بوسيله پيغام رسانها منتشر شوند.

روشهای تکثیر کرم

* **نامه‌هاي الكترونيكي يا تسهيلات پيام آنی:** يك كرم نسخه‌اي از خود را بصورت پست الكترونيكی به ساير كامپيوترها ارسال نموده و يا خود را بصورت يك ضميمه به خدمات پيامرسان آني الصاق مي‌نمايد. بطوريكه كد مربوط به آن كرم هنگام مطالعه پست الكترونيكی يا باز كردن ضميمه اجراء گردد.

* **اشتراك‌گذاري فايلها:** يك كرم يا يك نسخه از خود را بوجود آورده و يا مانند يك ويروس فايلهاي سودمند را در وسايل قابل حمل مانند حافظه‌های USB آلوده مي‌سازد. اين كرم بعدا زمان اتصال تجهيز USB آلوده به يك سيستم ديگر با استفاده از مكانيزم خودراه‌انداز و با بهربرداري از بعضي نرم-افزارهاي آسيب پذير، فعال مي‌گردد. و يا زماني شروع به فعاليت مي‌كند كه كاربر فايلهاي آلوده را در كامپيوتر هدف باز نمايد.

* **قابليت اجرای از راه دور:** يك كرم نسخه‌اي از خود را در يك سيستم ديگر به اجراء در مي‌آورد، اين عمل يا بصورت استفاده آشكار از امكانات اجرای از راه دور و يا بوسيله بهره‌برداري از نقص يك برنامه در خدمات شبكه، جهت خرابكاري انجام مي‌گردد.

* **دسترسي به فايلها از راه دور يا قابليت انتقال:** يك كرم از تسهيلات دسترسي به فايلها از راه دور يا خدمات انتقال به يك سيستم ديگر بمنظور كپي نمودن خود از يك سيستم به سيستم ديگر استفاده مي‌نمايد. جائي كه شايد كاربر سيستم بعدي آنرا به اجرا در آورد.

* **قابليت ورود به كامپيوتراز راه دور:** يك كرم بمانند يك كاربر در يك سيستم راه دور داخل شده و سپس از فرامين بمنظور كپي نمودن خود از يك سيستم به سيستم ديگر استفاده مي‌نمايد كه بعدا به اجرا در بيايد.

تکثیر – فعال سازی - اجرا

مرحله تکثیر عموما شامل دو بخش بنام جستجو براي يافتن بهترين طريقه دسترسي و استفاده از مكانيزم دسترسي پيدا شده براي انتقال يك نسخه از خود به يك سيستم راه دور و تحريك آن نسخه جهت عمل در آن سيستم می باشد.

اولين مرحله در تكثير كشف هدف است. استراتژي‌هاي مختلفی برای پويش شبكه كه توسط بدافزار كرم اجراء مي‌شوند عبارتند از:

* **تصادفي:** هر سيستم آلوده شده ميزبان كرم، شروع به تفحص تصادفي آدرسهاي مختلف كامپيوترهاي موجود در فضاي آدرس IP با استفاده از روشهاي پيگردي مختلف مي‌نمايد.

* **فهرست ضربه:** مهاجمان در مرحله اول يك فهرست بلند از سيستم‌هاي بالقوه آسيب پذير گردآوري مي‌نمايند.

* **برمبنای توپولوژی:** اين روش اطلاعاتي كه در يك سيستم آلوده شده قرباني وجود دارد را بمنظور يافتن ميزبان هاي بيشتر براي انجام عمل پويش در مورد آنها مورد استفاده قرار مي‌دهد.

* **زير شبكه محلي :** اگر يك كامپيوتر ميزبان با وجود استفاده از ديوارآتش آلوده شد، آن كامپيوتر ميزبان آنگاه در جستجوی اهدافي در شبكه محلي خواهد بود.

الگوي تكثير كرم

ويروسها و كرمهاي كامپيوتري رفتارهاي مشابه با ويروسهاي بيولوژيكي در نحوه تكرار و تكثير از خود بروز مي‌دهند. يك الگوي ساده كلاسيك همه‌گيري مي‌تواند بصورت زير تشريح گردد.

$$\frac{dI(t)}{dt} = \beta I(t)S(t)$$

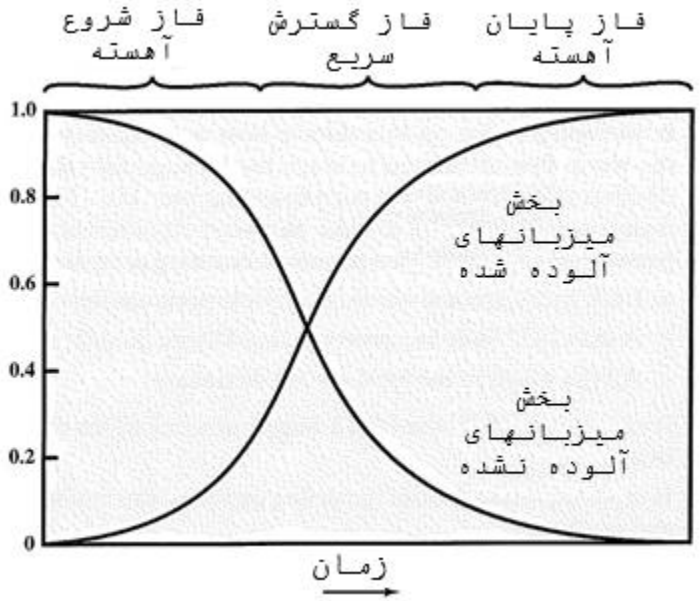
كه در آن :

$I(t)$ = تعداد سيستم های آلوده شده در زمان t

$S(t)$ = تعداد سيستم‌های مشكوک به آلودگی (مشكوک ولی هنوز آلوده نشده) در زمان t

β = نرخ آلودگی

N = *اندازه جمعيت*، $N=I(t) + S(t)$



حالتهای فن آوری کرم

چند پلتفرمی: کرم‌هاي جديد محدود به برنامه كامپيوتري سيتم عامل ويندوز نبوده بلكه مي‌توانند از برنامه‌هاي مختلف مانند برنامه هاي عمومي يونيكس يا برنامه‌هاي ماكرو و زبانهاي اسكريپتی استفاده نمايند.

چند منظوره: کرم‌هاي جديد از راههای مختلف مانند بهره‌برداري كردن از خدمات وب، مرورگرها، نامه‌هاي الكترونيكي، به‌اشتراک گذاري فايلها، و ساير كاربردهاي مبتني بر شبكه، و يا از طريق به اشتراک‌گذاری رسانه‌ها بدرون سيستم نفوذ مي‌كنند.

پخش شدن خيلي سريع: كرمهاي جديد از فن‌آوريهاي مختلف جهت رسيدن به بالاترين نرخ پخش شدن بهره برداري مي‌كنند (شناسائي تعداد بيشتري كامپيوتر آسيب پذير در يك دوره زماني كوتاه).

چندريختی: برای گريز از كشف شدن، فرار از فيلترهای پيشين، خنثي نمودن تحليلهاي بلادرنگ

دگرديس: اضافه بر تغيير ظاهر، كرمهاي متامورفيك يا دگرديس داراي مجموعه‌اي از الگوهاي رفتاري هستند كه در مراحل مختلف تكثير آماده بروز مي‌باشند.

وسيله انتقال: چون مي‌توانند خيلي سريع تعداد زيادي از سيستم‌ها را به سازش وادار نمايند، لذا براي پخش كردن طيف وسيعي از بدافزارهاي مخرب، مانند بات‌ها، روت‌كيت‌ها، هرزنامه‌هاي الكترونيكي و جاسوس-افزارها بكار ميروند.

سوءاستفاده روز صفر (زمان تولد): براي بدست آوردن حداكثر غافلگيري و پخش شدن، يك كرم در روز صفر (زمان تولد) و اولين لحظه شروع به كار، بايد از يك آسيب پذيری ناشناخته كه فقط بوسيله كميته شبكه عمومي كشف شده، بهربرداري نمايد.

هرزنامه الکترونیکی (نامه هاي ناخواسته)

نامه‌هاي ناخواسته معمولا بنام هرزنامه خوانده مي‌شوند. اين هرزنامه‌ها هزينه زيادي هم به كاربر و هم به سازمان شبكه وارد مي‌كند، سازمان شبكه از جهت نياز به بازپخش اين حجم از نامه‌ها و كاربر از جهت نياز به تصفيه نامه‌هاي مشروع خود از ميان حجم عظيم نامه‌هاي ناخواسته متحمل هزينه مي‌شوند.

بخش قابل ملاحظه‌اي از موضوعات هرزنامه‌ها فقط تبليغات است، كه سعي مي‌كنند كاربر را تشويق به خريد بعضي محصولات از طريق فضاي مجازي نمايند، يا در امر كلاهبرداري مانند كلاهبرداري در محموله‌ها و يا ارسال غير قانوني پول مورد استفاده واقع مي‌شوند.

اما در هر صورت هرزنامه‌ها حمل كننده‌هاي خوبي براي بدافزارها محسوب مي‌شوند. همانطوريكه در قسمت قبلي بحث گرديد، نامه‌هاي الكترونيكي ممكن است داراي مدارك ضميمه‌اي باشند، كه اگر باز شوند، احتمال دارد كه يك نرم افزار آسيب‌پذير سيستم را جهت نصب يك بدافزار بر روي آن سيستم مورد بهره‌برداري قرار دهند. يا اينكه حاوي يك برنامه تروجان ضميمه و يا كد اسكريپت باشند، كه اگر باز شوند، باعث نصب يك بدافزار بر روي آن سيستم خواهند شد.

هرزنامه‌ها، بطورمعمول، كاربر را به يك وب سايت جعلی كه برخی از خدمات قانوني مانند سايت بانكداري اينترنتي هدايت مي‌نمايند، كه اين عمل كوشش در جهت كسب جزئيات شناسه و رمزعبور كاربر و يا كامل نمودن بعضي جداول با جزئيات اطلاعات شخصي كافي جهت باز گذاشتن دست مهاجم بمنظور جعل هويت كاربر در يك دزدي هويتي مي‌باشد.

بات – زامبی- بات نت

يك بدافزار منبع محاسبات الگوريتمي و شبكه يك كامپيوتر آلوده شده را براي استفاده مهاجمان نابود مي-سازد. چنين سيستم آلوده شده‌اي معروف به بات (Robot)، زامبی (Zombieيا Drone) مي‌باشد و بطور پنهاني بر يك كامپيوتر متصل به اينترنت مسلط شده و آنگاه آن كامپيوتر را بمنظور شروع يا مديريت حملاتي مورد استفاده قرار مي‌دهد كه ردگيري آفريننده بات‌ها از آن كامپيوتر مشكل مي‌شود.

مجموعه بات‌ها اغلب قادر هستند كه به روش هماهنگ شده‌اي عمل نمايند؛ چنين مجموعه‌اي بنام بات شبكه يا Botnet نامگذاری شده است.

موارد استفاده از بات‌ها:

- حمله محروميت – از – خدمات توزيع شده (DDOS)
- هرزنامه پراكني
- ردگيري ترافيك
- ثبت كليدها
- پخش‌كردن بدافزار جديد
- نصب add-on تبليغاتي و اشياء كمكي مرورگر
- حمله‌كردن به شبكه‌هاي چت يا گپ دوستانه IRC
- دستكاری آراء و بازيهاي اينترنتي

جاسوس افزار و ثبت کلیدها

بطور معمول، كاربران نام كاربري و رمزعبور خود را براي عمليات بانكي، بازي و سايتهاي مربوطه از طريق كانال ارتباطي رمزگذاري شده مانند HTTPS يا POP3S ارسال مي‌كنند، كه اين كانالهاي ارتباطي اطلاعات كاربران را بوسيله بسته نظارتي شبكه محافظت مي‌كنند.

براي دور زدن آنها، يك مهاجم مي‌تواند يك ثبت‌كننده كليد نصب نمايد كه كليدهای فشار داده شده در يك كامپيوتر آلوده شده را بدست آورده و به او اجازه مي‌دهد كه اين اطلاعات حساس را مشاهده نمايد. از آنجائي كه نتيجه اينكار به مهاجم اجازه دريافت يك نسخه از كليه اسناد نوشتاري وارد شده در كامپيوتر قرلانی را مي‌دهد، ثبت‌كننده كليد بطور مشابه يك مكانيزم فيلترينگ را به اجرا در مي‌آورد كه تنها اطلاعات مطلوب برای موارد كليدی را بازگرداند (از قبيل نام كاربري يا رمزعبور و يا عبارتی مانند "Paypal.com").

*در جواب به استفاده از ثبت‌كننده كليد، برخي عمليات بانكي و ساير سايت‌ها استفاده از برنامه كاربردي گرافيكي براي وارد نمودن اطلاعات حساس، مانند رمز عبور، را جايگزين نموده‌اند. از آنجائي كه در اين برنامه از حروف نوشتاري توسط صفحه‌كليد استفاده نمي‌شود، لذا ثبت‌كننده كليدهاي سنتي نمي‌توانند اين اطلاعات را بدست آورند.

* برای مطالعه بیشترمیتوایند به کتاب Graphical User Authentication (GUA) به قلم دکتر آرش حبیبی لشکری و فرناز توحیدی مراجعه نمایید. (آدرس اینترنتی کتاب: http://www.amazon.com/Graphical-User-Authentication-GUA-Algorithms/dp/3843380724)

جعل صفحات اینترنتی و سرقت هویت

رویکرد دیگري که براي بدست آوردن نام کاربري و رمزعبور کاربر استفاده مي‌شود، عبارت است از ارسال يك آدرس اينترنتي يا همان URL متصل به يك سايت جعلي توسط هرزنامه، که اين سايت جعلي توسط مهاجم اداره مي‌گردد، و طوری طراحی شده است که صفحه اصلي يك بانك، بازي، يا سايتهاي مشابه را نمايش می‌دهد.

اين عمل بطور معمول از طريق پيامهائي انجام مي‌گردد که به کاربر پيشنهاد مي‌دهند لازم است جهت جلوگيري از بسته شدن حسابش عکس العمل فوري نشان داده و اين حرکت را تاييد نمايد.

اين عمل به نام حمله "جعل صفحات" يا Phishing معروف است، که با بهره برداري از مهندسي اجتماعي به قصد کسب اعتماد کاربر و با تغيير چهره و معرفی خود از يك منبع ارتباطي قابل اعتماد حاصل مي‌شود.

نوع خيلي خطرناك اين حمله را Spear-Phishing مي‌گويند. اين حمله باز هم يك هرزنامه است که ادعا مي‌کند از منبع قابل اطميناني فرستاده شده است. بهرحال، گيرندگان با دقت توسط مهاجم مورد تحقيق واقع شده‌اند، و هر هرزنامه بدقت تهيه شده تا مناسب استفاده آن کاربر باشد. همراه با آن، اغلب طيفي از اطلاعات ارسال مي‌گردد که خيال کاربر را از لحاظ صحيح بودن اعتبار راحت نمايد. اين حرکت بطور متنابهي احتمال جواب دادن گيرنده به آن هرزنامه، آنطور که دلخواه مهاجم است، را افزايش مي‌دهد.

درب مخفی و روت کیت

درب مخفی: يك درب مخفی يا Backdoor، كه گاهی درب تله يا Trapdoor نيز خوانده می‌شود، يك نقطه ورود مخفي به يك برنامه است كه اجازه مي‌دهد مهاجم يا هر شخصی كه از وجود اين درب آگاه باشد، بدون آنكه از روش‌هاي معمول دسترسي امنيتي استفاده نمايد، بتواند به آن برنامه دسترسي مستقيم داشته باشد.

در اصل يك درب مخفی بعنوان يك شبكه خدمات مجري ليست نمودن ورودیهاي غيراستانداردي برای رخنه به كامپيوتر است.

روت‌كيت‌ها: يك روت‌كيت در اصل دسته‌اي از برنامه‌ها است كه بر روي يك سيستم نصب شده تا دسترسي پنهاني به آن سيستم را در سطح مديرسيستم يا ريشه (Root) برقرار نمايند، ضمن اينكه شواهدی كه بر وجودش دلالت می‌كنند را تا بيشترين حد امكان از نظر مخفي نمايد.

يك روت‌كيت مي‌تواند بر اساس استفاده از ويژگي‌هاي زير دسته بندي شود:

پايدار: هر زمان كه سيستم راه اندازي شود آن هم شروع به فعاليت مي‌كند.

مستقر در حافظه: اين نوع كد ماندگار نيست و نمي‌تواند بعد از راه اندازي مجدد باقي بماند.

حالت خارجي: بدافزار در محلي خارج از حالت عملياتي معمول يك سيستم هدف قرار داده مي‌شود، بطور مثال در BIOS

مستقر در دستگاه مجازي: اين نوع روت‌كيت يك ماشين ناظر مجازي كم حجم و سبک نصب نموده و آنگاه سيستم عامل را در يک ماشين مجازی روی آن اجرا می‌نمايد.

اقدامات متقابل

پیشگیری: چهار عنصر اصلي پيشگيري را فهرست مي‌كند كه عبارتند از: خطمشي، هوشياري، كاهش آسيب پذيري، كاهش تهديد.

اگر پيشگيري موفقيت آميز نباشد:

كشف : هنگامي كه آودگي بوقوع بپيوندد، اين مكانيزم مشخص مي‌كند كه كامپيوتر آلوده شده و محل بدافزار را تعيين خواهد نمود.

شناسائي : هنگامي كه آلودگي كشف شده باشد، اين سيستم تعيين مي‌كند كه سيستم توسط چه بدافزار خاصي آلوده شده است.

حذف: هنگامي كه نوع خاص بدافزار شناسائي شده باشد، اين مكانيزم كليه آثار بدافزار را از سيستم آلوده شده طوري حذف مي‌كند كه نتواند در آينده بيشتر پخش شود.

اگر كشف موفقيت آميز باشد ولي شناسائي يا حذف غيرممكن باشد، آنگاه راه چاره جايگزين دور انداختن هركدام از فايلهاي آلوده يا بداندیش و نصب مجدد يك نسخه سالم است.

پويشگرهاي برپايه ميزبان

اولين محلي كه نرم افزار ضد ويروس از آن استفاده مي‌كند يک سيستم پايانی است. اين امر نه تنها به نرم افزار اجازه حداكثر دسترسي به اطلاعات مرتبط با رفتار بدافزاري كه با سيستم در ارتباط است را می‌دهد بلكه امكان بررسی كوچكترين فعاليتهای بدافزار روی اين سيستم را نيز ايجاد می‌نمايد.

بدافزارهاي اوليه از كدهاي ساده‌اي استفاده مي‌كردند كه بسهولت كشف مي‌شدند، و بهمين دليل مي-توانستند به آساني شناسائي شده و با استفاده از بسته‌هاي ضد ويروس ابتدايی، تصفيه شوند. همانطور كه مسابقه توليد بدافزار رشد نمود، در هر دو سمت، يعني كدنويسي بدافزار و لزوما نرم افزار سازي ضد ويروس خيلي بيشتر پيچيده و خبره شده‌اند.

چهار نسل از نرم افزارهاي ضد ويروس عبارتند از :

* **اولين نسل:** پويشگر ساده
* **دومين نسل:** پويشگر ابتكاري
* **سومين نسل:** تله‌هاي فعاليت
* **چهارمين نسل:** محافظت با خصيصه‌هاي كامل

چهار نسل پویشگرهای بدافزار

اولین نسل پويشگر نياز به امضاء بدافزار براي شناسائي آن داشت. اين امضاء ممكن است كه حاوي "Wildcarts" باشد ولي با بعضي ساختارهاي كامپيوتر بطور اساسي مطابقت نموده و اين ساختار صفات خود را در تمام نسخه‌هاي بدافزار بجا بگذارد. اين قبيل پويشگران اوليه، كه مخصوص بدافزارهاي داراي امضاء مشخص هستند، متاسفانه محدود به كشف بدافزارهاي شناخته شده هستند.

دومين نسل پويشگر بر روي امضاء مشخص بدافزار تمركز نمي‌كرد. بلكه بجاي آن، اين پويشگر از نقشهای اكتشافی جهت يافتن نمونه‌هاي بدافزار احتمالي استفاده مي‌برد. يك دسته از اين پويشگرها به دنبال پاره‌اي از كدها مي‌گشتند كه اغلب با بدافزار ممزوج مي‌شد. براي مثال، يك پويشگر ممكن است به دنبال ابتداي يك حلقه رمزگذاري بگردد كه توسط ويروسهاي چند ريختی استفاده شده است، و در آنجا كليد رمزگذاري را كشف نمايد.

سومين نسل برنامه‌ها عبارتند از برنامه‌های مقيم در برابر حافظه كه بدافزار را بوسيله فعاليتش بجاي ساختارش در يك برنامه آلوده‌شده شناسائي مي‌كنند. اين قبيل برنامه‌ها داراي اين امتياز هستند كه براي شناسائي بدافزار لزومي به وجود امضاء مشخصه و نقشهای اكتشافی گسترده بدافزار ندارند. بجاي آن، فقط لازم است كه گروه كوچكي از اعمالي كه دال بر كوشش برای انجام فعاليت‌هاي مضر بدافزار جهت خرابكاري در كامپيوتر هستند را شناسائي نموده و سپس وارد عمل شوند.

چهارمين نسل توليدات عبارت از بسته‌هائي است كه متشكل از انواع فنون ضدويروسها هستند كه در كنار هم استفاده مي‌شوند. اين بسته‌ها شامل تجهيزات پويش و تله برای فعاليتها مي‌باشند.

مبارزه موثر بر عليه بدافزارها

عموميت: رويكرد اتخاذ شده بايد قادر باشد كه از طيف وسيعي از حمله‌ها جلوگيري نمايد.

وقت شناسي: رويكرد اتخاذ شده بايد به سرعت جوابگو بوده تا تعداد برنامها يا سيستمهاي آلوده شده را محدود ساخته و فعاليت نتيجه بخشي را سامان دهد.

جهش: رويكرد اتخاذ شده بايد در مقابل فنون جهش و طفره رفتن كه توسط مهاجمان جهت اختفاي بدافزارشان استفاده مي‌شود، مقاوم باشد.

كمترين هزينه محروميت – از – خدمات :رويكرد مزبور بايد كمترين كاهش در ظرفيت يا خدمات را بعلت انجام اقدامات متقابل نرم افزاری نتيجه دهد، و نبايد گسيختگی قابل توجهي در عمليات معمول كامپيوتر ايجاد نمايد.

شفافيت: نرم افزار و شيوه اقدام متقابل نبايد نياز به انجام تغييرات در (legacy) سيستم عاملها، نرم افزارهاي كاربردي، و سخت افزار موجود داشته باشد.

پوشش محلي و جهاني: رويكرد اتخاذ شده بايد قادر باشد كه با منابع حمله چه از خارج و چه از داخل شبكه سازمان مقابله نمايد.

سوالات مرتبط

1. نقش فشرده سازی در عملکرد یک ویروس چیست؟
2. نقش رمزگذاری در عملکرد یک ویروس چیست؟
3. فازهای نمونه اجرای یک ویروس یا کرم چیستند؟
4. یک ویروس از چه مکانیزمهایی می‌تواند برای پنهان نمودن خود استفاده نماید؟
5. تفاوت بین ویروسهای قابل‌اجرای-ماشین و ماکرو در چیست؟
6. اینکه یک کرم می‌تواند به سیستم‌های راه دور برای انتشار دسترسی یابد، به چه معنی است؟
7. بمب منطقی چیست؟
8. فرق بین یک درب‌پشتی، یک بات، یک ثبت کننده صفحه کلید، جاسوس افزار و روت‌کیت در چیست؟ آیا همگی آنها می‌توانند در یک بدافزار ظاهر شوند؟
9. سطوح مختلفی که یک روت‌کیت می‌تواند در یک سیستم استفاده نماید را شرح دهید؟
10. چند عنصر مقابله با بدافزار را بیان نمایید؟
11. چهار نسل آنتی ویروسها را شرح دهید؟

خلاصه:

تعریف بدافزار ، انواع بدافزارها: بمب منطقی - اسب تروآ - درب پشتی - ویروس - کرم - خرگوش - جاسوس‌افزار - آگهی‌افزار - هیبرید ها ، dropperها ، و تهدیدهای مختلط - زامبی ها

ویروسها : بخشهای ویروس - فازهای ویروس - ساختمان ویروس - دسته بندی ویروس

کرمها : روشهای تکثیر کرم - الگوی تکثیر کرم - حالتهای فن آوری کرم

هرزنامه ها، تروجانها، باتها، جاسوس افزار و ثبت کلیدها، جعل صفحات اینترنتی و سرقت هویت، درب مخفی و روت کیت، اقدامات متقابل ، پویشگرهاي برپایه میزبان، مبارزه موثر بر علیه بدافزارها

جلسه بعدی: نفوذگرها

منابع:

کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها): دکتر آرش حبیبی لشکری، مهندس نسرین بدیع، مهندس فرنار توحیدی

ویروسها و بدافزارهای کامپیوتری: دکتر بابک بشری راد، دکتر آرش حبیبی لشکری

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.