

Keylogger

(کیلاگر، سارق اطلاعات کامپیوتر و موبایل)

www.ketab.ir

نویسنده:

احمد محمودی



شماره کتابشناسی ملی: ۲۶۸۹۱

قیمت: ۱۷۰۰۰ تومان

www.ketab.ir/pajo

حق چاپ و نشر محفوظ است.

طبق قانون حقوق نویسندگان و مصنفان هر گونه کپی برداری به هر روش پیگرد قانونی دارد.

305-1166 - 65924419

تهران: خیابان ۱۶ آذر شمالی، ساختمان بعثت، طبقه سوم

91611A511A - 332-2A-2 - 332192-2

اهواز: خیابان نادری شرقی، نبش، خیابان کرمی، خراط

فهرست

۱۳	مقدمه.....
۱۹	فصل اول: مبانی امنیت اطلاعات.....
۲۲	اهمیت امنیت اطلاعات و ایمن سازی کامپیوترها و تلفن های همراه.....
۲۲	داده های اطلاعات حساس در معرض تهدید.....
۲۳	انواع حملات و تهدیدات امنیتی.....
۲۴	ویروس ها.....
۲۵	برنامه های اسب تروا با توجه به دشمنانی در لباس دوست.....
۲۶	ویرانگران.....
۲۶	اشتراک های تحت ویندوز حفاظت نشده.....
۲۷	کدهای قابل انتقال (ActiveX , JavaScript Java).....
۲۷	اسکرپت های Cross-Site.....
۲۸	نامه های الکترونیکی ناخواسته.....
۲۸	ایمیل های جعلی.....
۲۹	ویروس های پیوست شده به ایمیل.....
۳۰	پسوندهای مخفی فایل.....
۳۱	سرویس گیرندگان چت.....
۳۱	شنود بسته های اطلاعات.....
۳۲	کلاهبرداری (ابتدا جلب اعتماد و سپس تهاجم).....
۳۲	ابزارهای امنیتی.....
۳۳	نرم افزارهای آنتی ویروس.....
۳۳	سیاست های امنیتی.....

۳۴		رمزهای عبور
۳۵		فایروال ها
۳۵		رمزنگاری
۳۵		گرفتن فایل پشتیبان بطور منظم از اطلاعات ارزشمند موجود در کامپیوتر
۳۵		بهنگام سازی نرم افزارها
۳۶		ارزیابی امنیتی کامپیوتر
۳۶		غیر فعال نمودن ارتباط با اینترنت در زمان عدم استفاده
۳۶		چگونه که هر در معرض هک قرار بگیرید
۳۶		ایمیل
۳۷		اماکن و سایت های عمومی
۳۷		ساخت پسورد مناسب
۳۷		فصل دوم: حمله کنندگان به کامپیوتر
۴۲		هکر (ضربه زن) کیست؟
۴۲		انواع مختلف هکرها و نوع کارهایشان
۴۲		هکهای کلاه سفید (Hacker)
۴۳		هکهای کلاه سیاه - واکر
۴۳		قفل باز کن یا کراکر
۴۴		پراکر
۴۴		هکهای جوان
۴۵		Preaker
۴۵		تاریخچه هک از آغاز تا کنون
۵۲		بزرگترین هکر جهان
۵۳		شناخته شده ترین هکهای جهان
۵۵		فصل سوم: انواع حملات در شبکه های کامپیوتری
۵۸		انواع حملات در شبکه
۵۹		حملات از نوع DoS

حملات از نوع Back door..... ۶۴

فصل چهارم: کیلاگر (واقعہ نگار) چیست؟..... ۶۷

کیلاگر چیست؟..... ۷۱

قابلیت های کیلاگرها..... ۷۳

انواع کیلاگر (واقعہ نگار)..... ۷۳

کاربردهای کیلاگر..... ۷۵

فصل پنجم: کیلاگر سخت افزاری..... ۸۱

کیلاگر سخت افزاری (USB KeyLogger)..... ۸۱

کیلاگر سخت افزاری، به شکل مبدل یا دوطرف PS2..... ۸۲

روش کار کیلاگرهای سخت افزاری..... ۸۳

روش ساخت کیلاگر سخت افزاری..... ۸۵

فصل ششم: روش کار کیلاگر نرم افزاری..... ۹۱

نرم افزارهای معروف هک..... ۹۳

کیلاگرهای نرم افزاری..... ۹۴

کد برنامه کیلاگر در محیط C++..... ۹۷

فصل هفتم: شناسایی و مبارزه با کیلاگرها (Anti keylogger)..... ۹۹

روش های مقابله..... ۱۰۱

مواردی که به کاربران کامپیوترهای متصل به شبکه و مدیران سیستم توصیه می شود..... ۱۰۹

پیشنهادهایی برای شناسایی کیلاگرها..... ۱۱۰

فصل هشتم: امنیت و حفاظت فیزیکی از کامپیوترهای شخصی..... ۱۱۷

۲۷ راه کار استاندارد در حفاظت فیزیکی از کامپیوترهای شخصی..... ۱۱۷

۱- اتصال به شبکه امن..... ۱۱۷

۲- فعال سازی فایروال و پیکربندی آن..... ۱۱۹

۳- نصب و استفاده از آنتی ویروس و آنتی اسپیم..... ۱۱۹

- ۴- حذف برنامه‌های غیرضروری..... ۱۲۰
- ۵- غیرفعال کردن سرویس‌های غیرضروری..... ۱۲۰
- ۶- تغییر ویژگی‌های پیش‌فرض غیرضروری..... ۱۲۱
- ۷- انجام کارها با توجه به اصل حداقل حق دسترسی..... ۱۲۱
- ۸- امن کردن مرورگر وب..... ۱۲۱
- ۹- اعمال به‌روز رسانی‌های نرم‌افزارها و فعال کردن قابلیت به‌روز رسانی‌های خودکار در آینده..... ۱۲۲
- ۱۰- مدیریت خالت‌ها..... ۱۲۳
- ۱۱- استفاده از سیستم عامل به روز و اصل..... ۱۲۴
- ۱۲- استفاده از نرم‌افزارهای امنیتی و به‌روز رسانی مداوم آن‌ها..... ۱۲۴
- ۱۳- عدم استفاده از رایانه‌های دیگران و یا رایانه‌های عمومی برای کارهای شخصی..... ۱۲۶
- ۱۴- عدم به اشتراک گذاشتن رمز عبور..... ۱۲۶
- ۱۵- اطمینان از صحیح بودن تاریخ سیستم..... ۱۲۶
- ۱۶- به‌روز رسانی دائمی درایورهای سخت‌افزار..... ۱۲۷
- ۱۷- به‌روز رسانی نرم‌افزارهای جانبی..... ۱۲۷
- ۱۸- عدم بهره‌گیری از نرم‌افزارهای کرک شده..... ۱۲۷
- ۱۹- عدم ورود به سایت‌های ناشناس..... ۱۲۸
- محافظةت از رایانه در برابر نفوذ با استفاده از دیواره آتش..... ۱۲۹
- ۲۰- عدم اشتراک منابع رایانه با افراد غریبه..... ۱۳۰
- ۲۱- سیستم عامل‌تان را پیچ شده نگهدارید..... ۱۳۰
- ۲۲- از ویندوز ایکس پی، دست بکشید..... ۱۳۰
- ۲۳- اپلیکیشن هایتان را پیچ شده نگهدارید..... ۱۳۱
- ۲۴- به نرم افزار های بد سابقه اعتماد نکنید..... ۱۳۲
- ۲۵- نام درایو D سیستم‌تان را تغییر دهید..... ۱۳۴
- ۲۶- از یک آنتی ویروس قابل اعتماد استفاده کنید..... ۱۳۴
- ۲۷- از اطلاعات شخصی مهمتان (اسناد، نامه ها، تصاویر و غیره) نسخه پشتیبان تهیه کنید..... ۱۳۵

فصل نهم: نقش عوامل انسانی در امنیت شبکه های کامپیوتری	۱۳۷
اشتباهات متداول مدیران سیستم	۱۴۱
اشتباهات متداول کاربران معمولی	۱۵۰
فصل دهم: نتیجه گیری	۱۵۷
اهمیت امنیت اطلاعات و ایمن سازی کامپیوترها	۱۵۷
داده ها و اطلاعات حساس در معرض تهدید	۱۵۷
منابع و مآخذ	۱۵۹
ضمائم	۱۶۳
ضمیمه ۱	۱۶۵
ضمیمه ۲	۱۷۱

اگر در حوزه امنیت کمی فعال باشید احتمالاً بارها واژه کیلاگر را شنیده اید کیلاگر برنامه ای است که به جمع آوری کلیدهای فشرده شده توسط شما مشغول است. تمام کلیدهایی را که شما می‌فشارید توسط این برنامه ذخیره شده و برای نویسنده برنامه به آدرس خاصی ارسال میشوند و برنامه نویسان این بدافزارها شروع به جمع آوری اطلاعات می‌کنند در میان این اطلاعات، نام‌های کاربری و رمزهای عبور با ارزش شما نیز وجود دارد نام‌های کاربری و کلمات عبور مربوط به اکانت‌های شما در سایت‌های مختلف. مطمئناً شما دوست ندارید که این اطلاعات با ارزش به دست دیگران برسد و آن‌ها از این اطلاعات گران‌بها سوء استفاده کنند ولی متأسفانه بدون اینکه بوجتان خبر داشته باشد با کیلاگر اطلاعات شخصی و مفیدی به یک هکر داده اید. ولی حالا باید اندیشید و راهکارهای مبارزه با اینگونه بدافزارها را پیدا کرد در اینجا به بررسی این بدافزار، انواع مختلف آن و راه‌های مقابله با آن خواهیم پرداخت.

تحقیقات نشان داده که کاربران ایرانی خیلی کم به امنیت رایانه هایشان اهمیت میدهند.

امنیت اطلاعات^۱ یعنی حفاظت از اطلاعات و سیستم‌های اطلاعاتی از فعالیت غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، جعل، نسخه برداری یا ضبط، خراب کردن، تغییر و دستکاری.

واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن، گاهی به اشتباه به جای هم بکاربرده می‌شود. اگر چه این‌ها موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و

قابل دسترس بودن را دارند ولی تفاوت های ظریفی بین آنها وجود دارد. این تفاوت ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش های استفاده شده برای حل مسئله و موضوعاتی که تمرکز کرده اند دارد.

امنیت کامپیوتر و موبایل در حصول اطمینان از در دسترس بودن و عملکرد صحیح سیستم کامپیوتری تمرکز دارد که بدون نگرانی از اطلاعاتی که توسط این سیستم کامپیوتری ذخیره یا پردازش می شود استفاده شود. برای افراد، امنیت اطلاعات تاثیر معنی داری بر حریم خصوصی دارد. البته در فرهنگ های مختلف این مفهوم تفسیرهای متفاوتی دارد.

ما در عصر دیجیتال زندگی می کنیم؛ آنقدر در زندگی های دیجیتالی مان غرق شده ایم که اگر یک روز اینترنت و گجت هایمان (تلفن همراه و تجهیزات سخت افزاری کوچک کمکی مثل کنترل هوا، کاره) را از ما بگیرند، احساس ناامیدی و یأس خواهیم کرد. پیداست که در دنیای دیجیتال، تنها سرعت و ارتباطات فوق العاده نیست که نصیبمان می شود. گاهی نیز ویروس ها، تروجان ها، نقایص امنیتی و غیره باعث می شوند که اطلاعاتمان از دست برود. بدتر این که: اطلاعاتمان را به دست افرادی می رسانند که هرگز نباید به آنها دسترسی پیدا می کردند. در این کتاب می خواهیم راه هایی را به شما معرفی کنیم تا بتوانید پرسی ها و تلفن های همراهتان را هر چه بهتر کنترل نمایید و از کدهای مخرب و مداخله خلاص شوید.

مطمئناً استفاده از برنامه های قابل اعتماد و معتبر و داشتن نرم افزارهای امنیتی مناسب (آنتی ویروس و...) شما را بسیار در حفظ امنیتتان یاری خواهد داد. اما این ها برای تأمین کامل امنیت شما کافی نخواهد بود. باید بدانید که راه های بسیار

زیادی برای نفوذ غیر مجاز به کامپیوتر و تلفن های همراهتان وجود دارد. شاید بگویید: "اگر مساله به این حد حساس بود، آنگاه محال بود که سیستم عامل من بتواند حتی یک ماه بدون ویروس باشد!" اما دقیقاً، نقطه اشتباهتان همین جاست: در ویندوز 10 که جدید ترین و امن ترین ویندوز کامپیوترهای شخصی است؛ با آپدیت روزانه‌ی ویندوز و آنتی ویروس و استفاده از برنامه‌های قابل اعتماد و با وجود User Account Control و فایروال و بسیاری چیز های دیگر؛ شما باز هم بعد از مدتی ممکن است به بدافزار آلوده شوید.

بسیار است اطلاعات در سال های اخیر به میزان قابل توجهی رشد کرده است و تکامل یافته است. راه های بسیاری برای ورود به این حوزه کاری به عنوان یک حرفه وجود دارد. موفقات تخصصی گوناگونی وجود دارد از جمله: تامین امنیت شبکه (ها) و زیرساخت ها، تامین امنیت برنامه‌های کاربردی و پایگاه داده ها، تست امنیت، حسابرسی و بررسی سیستم های اطلاعاتی، برنامه ریزی تداوم تجارت و بررسی جرائم الکترونیکی، و غیره.

استفاده اشخاص از رایانه و تلفن های همراه در کارهای روزمره رو به رشد است. به طور مثال برای کارهای بانکی خرید و فروش و برقراری ارتباط با دوستان و فامیل استفاده می‌شود. به دلیل نقش کلیدی رایانه و تلفن های همراه در زندگی روزمره و با توجه به داشتن اطلاعات شخص در آن، امنیت رایانه‌های شخصی و تلفن های همراه دارای اهمیت است.

مهاجمان می‌توانند رایانه و تلفن های همراه را با استفاده از یک نرم افزار مخرب یا بدافزار یا استفاده از یک رخنه امنیتی آلوده کنند. پس از آلوده شدن رایانه، مهاجمان قادر به دسترسی به اطلاعات رایانه بدون اطلاع ما هستند. آن‌ها می‌توانند

اطلاعات را سرقت کنند، پیکربندی رایانه را تغییر دهند یا حتی بدافزاری را روی رایانه نصب کنند.

جالب است بدانید که محققان آمریکایی توانسته اند اطلاعات درون مغز انسان را هک کرده و قدرت تصمیم گیری و استخراج اطلاعات درون مغز انسان را در دست بگیرند. پس از هم اکنون باید فکری برای امنیت اطلاعات درون مغز انسان نیز بکنیم.

امنیت کامپیوتر، شاخه ای از فناوری و معروف به امنیت اطلاعات و سیستم های اطلاعات از جنبه دسترسی غیر مجاز، استفاده، انتشار، اختلال، اصلاح یا تخریب از جنبه های فیزیکی و منطقی است.

امنیت کامپیوترهای شخصی و موبایل به دو جنبه کلی امنیت فیزیکی و نرم افزاری تقسیم بندی می گردند.

امنیت فیزیکی شامل مواردی از قبیل امنیت، شرایط نامساعد جوی، حوادث غیرمترقبه و سایر خطرات فیزیکی می گردد. در حالی که امنیت نرم افزاری می تواند جنبه های گسترده تری را شامل گردد که از مهم ترین آن ها می توان به حملات فیشینگ، نفوذ هکرها، نرم افزارهای تبهکارانه، حملات DOS و.... اشاره نمود.

باید توجه کنید که هر سیستم کامپیوتری (به عبارت بهتر هر سیستم عامل از dos تا آندروید در تلفن همراه) محصول کار تعدادی انسان است و حتما دارای تعدادی باگ^۱ (خطاهایی که بعد از ارائه محصول به بازار به تدریج کشف میشوند) خواهد بود. بعد از اینکه یک باگ مشخص شد، شرکت ها، نرم افزارهایی را به سرعت (در عرض چند ساعت) ایجاد می کنند تا مشکل رفع شود این ها را پچ^۲

(وصله کردن) می گویند و بعد مدیران شبکه^۱ در عرض چند روز تا چند سال آن‌ها را بارگذاری^۲ کرده و مشکل را حل میکنند.

با توجه به جایگاه داده در عصر حاضر و لزوم نگاه جامع به این مقوله مهم، بر آن شدم تا در زمینه امنیت درسیستم های کامپیوتری و کیلاگراها که علی رقم خطرناک بودن آن حتی بیش از ویروس ها و عدم آشنایی عموم با آن، کتاب مذکور را انتشار دهم. از این رو نتیجه تحقیق و ارایه کتاب زیر را در باب کیلاگراها که گونه ای از تروجان ها هستند خدمتتان ارایه می دهم. باشد گام هر چند کوچک در راه پیشرفت علمی هم وطنان عزیز و مخاطبان محترم بخصوص علاقه مندان علم رایانه ارایه شده باشم.

www.ketab.ir