

به نام خدا

۲۲۸۸۴۹۹

باج افزار

دفاع در برابر اخاذی دیجیتال

نویسندگان

Allan Liska, Timothy Gallo

مترجم:

سعید ترکمانی

۱۴۰۱

موسسه آموزشی تالیفی ارشدان

سرشناسه	: لیسکا، آلن Liska, Allan
عنوان و نام پدیدآور	: باج‌افزار: دفاع در برابر اخاذی دیجیتال / نویسندگان: مترجم سعید ترکمانی.
مشخصات نشر	: تهران: موسسه آموزشی تالیفی ارشدان، ۱۴۰۱.
مشخصات ظاهری	: ۱۹۸ ص: مصور (رنگی)، جدول.
شابک	: ۹۷۸-۶۲۲-۰۸-۲۸۹۷-۶
وضعیت فهرست نویسی	: فیبا
یادداشت	: عنوان اصلی: Ransomware : defending against digital extortion, 2016
یادداشت	: کتاب حاضر نخستین بار با عنوان "باج‌افزار: روش‌های دفاع در برابر باج‌گیری دیجیتال" توسط انتشارات گسترش علوم پایه در سال ۱۳۹۶ منتشر شده است.
یادداشت	: کتابنامه: ص: ۱۹۷-۱۹۸.
عنوان دیگر	: باج‌افزار: روش‌های دفاع در برابر باج‌گیری دیجیتال.
عنوان دیگر	: دفاع در برابر اخاذی دیجیتال.
موضوع	: نرم‌افزار بدافزار
موضوع	: کامپیوترها -- ایمنی اطلاعات
	: جرایم کامپیوتری - پیشگیری
شناسه افزوده	: گالو، تیموتی
شناسه افزوده	: ترکمانی، سعید، ۱۳۶۶-، مترجم
رده بندی کنگره	: QA۷۶۷۶
رده بندی دیویی	: ۳۵/۸۸
شماره کتابشناسی ملی	: ۸۸۰۸۴۱۳
اطلاعات رکورد کتابشناسی	: فیبا

www.ketab.ir
ارشدان

مؤسسه آموزشی تالیفی ارشدان

- نام کتاب: باج‌افزار-دفاع در برابر اخاذی دیجیتال
- ترجمه: سعید ترکمانی
- ناشر: آموزشی تالیفی ارشدان
- ویرایش: اول
- نوبت چاپ: اول ۱۴۰۱
- حروفچینی و صفحه آرایی: www.irantypist.com
- طراح و گرافیک: www.irantypist.com
- شابک: ۹۷۸-۶۲۲-۰۸-۲۸۹۷-۶
- شابک الکترونیک: ۹۷۸-۶۲۲-۰۸-۲۸۹۶-۹
- شمارگان: ۱۰۰۰
- مرکز خرید آنلاین: www.arshadan.com
www.arshadan.net
- مرکز پخش و توزیع: ۰۲۱۴۷۶۲۵۵۰۰
- قیمت: ۸۰۰۰ تومان

پیشگفتار ناشر:

به نام ایزد دانا که آغاز و انجام از آن اوست

هرگز دل من ز علم محروم نشد کم ماند ز سرار که مفهوم ن‌شد
اکنون که به چشم عقل در می‌نگرم معلوم شد که هیچ معلوم نشد

ای دانای بی‌همتا، ای بخشنده ایی که ناخواسته عطا فرمایی و هر نیازمندی را به عدالت بی‌نیاز گردانی، مگر اینکه نالایق باشد و آن عنایت را به بازگونه از دست دهد. در عرصه پیشرفت تکنولوژی در هزاره سوم، هنوز نیاز بر مطالعه کتاب در کنار استفاده از منابع کامپیوتری و اینترنت احساس می‌شود. از این بابت خوشحالیم که می‌توانیم در جهت اعتلای علم، دانش و فرهنگ کشور قدمی هر چند کوچک برداریم.

و من الله التوفیق

دکتر شمس الدین یوسفیان

مدیر مسئول انتشارات ارشدان

فهرست مطالب

۱۱.....	قسمت اول: شناخت باج افزار.....
۱۳.....	فصل اول: معرفی باج افزار.....
۱۶.....	۱-۲-۱ deployment.....
۱۸.....	۱-۲-۲ installation.....
۲۰.....	۱-۲-۳ command and control.....
۲۱.....	۱-۲-۴ Destruction.....
۲۱.....	۱-۲-۵ Extortion.....
۲۸.....	۱-۵-۱ سایر فاکتورها.....
۲۸.....	۱-۵-۱-۱ در دسترس بودن رمزگذاری قوی.....
۲۸.....	۱-۵-۱-۲ cryptocurrency در دسترس بودن.....
۲۸.....	۱-۵-۱-۳ dynamic DNS.....
۲۹.....	۱-۵-۱-۴ برنامه های گمراه کننده، ضد ویروس های تقلبی و باج افزارهای مدرن.....
۳۳.....	فصل دوم: مزایا و معایب پرداخت باج افزار.....
۴۰.....	۴-۱ PCI DSS۲ و باج افزار.....
۴۲.....	۴-۲ HIPPA.....
۴۴.....	فصل سوم: کنترل کننده باج افزارها و اهداف آنها.....
۴۷.....	2-3-1 باج افزار Tesla crypt.....
۴۸.....	۳-۲-۲ crypt xxx باج افزار.....
۴۸.....	۳-۲-۳ crypto wall باج افزار.....
۴۹.....	۳-۲-۴ locky باج افزار.....
۵۰.....	۳-۲-۵ Ranscam باج افزار.....
۶۰.....	قسمت دوم: تکنیک های دفاعی.....

۶۲	فصل چهارم: محافظت از ایستگاه نهایی و سرورها
۷۰	۴-۳-۱ جلوگیری از اجرای باج افزار
۷۲	۴-۳-۲ دنبال کردن packer و registry
۷۴	۴-۳-۳ Shadow copy
۷۶	۴-۳-۴ کنترل Command and Control یا C&C
۷۸	۴-۳-۵ متوقف کردن حمله در فرآیند رمزگذاری
۸۰	۴-۳-۶ جستجو کردن Executable post attack
۸۸	فصل پنجم: محافظت از نیروی کار
۹۳	۵-۲-۱ اسکن کردن پیوست های ایمیل
۹۴	۵-۲-۲ ردیابی وبسایت ها
۹۹	۵-۴-۱ ایجاد حمله فیشینگ برای کاربران
۱۰۳	فصل ششم: اطلاعات تهدید باج افزارها
۱۱۴	قسمت سوم: خانواده باج افزارها
۱۱۶	فصل هفتم: باج افزار Cerber
۱۲۶	فصل هشتم: باج افزار Locky
۱۳۴	۸-۵-۱ مسدود کردن spam ها
۱۳۶	۸-۵-۲ غیرفعال کردن macro ها در اسناد Microsoft office
۱۳۷	۸-۵-۳ جلوگیری از اجرای فایل های javascript
۱۴۰	۴-۵-۸ جلوگیری از Initial Callout
۱۴۴	۸-۵-۵ مهندسی معکوس DGA
۱۴۸	فصل نهم: باج افزار CryptXXX
۱۵۶	۹-۴-۱ جلوگیری از اجرای exploit kit ها
۱۵۸	۹-۴-۲ DNS firewall ها و IDS