به نام خدا

حملات سایبری هدفمند

حملات چند مرحله ای با استفاده از کدهای مخرب

(همراه با بررسی تخصصی حمله استاکس نت)

مولفان:

Adiya K Sood-Richard Enbody-Nicolas Falliere-Liam O Murchu-Eric Chien

مترجم:

مهندس محسن فردوست

مؤسسه فرهنگی هنری دیباگران تهران

◂ عنوان کتاب: **حملات سایبری هدفمند**

حملات چند مرحله ای با استفاده از کدهای مخرب(همراه با بررسی تخصصی حمله استاکس نت)

◂ مولفان : Adiya K Sood-Richard Enbody-Nicolas Falliere-Liam O Murchu-Eric Chien

◂ مترجم : محسن فردوست

◂ ناشر: موسسه فرهنگی هنری دیباگران تهران

◂صفحه آرایی: نازنین نصیری

◂طراح جلد:داریوش فرسایی

◂ نوبت چاپ: دوم

◂ تاریخ نشر: ۱۴۰۲

◂ چاپ و صحافی:صدف

◂ تیراژ:۱۰۰ جلد

◂ قیمت:۲۸۰۰۰۰۰ ریال

◂ شابک: ۲-۳۸۸-۲۱۸-۶۲۲-۹۷۸

نشانی واحد فروش: تهران، خیابان انقلاب، خ دانشگاه- تقاطع شهدای ژاندارمری -ساختمان اداری دانشگاه- طبقه دوم-واحد۴ تلفن: ۶۶۹۶۵۷۴۹-۲۲۰۸۵۱۱۱

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

www.dibbook.ir

نشانی تلگرام:mftbook@

نشانی اینستاگرام دیبا dibagaran_publishing

سرشناسه:سود، آدیتیا کی. Sood,Aditya K

عنوان و نام پدیدآور:حملات سایبری هدفمند:حملات چند مرحله ای با استفاده از کدهای مخرب...

مولفان:[آدیتیاکی سود] ؛مترجم: محسن فردوست.

مشخصات نشر: تهران : دیباگران تهران ،۱۳۹۹

مشخصات ظاهری:۳۰۲ص.مصور.

شابک: ۲-۳۸۸-۲۱۸-۶۲۲-۹۷۸

وضعیت فهرست نویسی: فیپا

یادداشت : عنوان اصلی : Targeted cyber attacks:multi-staged attacks driven by exploits and malware,2014.

عنوان دیگر: حملات چند مرحله ای با استفاده از کدهای مخرب....

موضوع:شبکه های کامپیوتری-تدابیر ایمنی

موضوع:computer networks-security measures

موضوع:فضای مجازی-تدابیر ایمنی

موضوع:cyberspace-security measures

موضوع:جرایم کامپیوتری-پیشگیری

موضوع: computer crimes-prevention

شناسه افزوده: ریچارد، انبادی Richard,Enbody

شناسه افزوده:فردوست، محسن، ۱۳۶۰- مترجم

رده بندی کنگره:۵۱۰۵/۵۹ TK

رده بندی دیویی:۰۰۵/۸

شماره کتابشناسی ملی:۷۳۹۵۶۰۰

هرکتاب دیباگران ،یک فرصت جدید شغلی.

هرگوشی همراه،یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای دیباگران،در هر جای ایران به کتابهای ما دسترسی دارید.

فهرست مطالب

فصل پنجم: مکانیزم‌های استخراج داده‌ها

فصل ششم: حفظ کنترل و حرکت جانبی

فصل هفتم: چرا حملات سایبری هدفمند به راحتی انجام می‌شوند؟

فصل هشتم: چالش‌ها و اقدامات متقابل

فصل نهم: نتیجه‌گیری

بخش دوم کتاب: بررسی و تحلیل کرم Stuxnet

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی است که بتواند
خواسته های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت **"جناب آقای محسن فردوست"** و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
bookmarket@mft.info

تقدیم به مادرم

مقدمه مترجم

امنیت اطلاعات امروزه یکی از مهم‌ترین دغدغه‌های سازمان‌ها و صنایع و مراکز دولتی است. نرم‌افزارهایی که این امنیت را به خطر می‌اندازند بدافزار نام دارند که بر حسب کارکردشان به انواع مختلفی تقسیم می‌شوند. زمانی که از این بدافزار یا سایر ابزارهای مفید یا مضر فناوری‌اطلاعات جهت حمله به کامپیوترها، داده‌ها، شبکه‌ها یا هر نوع زیرساختی استفاده می‌شود حمله سایبری نامیده می‌شود. حملات سایبری هدفمند، حملاتی اختصاصی هستند که علیه یک شخص خاص، شرکت یا سازمان برای دستیابی به داده‌های حیاتی یا اختلال در سیستم‌های کامپیوتری آن‌ها در اختفای کامل صورت می‌پذیرد. حملات هدفمند با حملات سایبری معمولی و تصادفی که گروه‌های مختلف و گسترده‌ای از کاربران را تحت تاثیر قرار می‌دهند متفاوت هستند. حمله سایبری هدفمند معمولا از پنج مرحله مختلف جمع‌آوری اطلاعات، آلوده کردن هدف، بهره‌برداری از سیستم، استخراج داده‌ها و مرحله کنترل و نگهداری اطلاعات تشکیل‌شده است. حمله سایبری استاکس‌نت که ناشی از کرم استاکس‌نت بود نمونه بارزی از حمله سایبری هدفمند است. هدف اصلی حمله استاکس‌نت سیستم‌های کنترل صنعتی بوده است که این کار را با آلوده کردن کنترلرهای منطقی قابل‌برنامه‌ریزی در سیستم‌های کنترل صنعتی انجام می‌دهد. استاکس‌نت، اولین کرمی است که از چهار آسیب‌پذیری روز–صفر سواستفاده کرده است. این کرم اعتبار دو گواهینامه دیجیتال را به خطر می‌اندازد و کدهای مخربی را به سیستم‌های کنترل صنعتی تزریق می‌کند و این در حالی است که این کدهای مخرب را از دید اپراتور پنهان می‌کند. این کرم به خصوص بانفوذ در سایت اتمی نطنز و با آلوده کردن و تغییر پارامتر کنترلرهای سانتریفیوژها، باعث ازکارافتادن آن‌ها شد که باتوجه‌به نحوه انتقال و پخش، نحوه عملکرد و برنامه‌ریزی خودکار و باتوجه‌به نحوه کدنویسی‌اش پیچیده‌ترین و هوشمندترین بدافزار محسوب می‌شود. این کتاب به بررسی حملات سایبری هدفمند می‌پردازد و تحلیل جامع و کاملی از نحوه عملکرد کرم استاکس‌نت را که توسط شرکت امنیتی سمنتک انجام شده است ارایه می‌دهد.

محسن فردوست

Fardoust.ir@gmail.com

دیدگاه‌های مختلف درباره کتاب «حملات سایبری هدفمند»

«این کتاب تا به امروز کامل‌ترین مرجع در حوزه‌ی حملات سایبری هدفمند بوده است. دکتر سود و دکتر انبادی این موضوع را به روشی ساده بیان کرده‌اند و خواننده را با مبانی حملات سایبری هدفمند، چگونگی گردآوری اطلاعات سیستم‌های هدف توسط مهاجمین، راهبردهای مورداستفاده برای حمله به سیستم و استخراج اطلاعات از سیستم‌های هدف آشنا نموده‌اند. این کتاب در ادامه به چگونگی ایجاد راهکارهای دفاعی چندلایه برای دفاع از سیستم در برابر حملات سایبری می‌پردازد. به عبارت دیگر ابتدا مسئله‌ای را بیان می‌کند و در ادامه راهکاری را برای حل آن ارائه می‌دهد. اگر به تازگی به حوزه‌ی حملات سایبری وارد شده‌اید یا قصد دارید مهارت‌های خود را در این حوزه تقویت کنید، پس مطالعه‌ی این کتاب را به شما پیشنهاد می‌کنم».

کریستوفر الیسان، مدیر تحقیقات بدافزار در شرکت RSA از زیرمجموعه‌های شرکت EMC.

«از آنجا که حملات هدفمند روز به روز بیشتر، پیچیده‌تر و مخرب‌تر می‌شوند، پس باید آنها را به خوبی شناخت، تشخیص داد و راهکارهای کاهش اثرات آنها را فرا گرفت. آدیتیا سود و ریچارد انبادی در این کتاب ابزاری را برای انجام این کار ارائه داده‌اند. تحلیل‌های فنی دقیق و روشن آنها به ما در کاهش ترس، عدم قطعیت، ابهامات و تصورات غلط پیرامون این موضوع کمک می‌کند تا بدانیم دقیقا چه اتفاقی در حال رخدادن است و چه کاری می‌توان در این زمینه انجام داد».

استیو مَنسفیلد–دیوین، ویراستار، متخصص امنیت شبکه، کلاهبرداری و امنیت کامپیوترها.

«دکتر آدیتیا کی سود و دکتر ریچارد جی. اِنبادی اقدام ارزشمندی را در خصوص مطالعه‌ی حملات هدفمند و تجزیه‌ی سیستماتیک آنها انجام دادند و به واسطه‌ی پژوهش آنها، اکنون ما می‌توانیم به راحتی روش‌ها، تاکتیک‌ها و رویه‌های حمله را بشناسیم و راهبردهای تدافعی مناسبی را برای مقابله با این حمله‌ها به کار گیریم. کتاب حملات سایبری هدفمند، دانشی را در رابطه با شاخص‌های متداول حمله به ما ارائه می‌دهد. بنابراین تیم‌های امنیتی می‌توانند در سریع‌ترین زمان ممکن، نسبت به حملات واکنش نشان داده و رفتارهای ناهنجار را از رفتارهای عادی و روزمره‌ی کاربران تشخیص دهند.«

استفان چِنِتِه، مدیر ارشد فناوری در شرکت اَتَک‌آی‌کیو.

«کتاب حملات سایبری هدفمند یک راهنمای کامل در حوزه‌ی جرایم سایبری به شمار می‌آید. این کتاب مدل و مکانیزم‌هایی را توصیف می‌کند که مجرمین سایبری از آنها در انجام حملات سایبری خود، به‌منظور استخراج اطلاعات یا سرقت پول، استفاده می‌کنند. از دیدگاه یک متخصص تست نفوذ[1]، هکرهای اخلاقی[2] عوامل مهمی را خواهند یافت تا از آنها برای آماده‌سازی یک رویکرد بهتر برای انجام تست‌های نفوذ سطح بالا استفاده کنند. آدیتا و ریچارد رازهایی را افشا می‌کنند؛ رازهایی که مجرمین سایبری از آنها برای ورود به امن‌ترین

[1] pen-tester’s perspective
[2] ethical hackers

شرکت‌های دنیا استفاده می‌کنند. من دانش بسیاری را از این کتاب فرا گرفتم؛ کتابی که توسط یک قهرمان آرسنال بلک‌هت تالیف شده است».

نبیل اوچن، موسس وبسایت ToolsWatch.org و موسس بلک‌هَت آرسنال.

«من همیشه از طرفداران مقالات منتشرشده توسط دکتر سود و دکتر انبادی بوده‌ام و این کتاب هم از همان کیفیتی برخوردار است که در نشر کراس‌تاک[1] از آن بهره می‌بریم. از نظر من این کتاب برای تمامی افراد علاقمند به مطالعه‌ی روش‌های مدرن در حمله‌ی سایبری جذاب و فراگیر است. روند بیان اطلاعات در فصل‌های این کتاب از یک الگوی کاملا منطقی پیروی می‌کند و اطلاعات آن حتی برای افرادی با دانش محدود در حوزه‌ی حمله‌ی سایبری هم قابل‌فهم است. از نظر من این کتاب بسیار جذاب است و از سبک پویا و لذت‌بخشی در تالیف آن استفاده شده است. این کتاب نه تنها برای فعالین حوزه‌ی نرم‌افزاری مناسب است بلکه افراد علاقمند به حریم شخصی و امنیت هم می‌توانند آن را مطالعه کنند».

جاستین هیل، مدیر اجرایی نشر کراس‌تاک، مجله مهندسی نرم‌افزارهای دفاعی.

«در عصر حاضر، حملات هدفمند یکی از مهلک‌ترین و خطرناک‌ترین تهدیدات سایبری هستند. تمام شرکت‌های بزرگ و کوچک، باید این حملات را به عنوان یک خطر بزرگ در نظر داشته باشند. این کتاب جدیدترین اطلاعات را به خوانندگان ارائه می‌دهد و به آنها کمک می‌کند تا از تهدید پیشی بگیرند و بتوانند پیش از قرارگیری در معرض حمله، اقدامات کنشی لازم را انجام دهند».

دنی بردبری، خبرنگار و ویراستار در امنیت سایبری.

---

[1] CrossTalk.

درباره نویسندگان

آدیتیا کی سود محقق و مشاور ارشد امنیت است. دکتر سود به تحقیق و مطالعه‌ی اتوماسیون و تحلیل بدافزار، امنیت اپلیکیشن، طراحی نرم‌افزار ایمن و جرایم سایبری علاقمند است. او در چندین پروژه‌ی مرتبط با تست نفوذ فعالیت داشته، و متخصص امنیت محصولات/تجهیزات، شبکه‌ها، موبایل و اپلیکیشن‌های وب است و با مشتری‌های شرکت‌های آی‌اوآکتیو[۱]، کاپی‌ام‌جی[۲] و دیگر شرکت‌های عضو ۵۰۰ شرکت برتر مجله فورچون[۳] همکاری می‌کند. او موسس آزمایشگاه‌های امنیت سِک‌نیچ[۴] است؛ آزمایشگاهی که به‌عنوان یک درگاه وب مستقل برای اشتراک‌گذاری پژوهش‌های انجام شده با جامعه‌ی پژوهشگرانی که در زمینه‌ی امنیت فعالیت می‌کنند، محسوب می‌شود. او چندین مقاله در مجلات مختلف از جمله IEEE، الزویر[۵]، کراس‌تاک، ایساکا[۶]، ویروس بولتین[۷]، یوزنیکس[۸] و مجلات دیگر منتشر کرده است. کارهای او در رسانه‌های مختلفی مثل آسوشیتدپرس[۹]، فاکس نیوز[۱۰]، گاردین[۱۱]، بیزینس اینسایدر[۱۲]، سی‌بی‌سی[۱۳] و رسانه‌های دیگر بازتاب داشته است. او سخنران فعالی در کنفرانس‌های صنعتی بوده و در کنفرانس‌های دیفکان[۱۴]، هَک‌این‌دِباکس، بلک‌هَت آرسنال، آراس‌ای، ویروس بولتین، اوَسپ[۱۵] و بسیاری از کنفرانس‌های دیگر ارائه داشته است. او مدرک دکتری خود را در رشته علوم کامپیوتر از دانشگاه ایالتی میشیگان کسب کرده است.

دکتر ریچارد اِنبادی دانشیار دانشکده علوم کامپیوتر و مهندسی است. او در سال ۱۹۸۷ و بعد از کسب مدرک دکترا در رشته علوم کامپیوتر از دانشگاه مینه‌سوتا به عضویت هیات علمی دانشگاه درآمد. ریچارد مدرک کارشناسی خود را در سال ۱۹۷۶ میلادی در رشته ریاضیات از دانشگاه کارلتون از شهر نورث‌فیلد در ایالت مینه‌سوتا کسب کرد و به مدت ۶ سال به آموزش ریاضیات دبیرستان در ایالت‌های ورمونت و نیوهمپشایر مشغول شد. ریچارد پژوهش‌ها مختلفی را در حوزه‌های متنوع منتشر کرده است که بیشتر این پژوهش‌ها در زمینه‌ی امنیت و معماری کامپیوتر بوده‌اند. او طی همکاری با فیزیک‌دانان توانست دو اختراع در زمینه نانوفناوری ثبت

---

[1] IOActive
[2] KPMG
[3] Fortune
[4] SecNiche
[5] Elsevier
[6] ISACA
[7] Virus Bulletin
[8] USENIX
[9] Associated Press
[10] Fox News
[11] Guardian
[12] Business Insider
[13] CBC
[14] DEFCON
[15] OWASP

کند. او با همکاری بیل پانچ[1] کتابی با عنوان پایتون در سی‌اس‌وان: پردازش با استفاده از پایتون (شرکت آدیسون–وِسلی[2]، ۲۰۱۰) منتشر کرده که ویرایش دوم آن نیز منتشر شده است. ریچارد اوقات فراغت خود را صرف هاکی، اسکواش و قایق‌سواری می‌کند و همچنین میزبان دوره‌همی‌های خانوادگی نیز هست.

[1] Bill Punch
[2] Addison-Wesley

مرور اجمالی مطالب کتاب

این کتاب به بررسی مکانیزم‌های حملات هدفمند و جرایم سایبری و همچنین بررسی تخصصی کرم استاکس‌نت می‌پردازد. این کتاب با سبکی انگیزشی تالیف شده است و مدلی سیستماتیک و سلسله‌مراتبی را از مراحل مختلف یک حمله‌ی هدفمند ارائه می‌دهد. هر فصل از این کتاب به تشریح یکی از مراحل حمله‌ی هدفمند می‌پردازد و فرایندهای داخلی و چگونگی اجرای موفق حملات هدفمند را بیان می‌کند. مرور فصل‌ها در بخش زیر ارائه می‌شود:

- فصل اول به معرفی موضوع حملات هدفمند می‌پردازد و مدل کامل و اهداف این حملات را توضیح می‌دهد. در این فصل، اصول لازم برای اجرای موفق حملات هدفمند ارائه می‌شود. این فصل مفاهیم مقدماتی مربوط به مدل حمله‌ی هدفمند را به خوانندگان ارائه خواهد داد؛ مفاهیمی کلی در زمینه‌ی گردآوری اطلاعات، آلوده‌کردن اهداف، سوءاستفاده از سیستم، استخراج داده‌ها و کنترل روی شبکه‌ی هدف. در این فصل، تفاوت‌های میان حملات هدفمند و تهدیدهای پیشرفته‌ی مستمر[1] نیز آشکار می‌شود.
- فصل دوم روش‌های متنوعی را نشان می‌دهد؛ روش‌هایی که مهاجمین سایبری به‌منظور گردآوری اطلاعات از آنها استفاده می‌کنند. بعضی از این روش‌ها عبارتند از اطلاعات منابع آشکار (اوسینت)[2]، اطلاعات فضای سایبری (سایبینت)[3]، و اطلاعات انسانی (HUMINT)[4]. در این فصل ارتباط میان این روش‌ها نیز بیان می‌شود. همچنین این فصل بررسی می‌کند که چگونه مهاجمین قبل از انجام هر گونه عملیات شناسایی[5]، از اینترنت و اطلاعاتی که در مورد افراد و سازمان‌ها (در منابع مختلفی مانند شبکه‌های اجتماعی آنلاین (OSN)[6]، وبسایت‌ها، مجلات و غیره) وجود دارد، استفاده می‌کنند. اطلاعات گردآوری شده در مورد اهداف، جهت حملات هدفمند را تعیین می‌کند.
- فصل سوم به بررسی راهبردهای متنوعی می‌پردازد؛ راهبردهایی که مهاجمین به‌منظور آلوده‌سازی اهداف و دریافت بدافزار، از آنها استفاده کرده و در نهایت به سیستم حمله می‌کنند. این فصل به بررسی پرکاربردترین راهبردهای آلوده‌سازی در حملات هدفمند می‌پردازد؛ که چند نمونه از آنها عبارتند از فیشینگ هدف‌دار[7]، حمله‌ی گودال آب[8]، مدل آلوده‌سازی آوردن دستگاه خود (BYOD)[9] و حملات مستقیم با سوءاستفاده از نقص‌های موجود در شبکه و نرم‌افزار. هدف از آلوده‌سازی یک هدف یافتن

---

[1] advanced persistent threats
[2] Open-source intelligence (OSINT)
[3] Cyber Space Intelligence (CYBINT)
[4] Human Intelligence (HUMINT)
[5] reconnaissance
[6] Online Social Networks (OSNs)
[7] spear phishing
[8] waterholing
[9] Bring-Your-Own-Device (BYOD) infection model

روزنه‌ای برای نفوذ بدافزار در هدف است تا بتوان به واسطه‌ی آن کنترل کامل سیستم را در دست گرفت. هر مدل از مسیر متفاوتی برای اجرای حملات هدفمند استفاده می‌کند.

- فصل چهارم به توصیف کامل سوءاستفاده از سیستم می‌پردازد و انواع کدهای مخرب و آسیب‌پذیری‌های مورداستفاده برای حمله به سیستم را پوشش می‌دهد. این فصل یک طرح سلسله‌مراتبی از مکانیزم‌های حفاظتی را ارائه می‌دهد که توسط فروشندگان طراحی شده‌اند. همچنین روش‌هایی که مهاجمین از آنها برای دورزدن این مکانیزم‌ها استفاده می‌کنند در این فصل ارائه می‌شود. در این فصل، همچنین به‌طور دقیق به بررسی روش‌های جلوگیری از اجرای داده (DEP)[1] و تصادفی‌سازی چیدمان فضای آدرس (ASLR)[2] مانند مکانیزم‌های ساخت کد مخرب از قبیل برنامه‌نویسی مبتنی بر بازگشت (ROP)[3] و درز اطلاعات مهم پرداخته می‌شود. همچنین این فصل راهکارهای امنیتی مختلفی را بیان می‌کند؛ راهکارهایی که توسط شرکت‌ها و به منظور مقابله با کد مخرب مهاجمین طراحی شده‌اند. علاوه بر این، اطلاعاتی در مورد بدافزارهای پیشرفته نیز ارائه شده است. همچنین در این فصل به روش‌هایی پرداخته شده است که بدافزارها از آنها برای دورزدن راهکارهای ثابت و پویایی استفاده می‌کنند که توسط پژوهشگران حوزه‌ی امنیت طراحی شده‌اند.
- فصل پنجم به مکانیزم‌های مختلف استخراج داده می‌پردازد؛ مکانیزم‌هایی که مهاجمین برای استخراج داده از سیستم‌های آلوده، از آنها استفاده می‌کنند. استخراج داده در دو مرحله انجام می‌شود: سرقت داده‌ها و سپس انتقال آنها به سروری که تحت کنترل مهاجم قرار دارد. در این فصل به موضوعاتی مانند تزریق در وب[4]، سرقت ویدیو و تصویر، ربودن اطلاعات فرم‌ها[5]، سرقت اطلاعات سیستم عامل و غیره پرداخته می‌شود. روش‌های مختلف انتقال اطلاعات مانند رمزنگاری اطلاعات و فشرده‌سازی آنها در کانال‌های پروتکلی مختلف از قبیل HTTP/HTTPS، نظیر به نظیر (P2P)[6]، رله‌ی گپ اینترنتی (IRC)[7]، نیز در این فصل بررسی می‌شوند. به‌طور کلی، در این فصل به ارائه‌ی حالت‌های مختلف استخراج داده در حملات هدفمند پرداخته می‌شود.
- فصل ششم به بررسی روش‌های متعددی می‌پردازد که مهاجمین به‌منظور کنترل شبکه و حضور بلندمدت در آن، از این روش‌ها استفاده می‌کنند. مهاجمین، عملیات شناسایی شبکه را در شبکه انجام می‌دهند تا بدین ترتیب بتوانند به سیستم‌های اضافه‌ی موجود در شبکه حمله کنند و در نتیجه، به راحتی بتوانند اطلاعات موجو در این سیستم‌ها را در مقیاس وسیع استخراج نمایند. مهاجم از ابزارهای

---

[1] Data Execution Prevention (DEP)
[2] Address Space Layout Randomization (ASLR)
[3] Return-oriented Programming (ROP)
[4] Web Injects
[5] Form-grabbing
[6] Peer-to-Peer (P2P)
[7] Internet Relay Chat (IRC)

خصوصی و عمومی مانند ابزارهای دسترسی راه دور (RAT)[1] استفاده می‌کند تا وظایف متعددی را از قبیل اسکن درگاه و سوءاستفاده از آسیب‌پذیری‌های موجود در شبکه هدف انجام دهد. این مرحله از نظر اجرای حمله‌های هدفمند بسیار اهمیت دارد؛ زیرا باعث می‌شود که حمله‌های انجام شده تا مدت زمانی طولانی شناسایی نشوند.

- فصل هفتم به بررسی مدل جاسوس‌افزار به عنوان یک سرویس (CaaS)[2] می‌پرازد تا اجزای حمله‌های هدفمند را با استفاده از ابزارهای ساده ایجاد کند. در کل، این فصل نشان می‌دهد که خیلی راحت می‌توان با صرف مقدار پول مشخص، اجزای مختلف نرم‌افزاری و سایر مولفه‌ها (از قبیل سرورهای میزبان آسیب‌دیده) را خریداری کرد. همچنین به بررسی نقش ارز دیجیتال در بازارهای زیرزمینیِ موجود در اینترنت و پردازش تراکنش‌ها نیز پرداخته می‌شود.
- فصل هشتم به ساخت لایه‌های دفاعی برای محافظت در برابر حملات هدفمند اختصاص یافته است. لایه‌های محافظ شامل امنیت کاربرمحور، امنیت سیستم نهایی، مدیریت وصله‌های امنیتی[3] و ارزیابی آسیب‌پذیری، نظارت بر شبکه، و برنامه‌ی پاسخ قوی هستند. این فصل نیاز و اهمیت ساخت لایه‌های دفاعی پیشرفته را برای مبارزه با بدافزارهای پیچیده بیان می‌کند.
- فصل نهم ابهامات و برداشت‌های اشتباه در مورد حمله‌های هدفمند را بیان می‌کند و طبیعت واقعی این نوع حمله‌ها را تعریف می‌کند.
- بخش دوم کتاب به بررسی فنی و تخصصی کرم استاکس‌نت می‌پردازد.

در ادامه‌ی این کتاب از اصطلاح حمله‌های هدفمند به جای اصطلاح حمله‌های سایبری هدفمند استفاده می‌شود.

---

[1] Remote Access Toolkits
[2] Crimeware-as-a-Service
[3] patch management