

مختار، محمدحسین، ۱۳۵۶ -
مرجع کامل ویروسهای کامپیوتری: شناسایی و راههای مقابله با آن /
مؤلف محمدحسین مختار. - تهران: زند، ۱۳۸۳.
۲۹۲ ص.: مصور، جدول.

ISBN: 964-6118-67-4: ریال ۱۷۰۰۰

فهرستنویسی براساس اطلاعات فیبا.

۱. ویروسهای کامپیوتری. الف. عنوان.

۵/۸۴

۹۳/۷۶/۷۶ QA

۸۳-۳۸۱۱۴ م

کتابخانه ملی ایران

مرجع کامل ویروسهای کامپیوتری
مؤلف: مهندس سید محمد حسین مختار
ناشر: انتشارات زند

چاپ: جبباری

صحافی: هدیه

تیراژ: ۳۰۰۰ جلد

نوبت چاپ: اول تابستان ۸۴

ریال ۱۸۰۰۰

مرکز بخش: تهران - ضلع جنوب شرقی میدان انقلاب

پلاک ۱۵۲۶ کتابسرای پارسیان ۶۴۹۷۹۰۶

۰۹۱۲۳۱۱۵۶۸۹

بسمه تعالی

حمد و سپاس ایزدمنان را که با الطاف بیکران خود این توفیق را به من ارزانی داشت تا بتوانم در راه ارتقای دانش عمومی به ویژه علوم کامپیوتر و انفورماتیک گامهایی هرچند کوچک برداشته و در انجام رسالتی که برعهده داشتم مؤثر واقع شوم.

در نیمه دوم قرن بیستم شاهد انقلابی عظیم در عرصه پیشرفت علم و صنعت بوده است ظهور و تکامل کامپیوتر و تأثیر روز افزون آن در علوم، فنون، صنایع، آموزش، کار، تجارت و زندگی روزمره باعث تحولات علمی، اجتماعی و فرهنگی گسترده ای شده است.

از سال ۱۹۸۷ تاکنون هر روز بیش از روزهای پیش کامپیوترها و عملکرد آنها در معرض خطر قرار می گیرد عده ای بنابر دلایلی اطلاعات در حال تبادل را سرقت برده و از آنها در راه غیر قانونی استفاده می کنند. این کتاب مجموعه ای مختصر از نحوه عملکرد هکرها و ویروس ها و راه های مبارزه با آنهاست. با پیشرفت تکنولوژی اطلاعات از طریق شبکه اینترنت و یا هر شبکه داخلی دیگر مبادله می شود اما واقعاً این اطلاعات تغییر نیافته به مقصد می رسند؟

اطلاعاتی که اگر بدست افراد خراب کار بیافتد ممکن است جان هزاران انسان بی گناه را بگیرد و یا خساراتی وارد کند که تا مدت ها یک کشور یا دنیا به خواب رود.

برای علاقمندان به ویروس و برنامه نویسی تحت جاوا، چند سرویس ویروس در این کتاب گردآوری کرده ام. محتوای این کتاب صرفاً برای دفاع از شبکه و کامپیوتر های شخصی می باشد.

امنیت دردنیای واقعی ما امری است اجتناب ناپذیر و همگی ما به نوعی سومی می کنیم تا امنیت را در محیط خود پیاده سازی نماییم. در نهایت از کسانی که مرا در نوشتن و چاپ این کتاب یاری کرده اند تشکر می کنم به خصوص خانواده های جادری و خدایاری و مدیر و مسئول بخش توسعه کتاب ایران فرهنگ محمد علی عزیزی که مرا همیشه پشتیبانی کرده است.

باتشکر

سید محمد حسین مختار

بسمه تعالی

«(امور) می‌تواند در متارهایی عصر از فعالیت‌ها را انجام دهنده (باشد)»
شرکت بخش و توسعه کتاب ایران فرهنگ ، باهدف گسترش فرهنگ
کتاب و کتابخوانی و آشنایی دانش پژوهان با آخرین تحولات و کاربردهای
نوین فناوری اطلاعات برگزار می‌کند.

کلینیک کامپیوتری ایران فرهنگ ، مرکز آفرینش انواع کتابهای کامپیوتری
از تمامی مهندسين، مؤلف و مترجمين و همچنین مربیان محترم
آموزشگاههای کشور که مایل به ارائه علوم کامپیوتری در زمینه‌های
مختلف هستند، رسماً دعوت به همکاری می‌نماید.

ضمناً از تمامی عزیزانی که مایل به ارائه راهنمای کتب دانشگاهی
هستند نیز دعوت به همکاری می‌گردد تا پس از بررسیهای لازم در بازار
عرضه گردد.

در پایان از تمام عزیزانی که ما را در تهیه این اتریاری نمودند خصوصاً آقای
سید محمد حسینی مختار (مؤلف)، سرکار خانم یازوکی مدیریت محترم
(مرکز فوریتهای تأییدی مهرگان) کمال احترام و سپاسگذاری را دارم و
امید آنکه در تمامی امور زندگی موفق و مؤید باشند.

انشاء الله

و من الله توفیق

مدیر و مسئول بخش کتاب ایران فرهنگ: محمدعلی عزیزی

فهرست مطالب

معاون

۱۸ فصل اول

توانایی تشخیص و از بین بردن ویروس های کامپیوتری
چرا انسان ها خالق ویروس های کامپیوتری می گردند؟
انگیزه ایجاد ویروس های کامپیوتری
ویروسها بخش از صنعت IT فن آوری اطلاعات هستند
تاریخچه ویروسهای کامپیوتری
اهمیت پرداختن به ویروس های کامپیوتری

۳۶ فصل دوم

آشنایی با ویروسهای کامپیوتری
توانایی تشخیص و از بین بردن ویروسهای کامپیوتری
وجه تشبیه ویروس
تعریف ویروس
ویروس چه ویژگیهایی باید داشته باشد
نحوه تکثیر
روش راه یابی ویروس به سیستم

۴۴ فصل سوم

انواع ویروس ها از نظر محل تاثیر گذاری ویروس

رکورد راه اندازی

ویروس های تاثیر گذار روی Boot sector

ویروس های تاثیر گذار روی جدول Partition دیسک

ویروس های تاثیر گذار روی فایل های اجرایی

۵۰

فصل چهارم.....

انواع ویروس ها

ویروس های آلوده کننده پرونده

نمونه ای از ویروس ها

Data crime

Jerusalem

ویروس های آلوده کننده سکتور راه انداز و سکتور پارتیشن

ویروس های ماندگار در حافظه

، ویروس های نوین

ویروس های چند ریختی

ویروس های ناپیدا

ویروس های هوشمند

جهت ایمنی در کار و عدم ورود ویروس به کامپیوتر

بمب های منطقی

۵۸

فصل پنجم.....

طبقه بندی جدید ویروس ها

خسارت ناشی از ویروس ها

مراحل زندگی ویروس ها

One half

ویروس MBR

ویروس ماکرو

ویروس های ترکیبی

ویروسهای فایل

ویروسهای رونویسی کننده

ویروس های همراه

ویروسهای پست دهنده

ویروسهای ابتدا قرار گیرنده

ویروس های داخل شونده

ویروسهای اسکریپتی

ویروسهای مقیم در حافظه

ویروسهای پست الکترونیکی

Hoax ویروسهای

۷۲

فصل هفتم.....

کرمها (Worms)

اسب های تروا (Trojans)

رایج ترین اسب ها ی تروا

Sub>

Back orifice 2000

Tridia vnc

ساختار اسب های تروا

اتفاقات نامعلومی که توسط یک Trojan بر روی یک

کامپیوتر پدیدار می گردد.

مشهور ترین و مهمترین اسب های تروای دنیای وب

تهدید ای آتی

Root king های معمولی

Root kit ها و خرابکاری آنها

مجموعه اسب های تروای Root kit ها

کشیف ترین نوع Root kit ها
 مخفی کردن فایلها در Root kit ها
 مخفی کردن پروسه
 مخفی کردن پورتهای ارتباطی
 پیاده سازی Root kit های سطح هسته

فصل هشتم ۱۰۸

ویروسها

Form

One half

Apadana

Anti cmos

WM/Appdar

Arya

Die hard

W/32 fun love

Kon KOOR

Nice fox

Win32/cih

WM/CAP

حملات DOS

انواع حملات DOS

حملات DOS از بیرون

ویروس EDWIN

بررسی برنامه ویروس جایگزین partition Table

ویروس IDIE

استخراج ویروس از فایل

فصل نهم ۱۳۴

زبانهای برنامه نویسی

زبان سطح پایین

زبان ماشین

زبان اسمبلی

زبان های سطح بالا

زبان

زبان ویژوال بیسیک

زبان جاوا

زبانهای اسکریپت

مفاهیم برنامه نویسی

اسکریپت موزیانه خدمات گیرنده

دسترسی به اسکریپتهای مزاحم

PHP

ASP

VBS

Perl

ویروسها و کرم ها

مثال کد ویروس

۱۵۰ فصل دوم

اشتراک شبکه

حفاظت کلمه عبور اشتراک ها در ویندوز ME/98/95

حذف اشتراک در ویندوز ME /98/95

حذف اشتراک در ویندوز XP/2000/NT

ابزارهای ملی شبکه

MS-DOS

Net stat

Ping

نصب در ویندوز ME/98/95

ابزار Tracert

ابزار NBTSTAT

ابزار Net view

ابزار net ase

کریک pass vword

تفاوت بین فایل‌های EXE.com

مراحل اجرای برنامه com

مراحل اجرای برنامه EXE

قطعه پیشوند برنامه PSP

سرآمد فایل Header

معرفی FCB ساده

معرفی FCB پیشرفته

بررسی ساختار FCB پیشرفته

ناحیه انتقال داده‌ها DATA

بلوک کنترل حافظه

بلوک محیط برنامه

معرفی Partiton table

معرفی Boot sector

فرمول محاسبه ظرفیت یک partion

اسکلت بوت سکتور

نمای فیزیکی دیسک از نظر DOS

محل ذخیره داده‌ها DATA

معرفی CMOS

فصل هشتم ۱۷۸

نحوه تشخیص ویروسی شدن سیستم

پیغام Program big to file in memory

کند شدن سیستم

ایجاد اشکال در راه اندازی سیستم

راه های مقابله با ویروسی شدن سیستم

جلوگیری از ورود ویروس ها به سیستم

از بین بردن ویروسها پس از ورود به سیستم

ویروس بابهای کامپیوتری

طرز ساختن دیسک سیستم

فصل پانزدهم ۱۸۶

ویروس های شبکه اینترنت

کرم موربسی

Miche langeli

Word concept

Wazza

ملیا

چرنوبیل

Explor zip

Bubble boy

Love boy

فصل شانزدهم ۱۹۰

نحوه کار با تعدادی از ویروس یابها

MSAV

VSAFE

خلاصه امکانات VSAFE.com

خارج ساختن VSAFE از حافظه

ویروس یاب Scan Disk

آنتی ویروس Dr.Soioman

برنامه Toolkit

چگونگی حذف یک ویروس سکتور راه اندازی از یک فلاپی

دیسک

متنوی Advanced در ویروس یاب Toolkit

متنوی Net Work در ویروس یاب Toolkit

فایل های فشرده آرشیوی

چگونگی حفاظت از هارد دیسک

چگونگی حفاظت از LAN شبکه

۲۲۸

فصل سیزدهم

ویروس های پنهان

روش های جلوگیری و مبارزه با این نوع ویروس ها

شرح دستورات و برنامه های موجود در فهرست Toolkit

برنامه Author.com

برنامه های certify.com, cert.EXE

برنامه Cleanboo.EXE

برنامه Clean par.EXE

برنامه Defer bat.EXE

برنامه های Defin key.com, Deferkey.com

برنامه Find Vira.EXE

سوییچ های برنامه

برنامه Guard.com

برنامه Tkutl.EXE

برنامه VGPOPUP.EXE

فایلهای پردازش دسته ای

۲۳۸

فصل چهاردهم

مجموعه نرم افزار Norton utilities

راه اندازی برنامه های Norton utilities

وظایف بهینه سازی عملکرد سیستم

وظایف یافتن و رفع مشکلات موجود در سیستم

Norton system Doctor

اجرای نرم افزار Un Erase wizard

اجرای نرم افزار Norton Disk Doctor

اجرای نرم افزار Norton win Doctor

اجرای نرم افزار Norton system check

وظایف نگهداری سیستم

اجرای نرم افزار System Information

نرم افزار ویروس کش Norton Antivirus 2002

ویژگیهای برجسته نرم افزار Norton Antivirus

شروع به کار نرم افزار Norton Antivirus

گزینه Auto-protect

گزینه E-mail scanning

دکمه Confidential info

عبارت Ad Blocks

دسترسی به گزینه های Internet security

۲۷۰ فصل هفدهم.....

هک کردن سایت شما

پیش بینی انواع مختلف هجوم

هجومهای رد سرویس

انواع هجوم های DOS

هجومهای نشت اطلاعات

تهاجمهای دسترسی به فایل

تهاجمات اطلاعات غلط

هجومهای دسترسی به فایل / بانک اطلاعات ویژه
انجام یک آنالیز خطر در سایت شما
تعیین سرمایه های شما
تست آسیب پذیریهای سایت شما
تعیین تکنیک آزمایشی
آیا تکنیکهای مخفی سازی ارزشی دارد؟
گزینه های Full system scan
گزینه virus Definitions
گزینه Subscription service
گزینه Automatic Live data
برنامه ریزی عملیات اسکن ویروس یابی
گزارش گیری از نرم افزار Norton Antivirus
گزینه Quarantine item
گزینه On line virus Encyclopedia
گزینه Activity log
گزینه virus list
نرم افزار Norton Internet security
گزینه Statas
گزینه Secarity
گزینه Privacy
تحقیق در مورد آسیب پذیری های شما
اجیر کردن یک تیم تست نفوذ