فصل‌نامه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان
شماره دوازدهم - زمستان ۱۴۰۰

- هشدار درخصوص اسکیمرها
- آمار حملات سایبری در سال ۲۰۲۲
- مدیریت فناوری اطلاعات سازمانی
- ماکروها در مجموعه آفیس، مفید یا مخرب؟
- چک‌لیست هجده کنترل بحرانی CIS در سازمان
- حملات باج‌افزاری و راهکارهای جلوگیری و محافظت در مقابل آن‌ها

درباره

مرکز آپا دانشگاه کردستان

آپا مخفف عبارت آگاهی‌رسانی، پشتیبانی و امداد رخدادهای رایانه‌ای است و معادل بومی اصطلاح CSIRT می‌باشد. مرکز آپا دانشگاه کردستان، در راستای انجام فعالیت‌های خود در زمینه آگاهی و اطلاع رسانی، با بکارگیری نیروهای متخصص و پتانسیل‌های پژوهشی در استان کردستان اقدام به انتشار نشریه‌ای الکترونیکی در حوزه امنیت فضای سایبری نموده است.
مخاطبان اصلی نشریه کارشناسان و متخصصان فناوری اطلاعات و شبکه، دانشجویان و علاقمندان فضای سایبری است. مطالب این نشریه عموماً محورهای زیر را شامل می‌شود:

- اطلاع‌رسانی رخدادهای اخیر فضای سایبری
- آگاهی‌رسانی نسبت به آخرین تهدیدات و آسیب‌پذیری فضای مجازی
- آموزش‌های تخصصی و عمومی در جهت ارتقاء دانش امنیت

شایان ذکر است، ویرا، اسم نشریه، واژه‌ای در زبان کردی به معنی صاحب‌فکر و هوشمند است.

صاحب امتیاز: مرکز آپا دانشگاه کردستان
مدیر مسئول: محمد فتحی
سردبیر: هادی گلباغی
سردبیر فنی: محمد حبیبی
ویراستاری، طراحی و صفحه‌آرایی: نازیلا خسروی
نویسندگان (به‌ترتیب مطالب):
محمد فتحی/ هادی گلباغی/محمد حبیبی/ ژینو سفاحی/ مونا علی‌اکبری/ نازیلا خسروی/ پدرام قاسمی/ آرین فقیراللهی/ ژوان عبدمؤخر

راه‌های ارتباطی:

تلفن مرکز: ۰۸۷۳۳۶۱۱۴۱۵
نشانی مجله: کردستان، سنندج، بلوار پاسداران، دانشگاه کردستان، دانشکده مهندسی، ساختمان شماره ۳، طبقه همکف، مرکز آپا
وب‌سایت: cert.uok.ac.ir
ایمیل: cert@uok.ac.ir

راهنمایی:

در فهرست مطالب می‌توانید با کلیک بر روی هریک از بخش‌ها و مطالب به صفحه مورد نظر منتقل شوید.
با کلیک بر روی لینک‌ها می‌توانید مستقیما به آدرس مورد نظر منتقل شوید.

فهرست
مطالب

مقاله‌های آموزشی

۰۱ مدیریت فناوری اطلاعات سازمانی

۰۷ ماکروها در مجموعه آفیس، مفید یا مخرب؟

آسیب‌پذیری

۱۵ جدیدترین آسیب‌پذیری‌های شناخته‌شده که مورد سوء استفاده قرار گرفته‌اند.

معرفی ابزار

۲۵ حملات باج‌افزاری و راهکارهای جلوگیری و محافظت در مقابل آن‌ها

دفترچه تقلب

۳۵ دفترچه تقلب فریمورک Volatility

معرفی دوره

۴۱ دوره FOR528

معرفی کتاب

۴۳ کتاب Ransomware Protection Playbook

مقاله‌های تحقیقاتی

۴۵ چک‌لیست هجده کنترل بحرانی CIS در سازمان

۵۱ آمار حملات سایبری در سال ۲۰۲۲

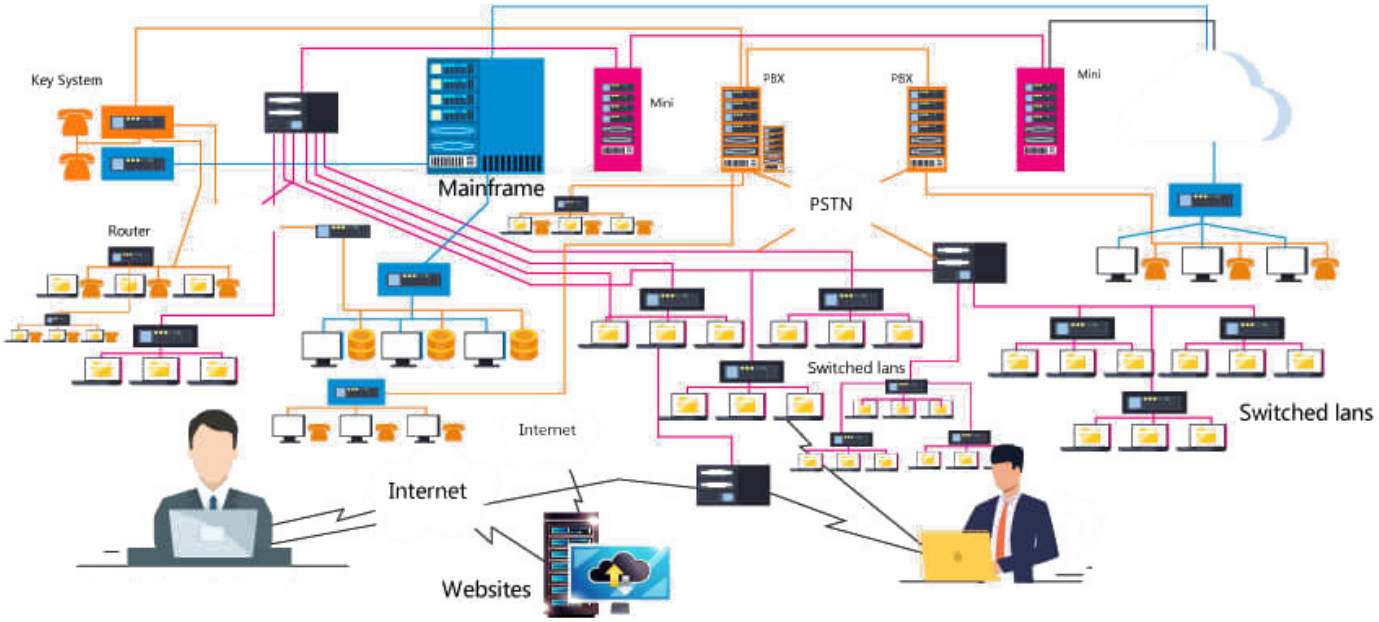
امنیت اطلاعات

۵۹ هشدار درخصوص اسکیمرها

محمد فتحی
m.fathi@uok.ac.ir

مقاله آموزشی

مدیریت فناوری اطلاعات سازمانی



مقدمه

منابع اطلاعاتی سازمان‌ها به سرعت در حال دیجیتالی شدن هستند و تعداد سرویس‌های الکترونیکی به تناسب در حال افزایش است. به‌همین دلیل امروزه یکی از ارکان مهم در هر سازمانی، مرکز فناوری اطلاعات و زیرساخت‌های نرم افزاری و سخت‌افزاری آن است. در این نوشتار تعدادی نکات کلیدی برای مدیریت صحیح و افزایش بهره‌وری منابع موجود در مراکز فناوری اطلاعاتی سازمانی که حاصل تجربیات نگارنده می‌باشد معرفی می‌گردند. این نکات که مخاطب آن عمدتاً مدیریت مرکز فناوری اطلاعات سازمان است در سه بخش **زیرساخت و شبکه**، **سامانه‌های کاربردی** و **امنیت** گردآوری و تشریح شده‌اند.

زیرساخت و شبکه

پشتیبان‌گیری داده

داده‌ها از منابع مهم و اصلی سازمان هستند و امروزه کارکنان با اطمینان به بسترهای فناوری اطلاعات داده‌های حیاتی سازمان را به‌صورت دیجیتال ذخیره می‌کنند، به‌نحوی‌که روزبه‌روز از منابع کاغذی کم شده و رویکرد Paperless در حال گسترش است. این در حالی است که کارشناسان فناوری اطلاعات از ریسک‌های این کار که عموماً خارج از کنترل و اراده مراکز فناوری اطلاعات است آگاه هستند. بلایای طبیعی، آتش‌سوزی، زلزله، بدافزار و باج افزارها از خطراتی هستند که احتمال وقوع دارند و هرکدام به تنهایی می‌توانند همه داده‌های یک سازمان را از بین برده یا با چالش مواجه سازند.

با در نظرگرفتن موارد فوق، داشتن یک سیستم پشتیان‌گیری داده از ضروریات یک سازمان است. این سیستم لازم است در مکان فیزیکی دیگری غیر از دیتاسنتر اصلی نگهداری شود و به‌صورت خودکار در زمان‌های مشخصی در شبانه‌روز از داده‌های سرورهای سازمان نسخه پشتیبان تهیه نمایند. تمهیدات فضای فیزیکی این سیستم از جمله حراست فیزیکی، تهویه، کولر و منبع تغذیه پشتیبان نیز باید در نظر گرفته شود.

منابع تغذیه پشتیبان

منابع تغذیه برق اتاق سرور از ضروریات ارائه سرویس مطمئن هستند و قطعی این منابع تغذیه علاوه‌بر قطع سرویس‌ها ممکن است عامل مشکلات سخت‌افزاری و نرم‌افزاری برای تجهیزات شود. در یک اتاق سرور که سرویس‌ها به‌صورت زنجیره‌ای و وابسته به‌هم هستند اختلال در عملکرد یک سرور یا سرویس می‌تواند عملکرد کلی اتاق سرور را با اخلال مواجه کند. عطف به این موارد، علاوه‌بر تامین تغذیه اتاق سرور از برق شهر، تهیه منابع تغذیه پشتیبان از ضروریات اتاق سرور است تا در صورت قطع منبع تغذیه اصلی، منابع پشتیبان به‌صورت خودکار وارد مدار شوند و مانع قطعی سرویس‌ها شوند. از جمله این منابع می‌توان به ژنراتور و UPS اشاره کرد که لازم است توان خروجی آن‌ها نیازمندی‌های اتاق سرور را تامین نماید.

چاه ارت

تجهیزات شبکه، دکل‌ها، آنتن‌ها و منابع تغذیه برای عملکرد درست و انتقال بارهای اضافی به چاه ارت نیاز دارند. در صورت نداشتن چاه ارت، بارهای اضافی القایی بر روی بدنه تجهیزات در هنگام رعد و برق و شرایط نامساعد آب و هوایی می‌توانند عامل آسیب و اختلال شوند. برای پیشگیری از این اتفاقات و همچنین خسارت‌های مالی به سازمان، تعبیه چاه ارت به تناسب تجهیزات و دکل‌ها ضروری است.

چتر Wi-Fi

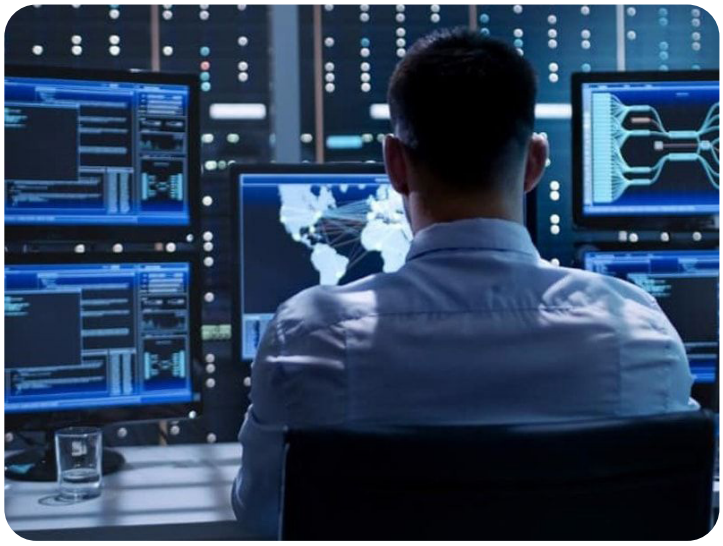
آمارها نشان می‌دهد امروزه بیشترین شیوه دسترسی کاربران به اینترنت از طریق گوشی موبایل و تبلت صورت می‌گیرد که از طریق شبکه Wi-Fi می‌باشد. پروتکل‌های دسترسی در شبکه Wi-Fi که عموماً برمبنای VPN و hotspot هستند مستلزم ایجاد اتصال از طریق کاربر در هر بار لاگین به شبکه هستند که استفاده از آن‌ها را خسته کننده و ناکارآمد می‌کند. ایجاد چتر Wi-Fi در سازمان‌های بزرگ شامل چندین ساختمان از طریق پروتکل‌هایی نظیر 1X. می‌تواند دسترسی آسان و پایدار را برای کاربران فراهم نماید. در این پروتکل، یکبار لاگین کاربر به شبکه، دسترسی دائمی کاربر در همه نقاط جغرافیایی سازمان را فراهم می‌نماید.

تهیه لینک پشتیبان از اینترنت

لینک‌های اینترنت و به‌خصوص لینک‌های بی‌سیم به‌دلایل مختلف دچار خرابی می‌شوند و سازمان را با مشکل مواجه می‌کنند. برای افزایش قابلیت اطمینان، لینک‌های پشتیبان و مطمئن اینترنت ترجیحاً از طریق اپراتورهای دیگری غیر از اپراتور اصلی تهیه شود. داشتن لینک‌های دسترسی گوناگون از اپراتورهای متفاوت به افزایش قابلیت اطمینان سرویس‌دهی سازمان کمک می‌کند.

مدیریت تخصیص IP

تعداد IP های واگذار شده به یک سازمان از طرف اپراتورها عموماً محدود است و به‌همین دلیل IP ها از منابعی هستند که باید به‌طور موثری مدیریت و تخصیص داده شوند. به‌دلیل گسترش تعداد سرویس‌ها، استفاده از یک IP برای هر سرویس می‌تواند منابع IP را با کمبود مواجه کند. استفاده از هاست‌های اشتراکی و همچنین Port Forwarding در فایروال‌ها می‌تواند در صرفه‌جویی از منابع IP موثر باشد.



تهیه نسخه پشتیبان از سرویس‌های مهم در خارج از سازمان

اگر به هر دلیلی از قبیل خرابی لینک اینترنت یا منابع تغذیه، دیتاسنتر سازمان از دسترس خارج شود ارتباط با کاربران قطع می‌شود. برای پیشگیری از این مشکل، شایسته است نسخه پشتیبان سرویس‌های مهم و پرکاربرد سازمان از قبیل DNS، پورتال اطلاع‌رسانی، ایمیل و غیره در خارج از سازمان نیز پیاده‌سازی شود تا در مواقع اضطراری در دسترس باشد. این نسخه‌ها به بازیابی سرویس‌های داخلی سازمان نیز کمک خواهند کرد.

فضای ذخیره‌سازی درون سازمانی

اشتراک منابع درون یک سازمان می‌تواند به استفاده موثر از منابع کمک نماید. با توجه به افزایش روزافزون داده سازمانی و کاربران، ایجاد یک فضای ذخیره سازی درون سازمانی، علاوه‌بر بازدهی در مصرف منابع و مدیریت بهتر، می‌تواند دسترسی کاربران به فایل‌های خود را تسهیل نماید، مخصوصاً در صورتی‌که فضای ذخیره‌سازی بر روی محیط ابری ایجاد شده باشد و کاربران بتوانند در مکان‌های مختلف و بر روی بسترهای گوناگون به داده دسترسی داشته باشند.

به‌روزرسانی بسترهای نرم‌افزاری

شرکت‌های توسعه‌دهنده سیستم‌عامل‌ها و نرم‌افزارهای سرورها و تجهیزات شبکه به‌صورت مداوم در حال ارتقاء و رفع باگ‌های محصولات خود هستند. برای داشتن یک سرویس امن و مطمئن لازم است ادمین‌های شبکه در فواصل زمانی مشخص نسبت به به‌روزرسانی همه سیستم عامل‌ها و firmware تجهیزات شبکه اقدام نمایند.

انتی‌ویروس

انتی‌ویروس‌ها از اجزای ضروری یک شبکه هستند که با استقرار بر روی تجهیزات و سرویس‌های شبکه مانع نفوذ انواع بدافزارها هستند. یکی از نکات مهم در انتی‌ویروس‌ها، به‌روزرسانی آنها است تا رد ویروس‌های جدید را کشف کند. به‌دلیل رشد و گسترش بدافزارهای ناشناخته و جدید، در صورت امکان از انتی‌ویروس‌های نسل جدید و همچنین سامانه‌های دیگر مانند IPS (Intrusion Prevention System) و IDS (Intrusion Detection System) نیز استفاده شود.

پیاده‌سازی سیاست‌های امنیتی بر روی تجهیزات لبه شبکه

تجهیزات لبه شبکه از قبیل روترها و فایروال دروازه ورود به شبکه هستند. هرگونه پیکربندی نامناسب و ناقص بر روی این تجهیزات و یا هرگونه آسیب‌پذیری امنیتی، به آسانی از طرف کاربران خارج از سازمان قابل رصد و کشف است. لازم است firmware های این تجهیزات به‌طور مرتب تازه‌سازی شوند و از پیکربندی تجهیزات نسخه پشتیبان تهیه شود. پورت‌های ورود و خروج کنترل و فیلتر شوند، این تجهیزات جهت تشخیص هرگونه فعالیت مخرب رصد شود. همچنین در صورت امکان، تجهیزات پشتیبان و منابع سخت‌افزاری مازاد برای تجهیزات لبه شبکه در سازمان موجود باشد تا در مواقع ضروری و خرابی این تجهیزات، بتوان شبکه را در اسرع وقت بازیابی کرد.

لاگ‌برداری از دسترسی کاربران به شبکه

به‌دلیل صرفه‌جویی در مصرف منابع IP، استفاده از قابلیت NAT (Network Address Translation) در سازمان‌ها امری مرسوم و پذیرفته شده است که در آن IP شبکه داخلی همه کاربران در ارتباط با شبکه بیرونی به یک IP نگاشت می‌گردد. در صورتی که سیستم یکی از کاربران شبکه به یک بدافزار آلوده و یا عامل حملاتی به خارج از سازمان باشد، رصد و پیگیری IP آلوده داخلی کاری دشوار است. برای پیشگیری از این مشکل و لزوم تشخیص سریع IP های آلوده، لاگ‌برداری از دسترسی کاربران به شبکه امری ضروری است.

مانیتورینگ محیطی و حراست فیزیکی دیتاسنتر

تجهیزات شبکه برای عملکرد صحیح نیاز به شرایط محیطی مناسب دارند. بنابراین یک مدیر شبکه باید با بهره‌برداری از سنسورهای مانیتورینگ محیطی مداوم به‌صورت زنده از وضعیت محیطی دیتاسنتر شامل دما، رطوبت، دود، سیستم تغذیه و UPS آگاه باشد تا در مواقع لازم اقدام مقتضی صورت پذیرد. حراست فیزیکی تجهیزات و دیتاسنتر را هم باید در نظر داشت و در صورت لزوم از طریق دوربین‌های مداربسته تجهیزات کنترل شوند.

ارزیابی امنیتی شبکه و سامانه‌ها

آسیب‌پذیری‌های فضای مجازی به شکل گسترده‌ای در حال افزایش هستند و حتی به‌روزترین سامانه‌ها نیز دچار آسیب‌پذیری می‌شوند. برای حفظ امنیت سامانه‌ها و حریم خصوصی کاربران لازم است آسیب‌پذیری‌های امنیتی و پیکربندی‌های ناصحیح سامانه‌ها به صورت مداوم رصد شود. برای این منظور انجام آزمایش‌های تست‌نفوذ به‌صورت دوره‌ای پیشنهاد می‌گردد.

سامانه‌های کاربردی

شناسه واحد و SSO

با افزایش روز افزون تعداد سامانه‌های یک سازمان، عموماً بر تعداد اکانت‌های کاربری هر فرد در سازمان افزوده می‌شود. به‌دلیل تعدد این اکانت‌ها، مدیریت آن‌ها شامل نگهداری و تعویض به‌موقع گذرواژه‌ها برای کاربران کار مشکلی است و همچنین فراموشی نام کاربری و رمزعبور به وفور اتفاق می‌افتد. برای حل این مشکل، می‌توان از گزینه‌های شناسه واحد و SSO (Single Sign On) استفاده کرد. برای این کار لازم است یک سامانه مرکزی مدیریت کاربران بر بستری مانند Active Directory ایجاد شود. با عضویت سرورهای مورد نظر در دامین یا گرفتن وب سرویس از AD برای سامانه‌های مورد نظر، امکان ورود به همه سامانه‌ها تنها با یک اکانت کاربری وجود دارد. همچنین در سرویس SSO، کاربر با یک بار لاگین به این سرویس به بقیه سرویس‌های مورد نظر دسترسی پیدا می‌کند.

شناسه واحد و SSO علیرغم داشتن مزایای زیاد و سادگی استفاده، از نظر امنیتی می‌توانند مشکل ساز باشند چرا که با لو رفتن اطلاعات حساب کاربری، امنیت همه سامانه‌ها به خطر می‌افتد. لذا لازم است در این مورد تمهیدات لازم اتخاذ شود. همچنین از ارسال اطلاعات حساب‌کاربری به‌صورت رمزگذاری نشده بر روی شبکه پرهیز شود، گذرواژه‌ها دارای پیچیدگی کافی باشند و کاربران از اهمیت حفظ حساب‌کاربری آگاه باشند.

سامانه ثبت‌نام کاربران و مدیریت حساب‌کاربری

ایجاد حساب‌کاربری برای کاربران جدید یک سازمان، ایجاد دسترسی به سامانه‌ها و کنترل دسترسی یکی از چالش‌های سازمان‌های بزرگ مانند دانشگاه‌ها است که مقاطع مشخصی با حجم زیادی از کاربران مواجه می‌شوند. در این سازمان‌ها لازم است یک سامانه احراز هویت و ثبت‌نام کاربران ایجاد شود. علاوه‌بر ثبت‌نام کاربران، هر کاربر باید قادر باشد به حساب‌کاربری خود لاگین کرده و اطلاعات حساب‌کاربری را ویرایش نماید. در این سامانه باید امکان اعمال کلمه‌عبور جدید در هنگام فراموشی کلمه‌عبور از طریق شماره همراه یا ایمیل وجود داشته باشد.

دانلود درون سازمانی

حجم زیادی از نرم‌افزارهای مورد استفاده کاربران در یک سازمان مشترک است و در مواقع ضروری هر کاربر راساً اقدام به دانلود و نصب نرم‌افزار مورد نظر می‌نماید. برای صرفه‌جویی در مصرف پهنای باند سازمان و همچنین دسترسی کاربران با تاخیر کم، می‌توان یک بانک از نرم‌افزارهای مورد نیاز کاربران را بر روی یک سرور داخلی گردآوری نمود. از آنجایی‌که دانلود نرم‌افزار از سایت‌های مخرب عامل نفوذ بدافزار به داخل شبکه است سامانه دانلود درون سازمانی می‌تواند به ارتقاء امنیت سازمان نیز کمک نماید.

تهیه و تازه‌سازی توپولوژی شبکه دیتاسنتر

مستندسازی ساختار و توپولوژی شبکه از ضروریات یک شبکه سازمانی است. این مستندسازی علاوه‌بر اینکه در ارائه و معرفی شبکه مفید است برای عیب‌یابی و رفع نقص در شبکه هم می‌تواند کمک شایانی نماید.

پشتیبان‌گیری از پیکربندی تجهیزات

ارائه سرویس مطمئن در یک سازمان وابسته به عملکرد درست تجهیزات آن از قبیل روتر، سویچ، فایروال و غیره می‌باشد. گاهاً به دلایل مختلف این تجهیزات دچار مشکل می‌شوند و پیکربندی آن‌ها دچار خطا می‌شود. برای رفع این مشکل لازم است از پیکربندی صحیح تجهیزات نسخه پشتیبان تهیه نمود تا در مواقع لازم بتوان تجهیزات دارای مشکل را بازیابی کرد.

توسعه و ارتقاء منابع سخت‌افزاری

یکی از نیازهای مهم در عملکرد صحیح شبکه وجود منابع سخت‌افزاری مناسب است. با افزایش روزافزون سامانه‌ها و گسترش حجم داده سازمانی، معمولاً مصرف منابع سخت‌افزار شامل حافظه‌ها و پردازنده‌ها زیاد می‌شود. با توجه به طولانی بودن فرآیند تهیه منابع، مخصوصاً در سازمان‌های دولتی، لازم است یک مدیر شبکه همیشه پیش‌بینی‌هایی از منابع مورد نیاز در آینده داشته باشد و پیشاپیش نسبت به تهیه آن‌ها اقدام نماید.

توانمندسازی نیروی فناوری اطلاعات

بسترها و سرویس‌های فناوری اطلاعات پویا هستند و نیاز است دانش کارشناسان این حوزه متناسب با آن تازه‌سازی شود. دوره‌های آموزشی، کارگاه‌ها و وبینارها می‌تواند در این زمینه مفید باشد. همچنین یکی از روش‌های موثر انتقال و اشتراک دانش و تجربیات بین کارشناسان یک سازمان و یا چند سازمان است که ضمن به‌روزرسانی دانش افراد می‌تواند عاملی برای شناسایی راه‌حل‌های چالش‌های سازمان باشد.

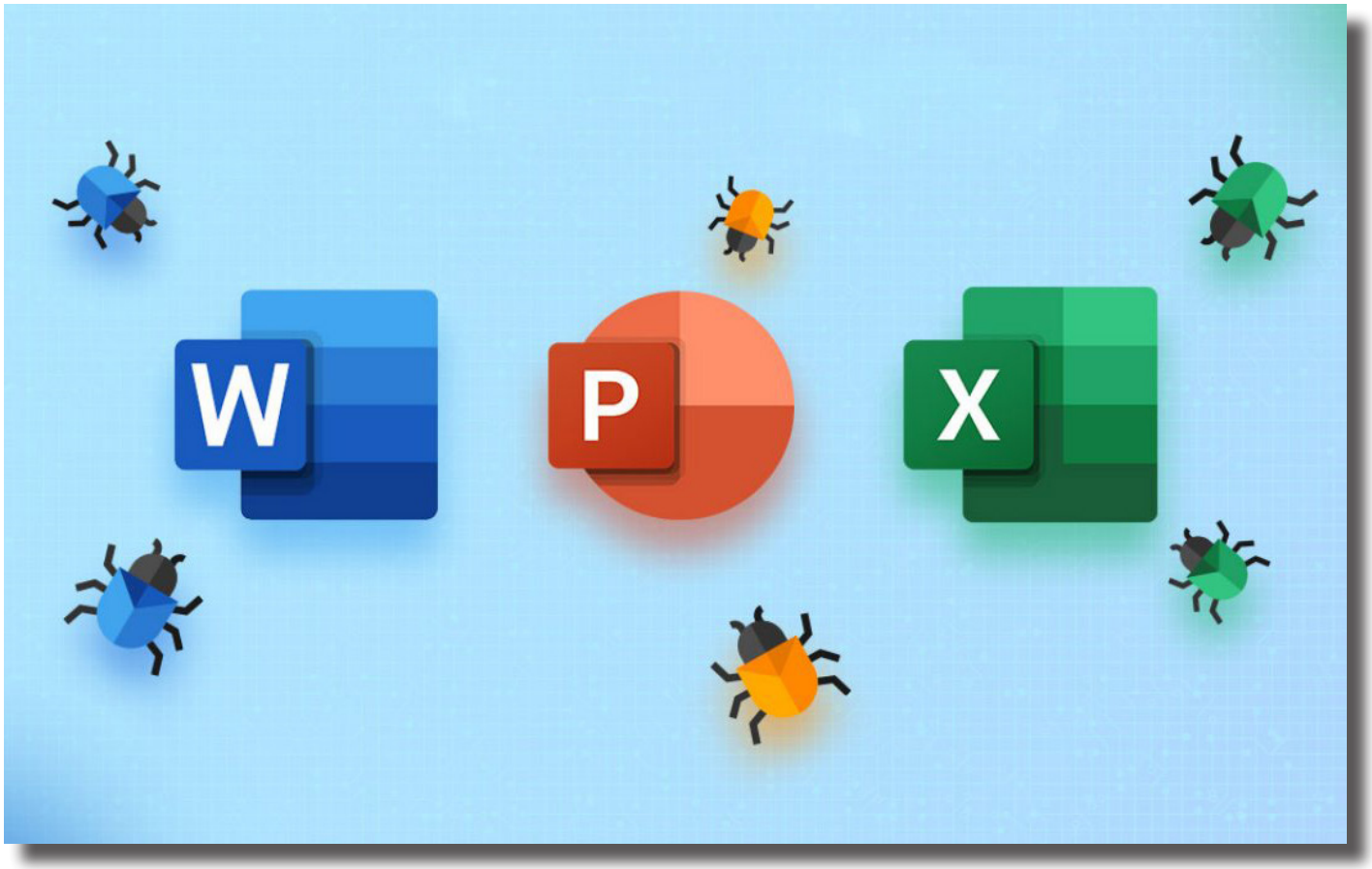
ارزیابی عملکرد سرویس‌های موجود و نیازسنجی سرویس‌های جدید

به‌دلیل تغییرات یک سازمان از جنبه‌های گوناگون، نیازمندی‌های آن و به طبع سرویس‌ها و بسترهای آن در طول زمان تغییر می‌کند. لذا لازم است از سرویس‌های موجود ارزیابی مستمر از لحاظ رضایت و برآوردسازی نیازها صورت گیرد و همچنین برای آینده سازمان متناسب با نیازمندی‌های پیش‌رو برنامه‌ریزی صورت گیرد. این برنامه‌ریزی می‌تواند در سطوح متفاوت و متناسب با برنامه استراتژیک سازمان باشد.

هادی گلباغی
h.golbaghi@uok.ac.ir

مقاله آموزشی

ماکروها در مجموعه آفیس، مفید یا مخرب؟



مقدمه

می‌توان گفت در دو دهه اخیر مجموعه آفیس به یکی از پرکاربردترین نرم‌افزارهای مورداستفاده کاربران تبدیل شده است. این مجموعه مورد استفاده کاربران عادی می‌باشد و همچنین کارمندان در ادارات و شرکت‌ها و نیز افراد متخصص در حوزه‌های مختلف از کاربردهای متفاوت این مجموعه بهره برده‌اند. کارکردهای این مجموعه برای اموری مانند تایپ‌کردن، ایجاد و ویرایش اسناد، انجام محاسبات ریاضی، ارائه و سخنرانی، مدیریت پایگاه‌های داده و ارسال و دریافت اطلاعات از ایمیل و ده‌ها عملیات دیگر است. سه نرم‌افزار پرکابرد این مجموعه Word ،Excel و PowerPoint هستند که به دلایل و استفاده‌های مختلف فایل‌های آن‌ها اغلب بین کاربران ردوبدل می‌شود. نکته‌ای که اغلب کاربران در مورد آن اطلاعاتی ندارند این است که نرم‌افزارهای این مجموعه، از ماکرونویسی پشتیبانی می‌کنند. یکی از روش‌هایی که مهاجمان و گروه‌های هکری از آن سوءاستفاده می‌کنند این است که کدهای مخرب را ایجاد کرده و آن را مبهم‌سازی می‌کنند و از طریق فایل‌های مجموعه آفیس به‌وسیله روش‌های مختلف مهندسی اجتماعی، آن را برای قربانیان ارسال می‌کنند و فرایند آلوده‌سازی سیستم قربانیان را شروع می‌کنند. جالب است که شروع استفاده از این نوع حملات به دهه‌ی ۹۰ میلادی می‌رسد و بر اساس گزارش سیسکو بیش از ۳۸ درصد بدافزارهای ارسالی از طریق ایمیل، در قالب فایل‌های آفیس هستند. در گزارش دوره‌ای که توسط آزمایشگاه امنیت سایبری مک‌آفی مربوط به سال ۲۰۲۱ منتشر شده است اشاره شده که آمار مربوط به تعداد بدافزارهای مجموعه آفیس به نسبت گزارش دوره‌ای قبل این آزمایشگاه، ۱۹۹ درصد افزایش را نشان می‌دهد که این خود زنگ خطری برای کاربران در ارتباط به نرخ تکثیر آلودگی فایل‌های مخرب مجموعه آفیس است. همچنین گزارشی از سایت Cofense نشان داده است که در میان مهاجمان سایبری، ضمیمه‌کردن فایل‌های مجموعه آفیس دارای ماکروها در ایمیل یک روش اصلی برای جاسازی پیلود مخرب است. در تحلیل‌های این گزارش آمده است، از بین مکانیسم‌های انتشار بدافزار، ۴۵ درصد از مهاجمان اسناد آفیس را برای تحویل ماکروهای مخرب انتخاب می‌کنند؛ زیرا به‌راحتی بر روی یک سیستم فعال می‌شوند و یا در بدترین حالت نیاز به یک کلیک برای اجراشدن دارند. به‌همین دلیل ماکروها یک بخش مهم برای راه‌اندازی اولین مرحله از زنجیره انتشار آلودگی هستند.

ازجمله بدافزارهایی که از این روش برای انتشار استفاده می‌کنند می‌توان به AZORult, Chanitor, Geod و GandCrab اشاره کرد. همچنین طبق بررسی مایکروسافت در چند سال اخیر بدافزارهای ماکرو در خانواده‌های زیر مشاهده شده‌اند:

- Ransom:MSIL/Swappa
- Ransom:Win32/Teerac
- TrojanDownloader:Win32/Chanitor
- TrojanSpy:Win32/Ursnif
- Win32/Fynloski
- Worm:Win32/Gamarue

نکته حائز اهمیت این است که مهاجمان و بدافزارنویسان با تقویت و رشد توان ضدبدافزارها و انتی‌ویروس‌ها به طور مداوم روش و تکنیک‌های خود را به‌روز کرده و از شیوه‌های نوین در بدافزارهای خود برای فرار از شناسایی شدن و دور زدن فیلترهای امنیتیِ ایجاد شده توسط ضدبدافزارها و نرم‌افزارهای امنیتی بهره می‌برند.

در ادامه درخصوص ماکروها در مجموعه آفیس و استفاده سوء و مخرب از آن‌ها توضیحاتی داده خواهد شد.

ماکرو

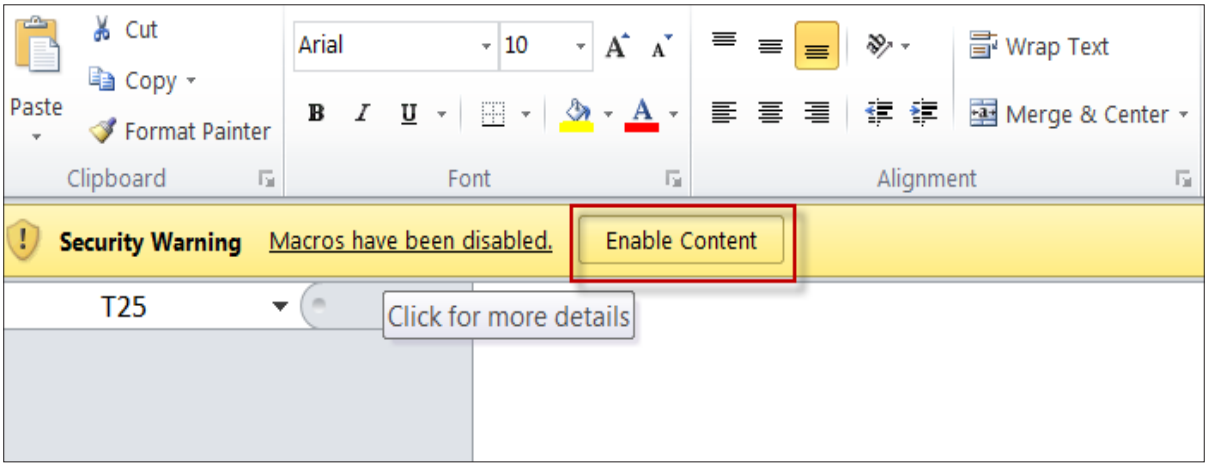
به زبان ساده ماکرو مجموعه‌ای از دستورات و تابع‌های ذخیره شده است که یک بار نوشته شده و بارها مورد استفاده قرار می‌گیرد. درحقیقت یك ماکرو با هدفی مشخص یکبار ایجاد و به‌صورت مداوم از آن استفاده می‌شود. با این شیوه می‌توان تعدادی دستور را در قالب یك ماکرو ذخیره کرد و همگی آن‌ها را همزمان اجرا کرد. زبان برنامه‌نویسی ماکرو، اغلب زبان اسکریپتی بوده و با دسترسی مستقیم به ویژگی‌های برنامه ممکن است برخی امور را در جهت سهل‌کردن کارکردهای مختلف به‌صورت خودکار پیاده‌سازی کند. مزایای استفاده از ماکروها به شرح زیر است:

- اجرای مجموعه‌ای از دستورات به‌صورت همزمان
- سرعت بخشیدن به عمل ویرایش و قالب‌بندی سند
- اجرا کردن خودکار دستورات
- ضبط و ذخیره‌کردن کارهای تکراری و استفاده مجدد از آن
- امکان ویرایش و توسعه دادن کدهای ذخیره شده
- بازیابی و انتقال داده‌های موجود در موقعیت‌های مختلف به‌منظور رسم نمودارهای مختلف

برای سهولت پیاده‌سازی ماکروها، زبان برنامه نویسی Visual Basic for Applications یا VBA توسط مایکروسافت معرفی شد. VBA نوعی زبان برنامه‌نویسی است که توسط مایکروسافت و با هدف کنترل قسمت‌های مختلف نرم‌افزارهای این کمپانی طراحی شده است. بسیاری از کارهایی که کاربران در سیستم و نرم‌افزارهای مایکروسافتی می‌توانند با استفاده از موس و کیبورد انجام دهند با استفاده از زبان ویژوال بیسیک و ماکرونویسی در مجموعه آفیس نیز قابل انجام است. برای مثال همان‌طور که در اکسل می‌توان یک نمودار طراحی کرد، با استفاده از زبان VBA نیز می‌توان این کار را انجام داد.

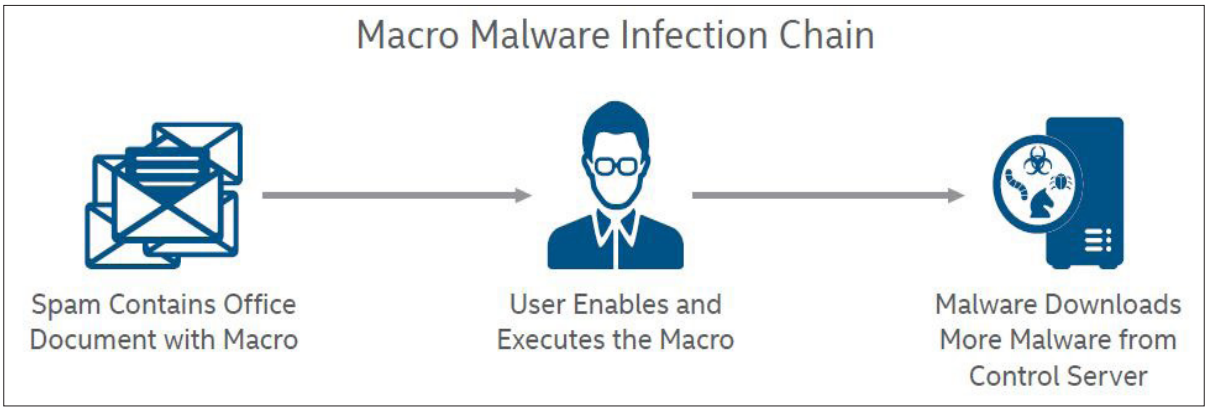
استفاده از VBA برای ایجاد ماکروها باعث می‌شود در این خصوص آزادی عمل بیشتری پیدا کرده و به توابع و قابلیت‌های بیشتری دسترسی پیدا کرد.

باتوجه به موارد گفته شده ماکروها و زبان VBA مزیت‌های زیادی دارند و در تسهیل امور به کاربران کمک شایانی کرده‌اند اما از جهتی دیگر دارای جنبه‌های منفی نیز هستند. مهاجمان و نفوذگران سایبری از همان اوایل معرفی و استفاده از ماکروها و زبان VBA، از این قابلیت‌ها برای فعالیت‌های مخرب و آلوده‌کردن سیستم کاربران بهره برده‌اند. پیدایش نخستین گونه از فایل‌های مخرب VBA به اواخر سال‌های دهه ۹۰ میلادی باز می‌گردد. در همه این سال‌ها اخبار مربوط به سوءاستفاده از ماکروها برای انجام فعالیت‌های مخرب منتشر می‌شد اما در سال‌های اخیر شمار این نوع بدافزارها رو به افزایش بوده است. طبق گزارش‌های شرکت امنیتی Sophos، بدافزار ماکرو عملاً نقطه شروع بسیاری از حملات هستند. باید توجه داشت که استفاده از کد مخرب VBA تمام داستان نیست. در بسیاری مواقع با باز شدن فایلی آلوده از مجموعه آفیس حاوی کد مخرب VBA که به یک هرزنامه پیوست شده است، در پشت صحنه و بدون اطلاع کاربر، فایل اجرایی بدافزار اصلی دانلود شده و سپس نصب و اجرا می‌شود. البته در نسخه‌های قبل از آفیس ۲۰۰۷ ماکروها می‌توانستند به‌صورت خودکار و بدون اجازه کاربر و فقط با بازشدن فایل آلوده اجرا شوند اما در نسخه‌های بعد آن، این قابلیت و اجرای آن با اجازه کاربر ممکن است. عکس زیر پیامی که در صورت وجود ماکرو در یک فایل Word وجود دارد را نشان می‌دهد که در صورت زدن Enable این قابلیت فعال خواهد شد. توصیه می‌شود در صورتی که از صحت فایل اطمینان کامل ندارید فعال‌سازی انجام نشود.



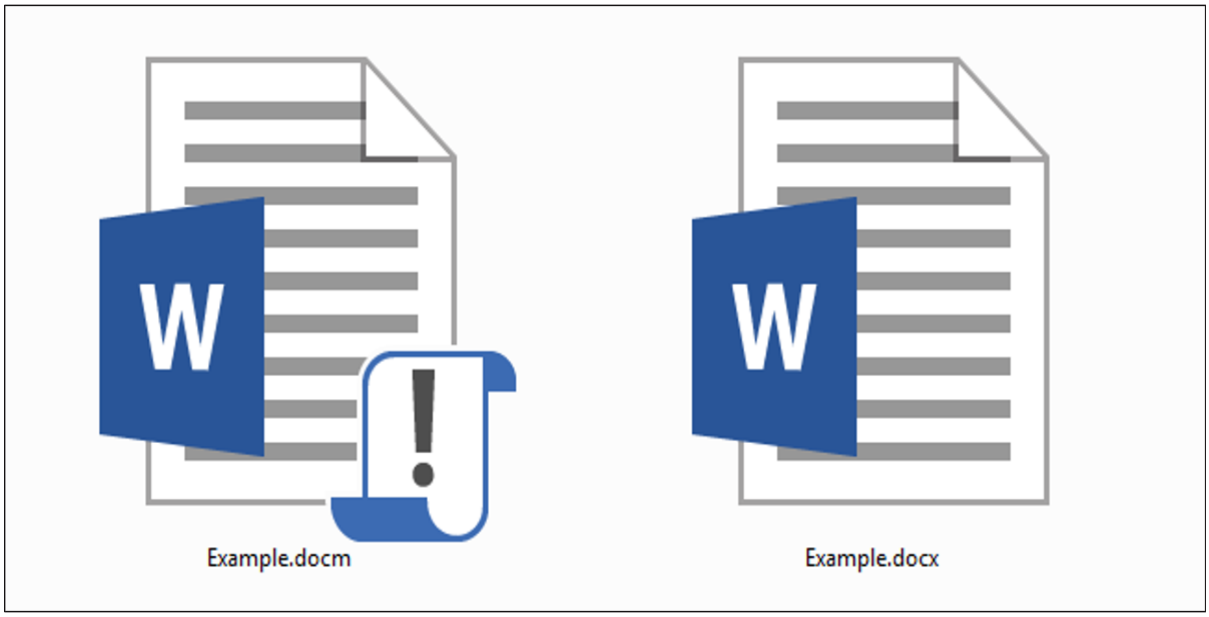
بدافزارهای ماکرو

اگر بخواهیم زنجیره آلودگی یک بدافزار ماکرو را نشان دهیم این فرآیند به صورت زیر خواهد بود.



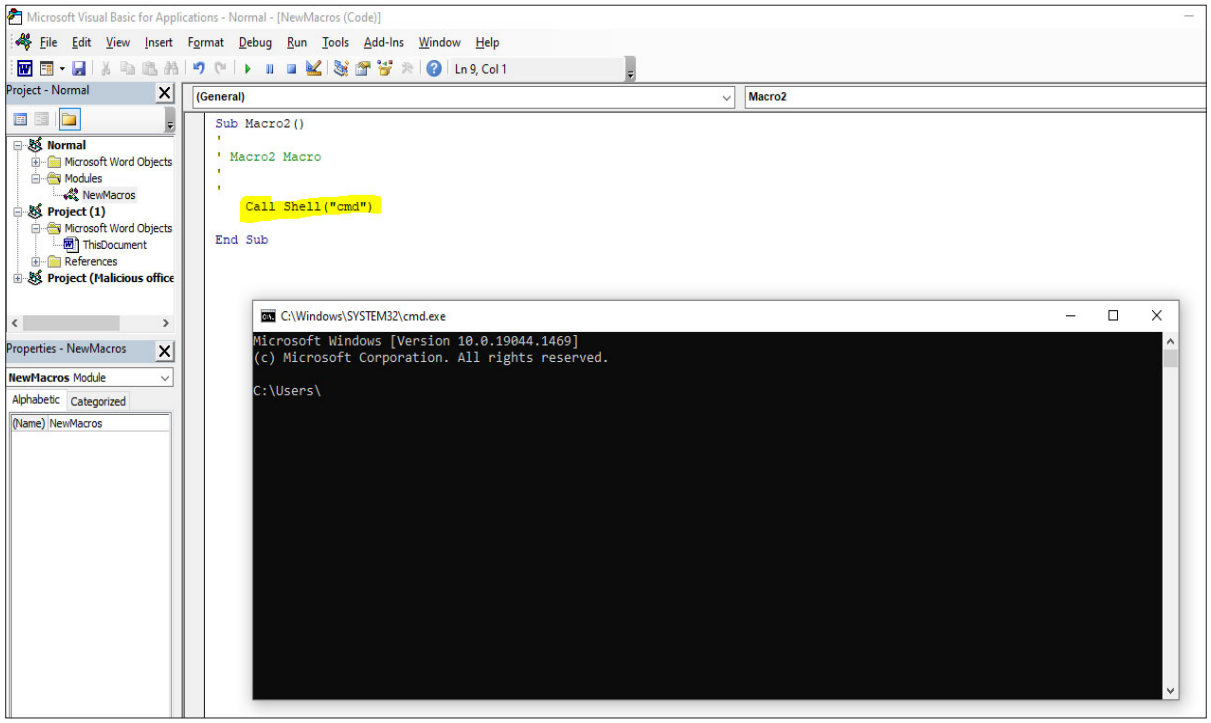
یکی از شیوه‌های مرسوم برای شروع حملات، هرزنامه‌هایی است که فایل‌های مجموعه آفیس مخرب را در پیوست خود دارند. کاربر با دریافت این فایل‌های مخرب و فعال‌کردن اجرای ماکرو، آن را اجرا می‌کند و فرایند آلوده‌سازی سیستم شروع می‌شود. از طرفی دیگر مایکروسافت از آفیس ۲۰۰۷ به بعد قابلیتی را برای اجرای ماکروها در اسناد ایجاد کرد.

به‌طورمثال فایل‌های WORD با پسوند DOCX بودند اما در این قابلیت جدید از پسوند DOCM با توانایی اجرای ماکرو استفاده شده است. در عکس زیر تفاوت دو فایل از این نوع را از نظر شکل آیکون و فرمت آن مشاهده می‌کنید.

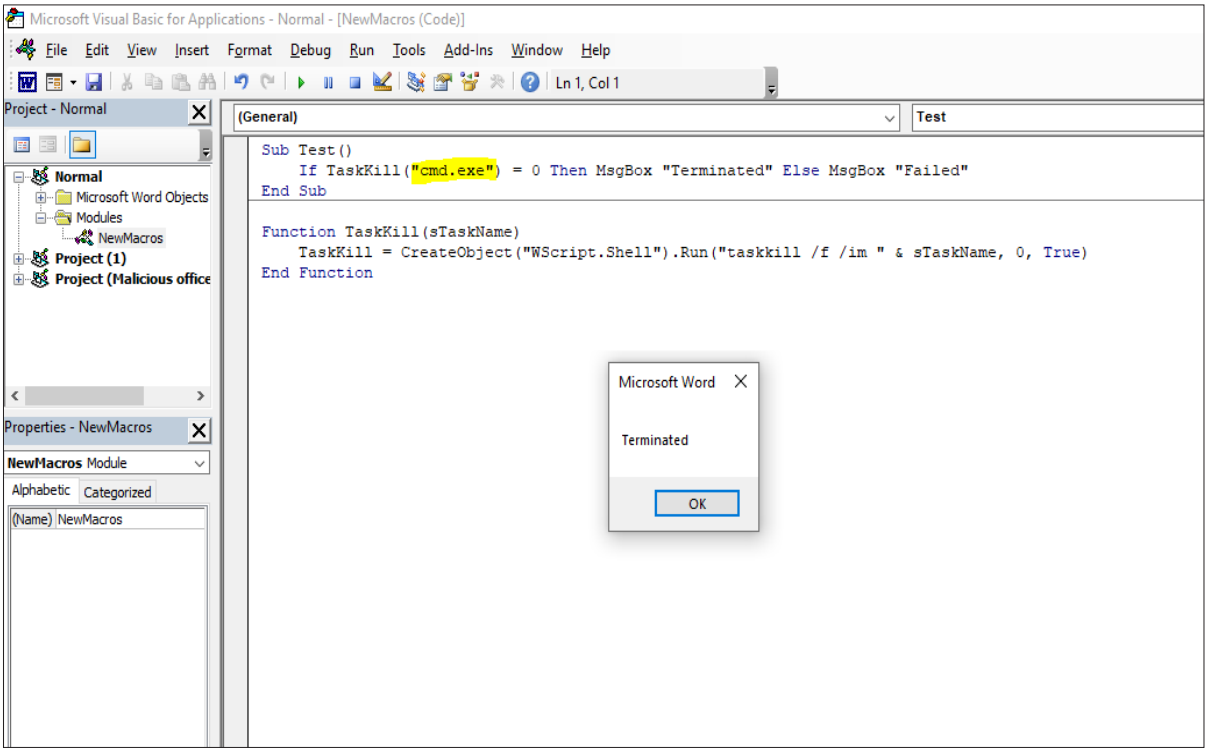


همین مورد برای فایل‌های اکسل با پسوند XLSM و برای فایل‌های پاورپوینت با پسوند POTM صادق است. موضوعی که می‌تواند بسیار خطرناک باشد این است که اکثر کاربران با توجه به شباهت‌های این دو نوع فایل، ممکن است به شکل ظاهری و پسوند فایل توجه نکنند و از طریق مختلفی مانند ارسال از طریق پیام‌رسان‌ها، پیوست ایمیل‌ها یا هرزنامه‌ها و یا هر روش دیگری فایل‌هایی با پسوند XLSM، DOCM یا POTM که حاوی ماکرو آلوده با فعالیتی مخرب است را دریافت کنند و بدون توجه به میزان ریسک، آن را اجرا کنند!

نکته حائز اهمیت این است که ماکروها با استفاده از فرامین و دستورات VBA SHELL قادر به اجرای دستورات و برنامه‌های دلخواه هستند و با بهره‌گیری از فرامین VBA KILL می‌توانند فایل‌ها و برنامه‌ها را از سیستم شما حذف کنند. برای نمونه در عکس زیر مشاهده می‌کنیم که در قالب یک ماکرو در فایل Word با استفاده از دستورات VBA می‌توان CMD را در سیستم اجرا کرد.

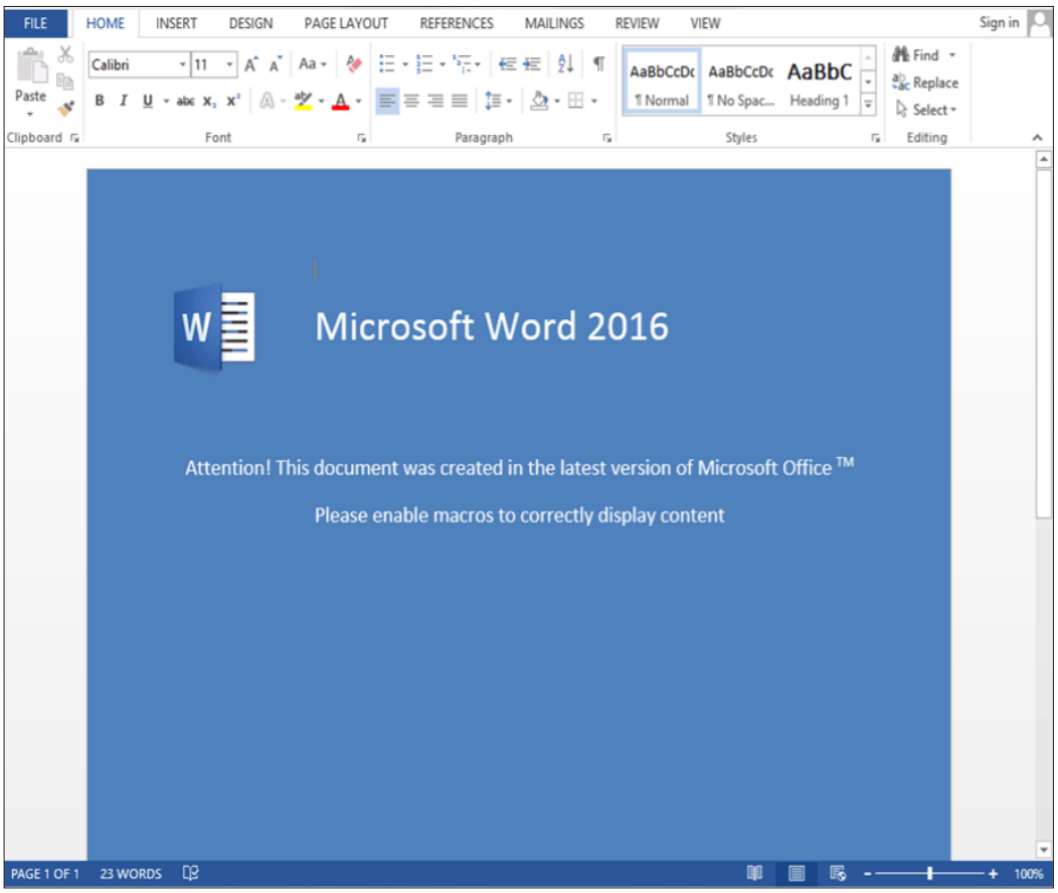


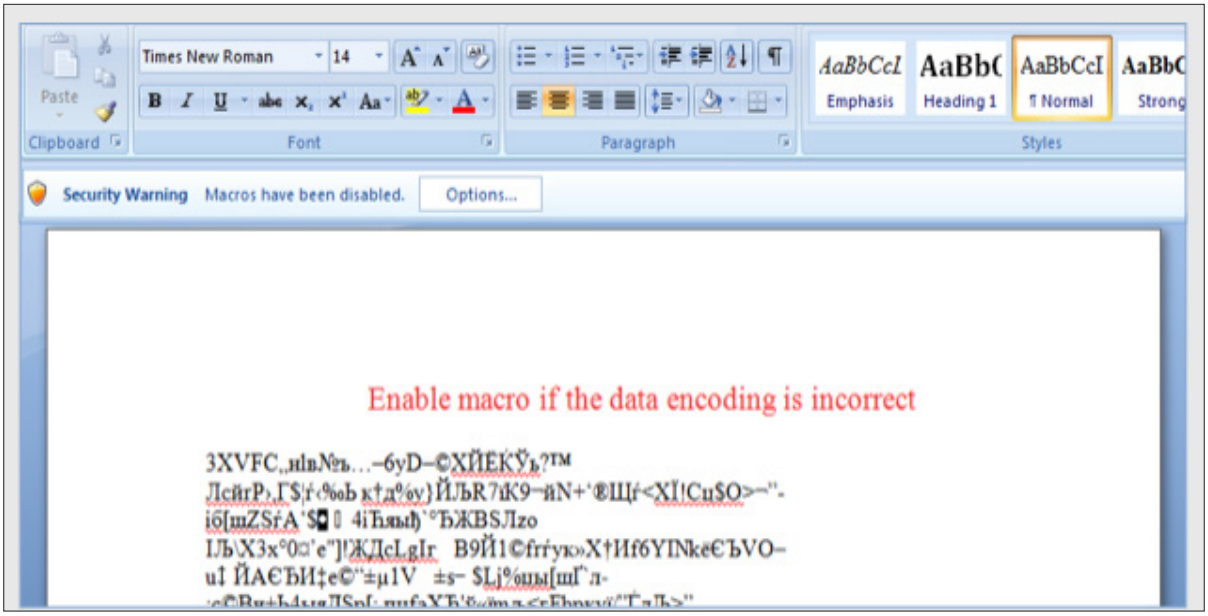
در ادامه در عکس زیر مشاهده می‌کنید که CMD در ماکرو قبل اجرا شد را می‌توان با یک ماکرو جدید متوقف و اصطلاحاً پروسه آن را KILL کرد.

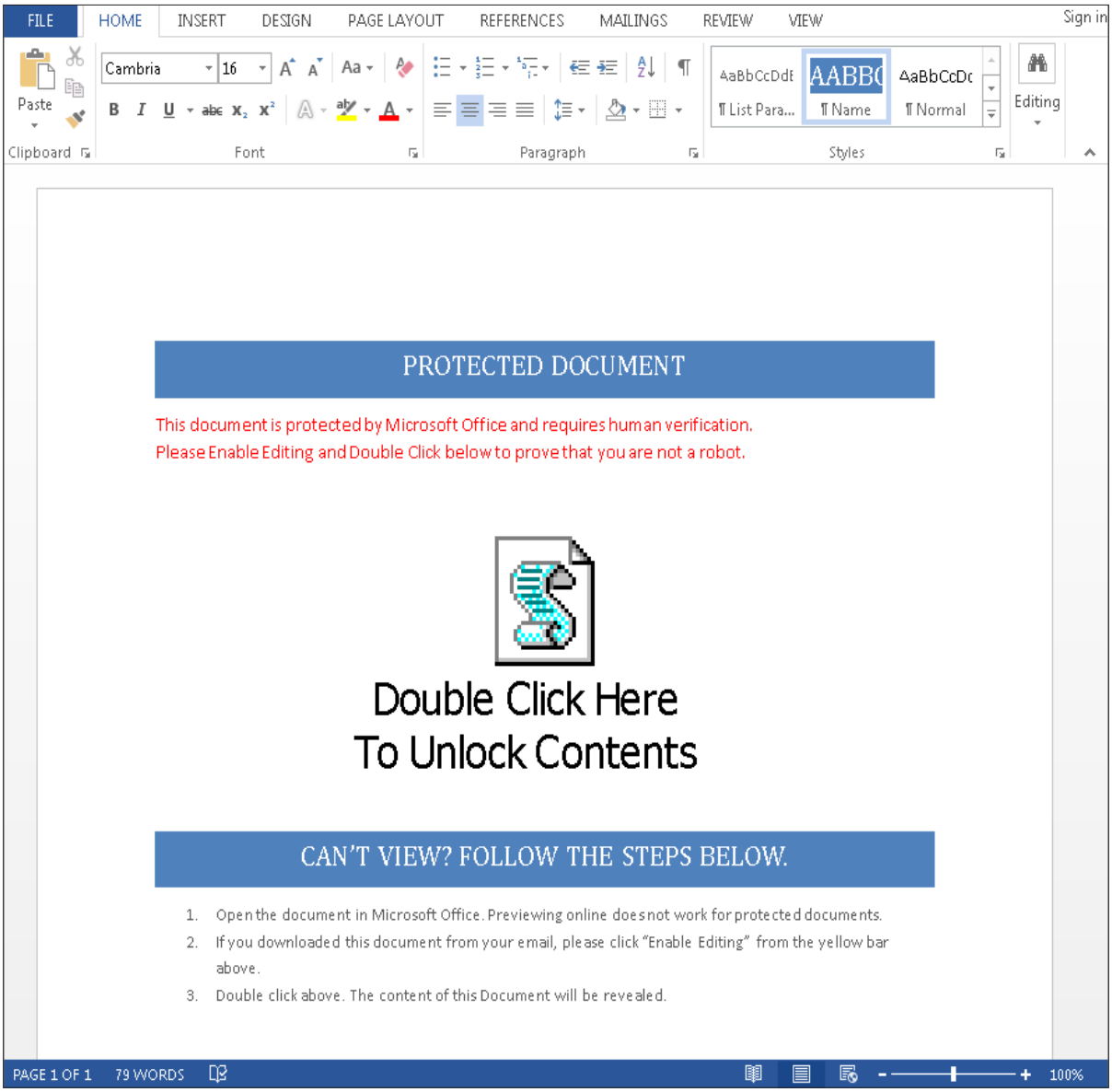


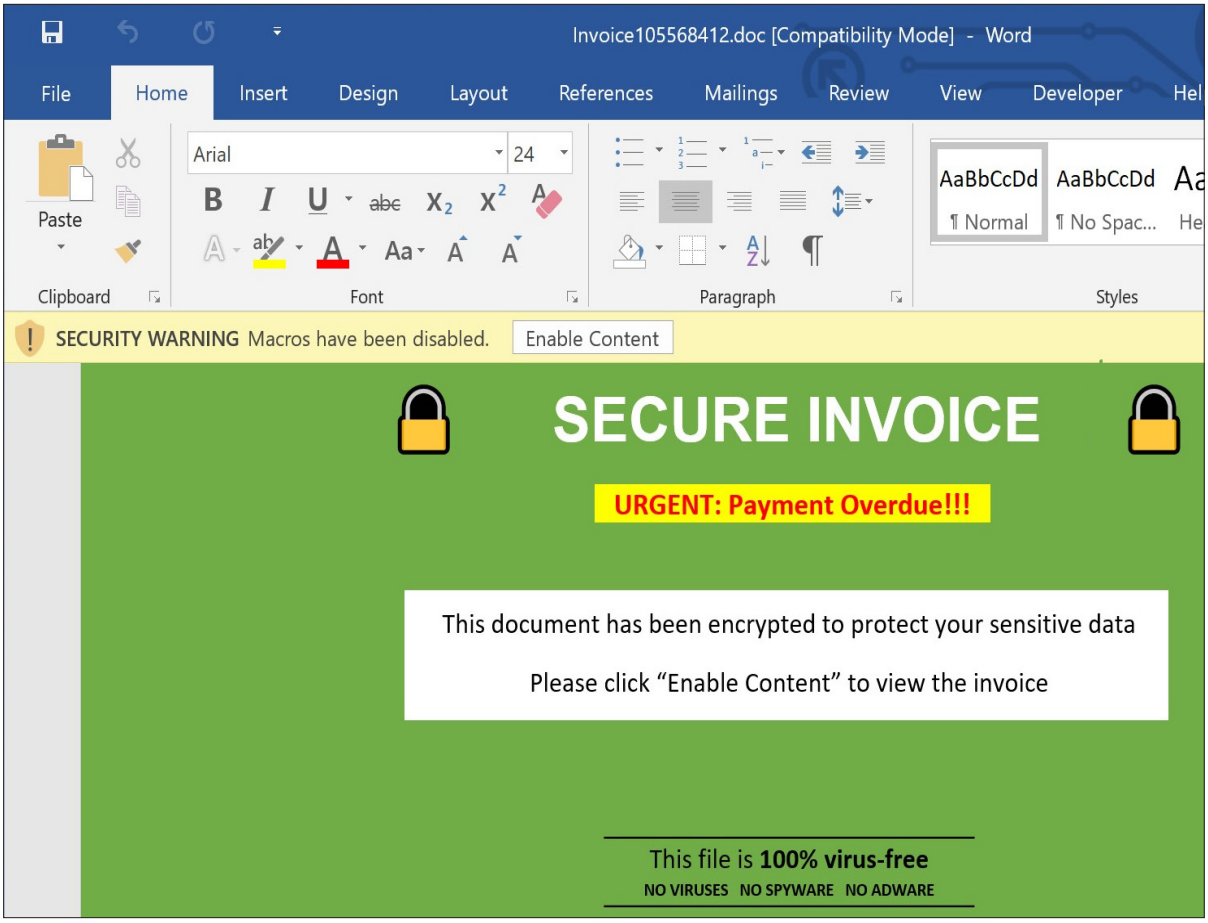
باید توجه داشت که مثال‌هایی که در این مطلب ذکر شد، ساده‌ترین حالت ممکن است و دسترسی‌های بسیار بیشتر و پیشرفته‌تری که پتانسیل مخرب‌تری دارند نیز به‌راحتی قابل انجام است.

در سال‌های اخیر نکته‌ای که آزمایشگاه امنیت سایبری مک‌آفی در کمپین‌های فیشینگ مشاهده کرده است این بوده که این کمپین‌ها با استفاده از روش‌های مختلف کاربر را ترغیب به فعال‌سازی اجرای ماکرو در فایل‌های مجموعه آفیس می‌کنند و قربانیان را به زنجیره آلوده‌سازی خود اضافه می‌کنند. در عکس‌های زیر مشاهده می‌کنیم که از همین روش برای ترغیب کاربر برای فعال‌سازی اجرای ماکرو بهره برده‌اند.




Times New Roman
14
Paste
Clipboard
Font
Paragraph
Styles
Emphasis
Heading 1
¶ Normal
Strong
Security Warning
Macros have been disabled.
Options...
Enable macro if the data encoding is incorrect


FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
Sign in
Cambria
16
Paste
Clipboard
Font
Paragraph
¶ List Para...
¶ Name
¶ Normal
Styles
Editing
PROTECTED DOCUMENT
This document is protected by Microsoft Office and requires human verification.
Please Enable Editing and Double Click below to prove that you are not a robot.
Double Click Here
To Unlock Contents
CAN'T VIEW? FOLLOW THE STEPS BELOW.
1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Double click above. The content of this Document will be revealed.
PAGE 1 OF 1
79 WORDS
100%



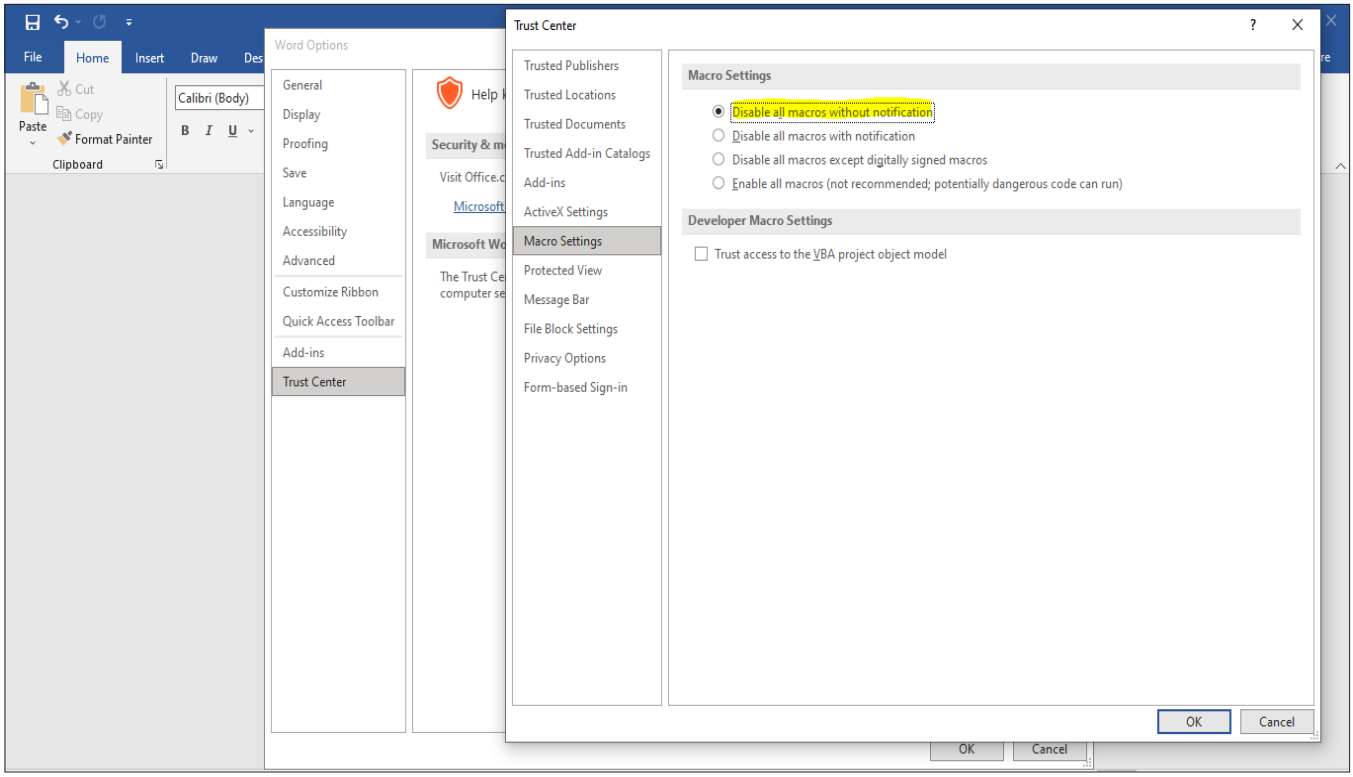
همچنین مهاجمان به‌صورت پیوسته تکنیک‌های جدید را برای آلوده‌سازی سیستم کاربران با استفاده از ماکروهای مخرب به‌کار می‌گیرند که برخی از این تکنیک‌ها شامل مبهم‌سازی ماکروها، دور زدن مکانیزم غیرفعال شدن ماکرو، LOLBAS، DDE و حتی استفاده از فرمت‌های پشتیبانی‌شده XLS برای اجرای تمامی عملیات‌ها است. مهاجمان در حملات اخیر روش‌های خود را به سمتی هدایت کرده‌اند که هیچ پیام، هشدار یا سوالی از کاربر برای اجرای ماکرو، با وجود غیرفعال بودن اجرای ماکرو، نداشته باشند. همچنین با وجود استفاده از Microsoft Office sandbox برای اجرای امن‌تر ماکروها در مجموعه آفیس، مهاجمان برای اجرای ماکروی مخرب خود درصدد دور زدن این مکانیزم و اجرای آن خارج از محیط سندباکس هستند. این نکته حائز اهمیت است که با استفاده از ابزارهای مختلفی مانند Metasploit امکان دارد پیلودهای مخرب و مبهم‌سازی شده برای VBA ایجاد گردد و از این پیلودها در پیاده‌سازی ماکرو اصلی بهره برد که می‌تواند بسیار خطرناک باشد.

بدافزارهای ماکرو

رعایت توصیه‌های زیر درخصوص در امان ماندن از آلودگی‌های فایل‌های مخرب با استفاده از ماکروها ضروری به نظر می‌رسد:

- اطمینان حاصل کنید که در مجموعه آفیس مورد استفاده در سیستم خود و حتی سیستم‌های زیرمجموعه، اجرای ماکرو غیر فعال شود. این کار از طریق منوی زیر در مجموعه آفیس قابل انجام است.

Options --> Trust Center --> Trust Center Settings --> Macro Settings --> Disable all macros without notification



- به‌هیچ‌عنوان ایمیل‌های مشکوک و پیوست‌های آن را باز، دانلود و اجرا نکنید.

- ایمیل‌هایی که از طرف اشخاص ناشناس است و یا محتوای مشکوکی دارد را حذف کرده و آن را در دسته هرزنامه‌ها قرار داده و گزارش کنید.

- در صورت دریافت فایل‌های مجموعه آفیس از طریقی دیگر مانند پیام‌رسان‌ها، فلش، دانلود از سایت، اتوماسیون و غیره نیز احتیاط‌های لازم صورت گیرد.

- توجه به این نکته ضروری است که یکی از روش‌های پیشگیری از آلودگی به باج‌افزارها عدم استفاده از ماکروها در فایل‌های مجموعه آفیس می‌باشد.

- در صورتی که مجبور به دانلود فایل‌های مجموعه آفیس از منبعی نامطمئن بودید حتما آن فایل را با انتی‌ویروس خود و یا یکی از انتی‌ویروس‌های آنلاین مانند virustotal.com اسکن کنید. حتی با استفاده از این سایت می‌توانید قبل از دانلود فایل، لینک فایل را نیز اسکن کرده و در صورتی که مخرب باشد دانلود را انجام ندهید.

- در صورت داشتن دانش برنامه‌نویسی، قبل از اجرای ماکرو، سورس کد آن را مشاهده کرده و روند اجرایی آن را کنترل کنید و در صورت مشاهده هرگونه فرایند مشکوک، آن را اجرا نکنید.

سخن پایانی

در گزارش‌هایی که اخیراً توسط مایکروسافت درخصوص انتشار نسخه ۲۰۲۳ از مجموعه آفیس منتشر شده است حاکی از آن است که مایکروسافت قصد دارد ماکروها را در پنج نرم‌افزار اصلی این مجموعه یعنی Excel، Word، Access، Power Point و Visio غیرفعال کند. بعد از اعمال این تغییر، هنگام باز کردن فایل‌های دارای ماکرو، به جای گزینه Enable Editing، پیامی حاوی ریسک موجود در اجرای ماکروهای فایل و یک گزینه‌ی Learn More به کاربر نمایش داده می‌شود. کاربر با کلیک بر روی گزینه Learn More به صفحه‌ای هدایت می‌شود که در آن راهنمایی برای فعال کردن ماکروها با ذخیره فایل و حذف MOTW آورده شده است.

محمد حبیبی
m.habibi@uok.ac.ir

آسیب‌پذیری

جدیدترین آسیب‌پذیری‌های شناخته‌شده که مورد سوء استفاده قرار گرفته‌اند.

مقدمه

CISA چند آسیب‌پذیری جدید را به کاتالوگ آسیب‌پذیری‌های شناخته شده خود اضافه کرده است. براساس شواهد به‌دست آمده مهاجمین به‌صورت فعال از این آسیب‌پذیری‌ها استفاده کرده‌اند، این آسیب‌پذیری‌ها در حملات گسترده‌ای توسط عوامل سایبری استفاده شده است و خطرات قابل توجهی برای شرکت و سازمان‌ها به همراه دارند.

لیست آسیب‌پذیری‌ها

آسیب‌پذیری‌های ذکر شده از سال ۲۰۱۳ تا ۲۰۲۲ می‌باشند و ترتیب و اولویت‌بندی خاصی ندارند.

CVE Number	CVE Title	Remediation Due Date
CVE-2021-22017	VMware vCenter Server Improper Access Control Vulnerability	24/01/2022
CVE-2021-36260	Hikvision Improper Input Validation Vulnerability	24/01/2022
CVE-2021-27860	FatPipe WARP, IPVPN, and MPVPN Privilege Escalation vulnerability	24/01/2022
CVE-2020-6572	Google Chrome prior to 81.0.4044.92 Use-After-Free Vulnerability	10/07/2022
CVE-2019-1458	Microsoft Win32K Elevation of Privilege Vulnerability	10/07/2022
CVE-2013-3900	Microsoft WinVerify Trust Function Remote Code Execution Vulnerability	10/07/2022
CVE-2019-2725	Oracle WebLogic Server, Injection Vulnerabilitynerability	10/07/2022
CVE-2019-9670	Synacor Zimbra Collaboration Suite Improper Restriction of XML External Entity Reference Vulnerability	10/07/2022
CVE-2018-13382	Fortinet FortiOS and FortiProxy Improper Authorization Vulnerability	10/07/2022
CVE-2018-13383	Fortinet FortiOS and FortiProxy Improper Authorization Vulnerability	10/07/2022
CVE-2019-1579	Palo Alto Networks PAN-OS Remote Code Execution Vulnerability	10/07/2022
CVE-2019-10149	Exim Mail Transfer Agent (MTA) Improper Input Validation Vulnerability	10/07/2022
CVE-2015-7450	IBM WebSphere Application Server and Server Hy Server Hypervisor Edition Remote Code Execution Vulnerability	10/07/2022
CVE-2017-1000486	Primetek Primefaces Application Remote Code Execution Vulnerability	10/07/2022
CVE-2019-7609	Elastic Kibana Remote Code Execution Vulnerability	10/07/2022
CVE-2022-22587	Apple IOMobileFrameBuffer Memory Corruption Vulnerability	11/02/2022
CVE-2021-20038	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability	11/02/2022
CVE-2014-7169	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability	28/07/2022

CVE Number	CVE Title	Remediation Due Date
CVE-2014-6271	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability	28/07/2022
CVE-2020-0787	Microsoft Windows Background Intelligent Transfer Service (BITS) Improper Privilege Management Vulnerability	28/07/2022
CVE-2014-1776	Microsoft Internet Explorer Use-After-Free Vulnerability	28/07/2022
CVE-2020-5722	Grandstream Networks UCM6200 Series SQL Injection Vulnerability	28/07/2022

جزئیات بیشتر درخصوص آسیب‌پذیری‌ها

در ادامه به بررسی مختصری از آسیب‌پذیری‌های ذکر شده می‌پردازیم.

شناسه آسیب‌پذیری	CVE-2021-22017
عنوان آسیب‌پذیری	VMware vCenter Server Improper Access Control Vulnerability
توضیحات	Rhttproxy که در سرورهای vCenter استفاده می‌شود آسیب‌پذیر است، یک مهاجم با دسترسی به پورت ٤٤٣ سرور vCenter قادر به بهره‌برداری از این آسیب‌پذیری می‌باشد و با بهره‌برداری از این آسیب‌پذیری می‌تواند پروکسی را دور زده و به یک endpoint در شبکه داخلی دسترسی پیدا کند.
محصولات آسیب‌پذیر	Vmware vcenter server 6.7
منابع	https://nvd.nist.gov/vuln/detail/CVE-2021-22017#match-6975744 https://cve.report/CVE-2021-22017

شناسه آسیب‌پذیری	CVE-2021-36260
عنوان آسیب‌پذیری	Hikvision Improper Input Validation Vulnerability
توضیحات	وب سرور برخی از محصولات Hikvision به‌دلیل عدم کنترل صحیح ورودی‌ها نسبت به حملات command injection آسیب‌پذیر است و مهاجم می‌تواند با ارسال پیام‌های حاوی فرامین مخرب به سمت وب‌سرور از این آسیب‌پذیری بهره‌برداری کند.
محصولات آسیب‌پذیر	Hikvision-Web-Server-Build-210702
منابع	https://packetstormsecurity.com/files/164603/Hikvision-Web-Server-Build 210702-Command-Injection.html https://www.cvedetails.com/cve/CVE-2021-36260/

شناسه آسیب‌پذیری	CVE-2021-27860
عنوان آسیب‌پذیری	FatPipe WARP, IPVPN, and MPVPN Privilege Escalation vulnerability
توضیحات	یک آسیب‌پذیری در رابطه مدیریتی تحت وب سامانه‌های FatPipe WARP، IPVPN و MPVPN در نسخه‌های قبل از 10.1.2r60p92 و 10.2.2r44p1 پیدا شده است که به مهاجم احراز هویت نشده از راه دور، امکان آپلود فایل به مسیر دلخواه را می‌دهد.
محصولات آسیب‌پذیر	https://nvd.nist.gov/vuln/detail/CVE-2021-27860
منابع	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27860 https://nvd.nist.gov/vuln/detail/CVE-2021-27860

شناسه آسیب‌پذیری	CVE-2020-6572
عنوان آسیب‌پذیری	Google Chrome prior to 81.0.4044.92 Use-After-Free Vulnerability
توضیحات	آسیب‌پذیری Use after free در بخش Media گوگل کروم نسخه‌های قبل از 81.0.4044.92 به مهاجم امکان اجرای کد دلخواه از راه دور را با استفاده از یک صفحه HTML مخرب می‌دهد.
محصولات آسیب‌پذیر	گوگل کروم نسخه‌های قبل از 81.0.4044.92
منابع	https://googleprojectzero.github.io/0days-in-the-wild//0day-RCAs/2020/CVE-2020-6572.html https://nvd.nist.gov/vuln/detail/CVE-2020-6572 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6572

شناسه آسیب‌پذیری	CVE-2019-1458
عنوان آسیب‌پذیری	Microsoft Win32K Elevation of Privilege Vulnerability
توضیحات	ضعف کامپوننت Win32k ویندوز برای مدیریت اشیاء در حافظه سبب به‌وجود آمدن آسیب‌پذیری ارتقا سطح دسترسی شده است. این آسیب‌پذیری به‌عنوان Win32k Elevation of Privilege Vulnerability نیز شناخته می‌شود.
محصولات آسیب‌پذیر	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-1458
منابع	https://nvd.nist.gov/vuln/detail/CVE-2019-1458 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-1458 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1458

شناسه آسیب‌پذیری	CVE-2013-3900
عنوان آسیب‌پذیری	Microsoft WinVerify Trust Function Remote Code Execution Vulnerability
توضیحات	تابع WinVerifyTrust در محصولات ذکر شده، نمی‌تواند به‌صورت صحیح فایل PE را در فرایند Authenticode signature verification بررسی کند و این ضعف به مهاجم از راه دور امکان می‌دهد که با استفاده از یک فایل PE مخرب، کد دلخواه خود را بر روی سیستم قربانی اجرا کند.
محصولات آسیب‌پذیر	Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1
منابع	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-098 https://nvd.nist.gov/vuln/detail/CVE-2013-3900 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3900

شناسه آسیب‌پذیری	CVE-2019-2725
عنوان آسیب‌پذیری	Oracle WebLogic Server, Injection Vulnerability
توضیحات	در کامپوننت Oracle WebLogic Server مربوط به Oracle Fusion Middleware در نسخه‌های 10.3.6.0.0 و 12.1.3.0.0 یک آسیب‌پذیری وجود دارد که به‌سادگی توسط یک مهاجم احراز هویت نشده که به شبکه دسترسی دارد از طریق پروتکل HTTP قابل بهره‌برداری است. بهره‌برداری موفق از این آسیب‌پذیری می‌تواند باعث تصاحب سرور Oracle WebLogic شود.
محصولات آسیب‌پذیر	Oracle WebLogic Server 10.3.6.0.0 Oracle WebLogic Server 12.1.3.0.0
منابع	https://www.oracle.com/security-alerts/alert-cve-2019-2725.html https://nvd.nist.gov/vuln/detail/cve-2019-2725 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2725

شناسه آسیب‌پذیری	CVE-2019-9670
عنوان آسیب‌پذیری	Synacor Zimbra Collaboration Suite Improper Restriction of XML External Entity Reference Vulnerability
توضیحات	کامپوننت mailboxd در Synacor Zimbra Collaboration Suite 8.7.x در نسخه‌های قبل از 8.7.11p10 دارای آسیب‌پذیری XXE یا XML External Entity injection می‌باشد.
محصولات آسیب‌پذیر	Synacor Zimbra Collaboration before 8.7.11p10
منابع	https://packetstormsecurity.com/files/152487/Zimbra-Collaboration-Autodiscover-Servlet-XXE-ProxyServlet-SSRF.html https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9670 https://www.tenable.com/cve/CVE-2019-9670

شناسه آسیب‌پذیری	CVE-2018-13382
عنوان آسیب‌پذیری	Fortinet FortiOS and FortiProxy Improper Authorization Vulnerability
توضیحات	برخی از نسخه‌های Fortinet FortiOS و FortiProxy به یک مهاجم احراز هویت نشده امکان تغییر گذرواژه یک کاربر در پورتال وب SSL VPN را با ارسال یک درخواست HTTP بخصوص می‌دهد.
محصولات آسیب‌پذیر	Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.8 and 5.4.1 to 5.4.10 And FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN web portal
منابع	https://www.fortiguard.com/psirt/FG-IR-18-389 https://nvd.nist.gov/vuln/detail/cve-2018-13382 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13382

شناسه آسیب‌پذیری	CVE-2018-13383
عنوان آسیب‌پذیری	Fortinet FortiOS and FortiProxy Improper Authorization Vulnerability
توضیحات	برخی نسخه‌های Fortinet FortiOS و FortiProxy دارای آسیب‌پذیری heap buffer overflow هستند.
محصولات آسیب‌پذیر	Fortinet FortiOS 6.0.0 through 6.0.4, 5.6.0 through 5.6.10, 5.4.0 through 5.4.12, 5.2.14 and earlier and FortiProxy 2.0.0, 1.2.8 and earlier
منابع	https://www.fortiguard.com/psirt/FG-IR-18-388 https://nvd.nist.gov/vuln/detail/CVE-2018-13383 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13383

شناسه آسیب‌پذیری	CVE-2019-1579
عنوان آسیب‌پذیری	Palo Alto Networks PAN-OS Remote Code Execution Vulnerability
توضیحات	برخی از نسخه‌های PAN-OS دارای آسیب‌پذیری اجرای کد از راه دور هستند که به مهاجم احراز هویت نشده از راه دور امکان اجرای کد دلخواه را می‌دهند.
محصولات آسیب‌پذیر	PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11-h1 and earlier, and PAN-OS 8.1.2 and earlier with GlobalProtect Portal or GlobalProtect Gateway Interface enabled
منابع	https://www.tenable.com/blog/cve-2019-1579-critical-pre-authentication-vulnerability-in-palo-alto-networks-globalprotect-ssl https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1579 https://nvd.nist.gov/vuln/detail/cve-2019-1579

شناسه آسیب‌پذیری	CVE-2019-10149
عنوان آسیب‌پذیری	Exim Mail Transfer Agent (MTA) Improper Input Validation Vulnerability
توضیحات	یک رخنه امنیتی در Exim از نسخه 4.87 تا 4.91 به‌دلیل اعتبارسنجی نادرست آدرس گیرنده (recipient address) در تابع deliver_message() در فایل src/deliver.c وجود دارد که می‌تواند منجر به اجرای کد از راه دور شود.
محصولات آسیب‌پذیر	Exim 4.87: 206,024 Exim 4.88: 24,608 Exim 4.89: 206,571 Exim 4.90: 5,480 Exim 4.91: 3,738,863 Exim 4.92: 475,591
منابع	https://www.tenable.com/blog/cve-2019-10149-critical-remote-command-execution-vulnerability-discovered-in-exim https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10149 https://nvd.nist.gov/vuln/detail/cve-2019-10149

شناسه آسیب‌پذیری	CVE-2015-7450
عنوان آسیب‌پذیری	IBM WebSphere Application Server and Server Hy Server Hypervisor Edition Remote Code Execution Vulnerability
توضیحات	رابط Serialized-object در برخی از نسخه‌های business solutions، IBM analytics، cognitive، زیرساخت‌های فناوری اطلاعات، موبایل و محصولات اجتماعی به مهاجم از راه دور امکان اجرای فرمان دلخواه با استفاده از یک serialized Java object به‌خصوص را می‌دهد، که مرتبط با کلاس InvokerTransformer در کتابخانه Apache Commons Collections می‌باشد.
محصولات آسیب‌پذیر	https://nvd.nist.gov/vuln/detail/CVE-2015-7450
منابع	https://www.rapid7.com/db/vulnerabilities/ibm-was-cve-2015-7450/ https://support.hcltechsw.com/csm/en?id=kb_article&sysparm_article=KB0013731 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7450

شناسه آسیب‌پذیری	CVE-2017-1000486
عنوان آسیب‌پذیری	Primetek Primefaces Application Remote Code Execution Vulnerability
توضیحات	Primetek Primefaces نسخه 5.x نسبت به weak encryption flaw آسیب‌پذیر است که این آسیب‌پذیری می‌تواند منجر به اجرای کد از راه دور شود.
محصولات آسیب‌پذیر	Primetek Primefaces 5.x
منابع	https://nvd.nist.gov/vuln/detail/CVE-2017-1000486 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000486

شناسه آسیب‌پذیری	CVE-2019-7609
عنوان آسیب‌پذیری	Fortinet FortiOS and FortiProxy Improper Authorization Vulnerability
توضیحات	برخی از نسخه‌های Kibana دارای آسیب‌پذیری اجرای کد دلخواه در Timelion visualizer می‌باشند. بهره‌برداری موفق از این آسیب‌پذیری می‌تواند منجر به اجرای فرمان دلخواه با سطح دسترسی پروسه Kibana شود.
محصولات آسیب‌پذیر	Kibana versions before 5.6.15 and 6.6.1
منابع	https://www.tenable.com/blog/cve-2019-7609-exploit-script-available-for-kibana-remote-code-execution-vulnerability https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7609 https://nvd.nist.gov/vuln/detail/CVE-2019-7609

شناسه آسیب‌پذیری	CVE-2022-22587
عنوان آسیب‌پذیری	Apple IOMobileFrameBuffer Memory Corruption Vulnerability
توضیحات	یک آسیب‌پذیری روز صفرم بحرانی در Apple iOS and iPadOS up to 15.2.1 پیدا شده است. این آسیب‌پذیری یک تابع شناخته نشده در کامپوننت IOMobileFrameBuffer را تحت تاثیر قرار می‌دهد و با استفاده از یک ورودی نامشخص منجر به memory corruption می‌شود.
محصولات آسیب‌پذیر	Apple iOS and iPadOS up to 15.2.1
منابع	https://sensorstechforum.com/apple-zero-days-cve-2022-22587-cve-2022-22594/ https://vuldb.com/?id.191709

شناسه آسیب‌پذیری	CVE-2021-20038
عنوان آسیب‌پذیری	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability
توضیحات	یک آسیب‌پذیری سرریز بافر مبتنی بر Stack در ماژول mod_cgi سرورهای SMA100 Apache httpd پیدا شد که به مهاجم احراز هویت نشده امکان اجرای کد با نام‌کاربری «nobody» را می‌دهد.
محصولات آسیب‌پذیر	SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions.
منابع	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20038 https://nvd.nist.gov/vuln/detail/CVE-2021-20038

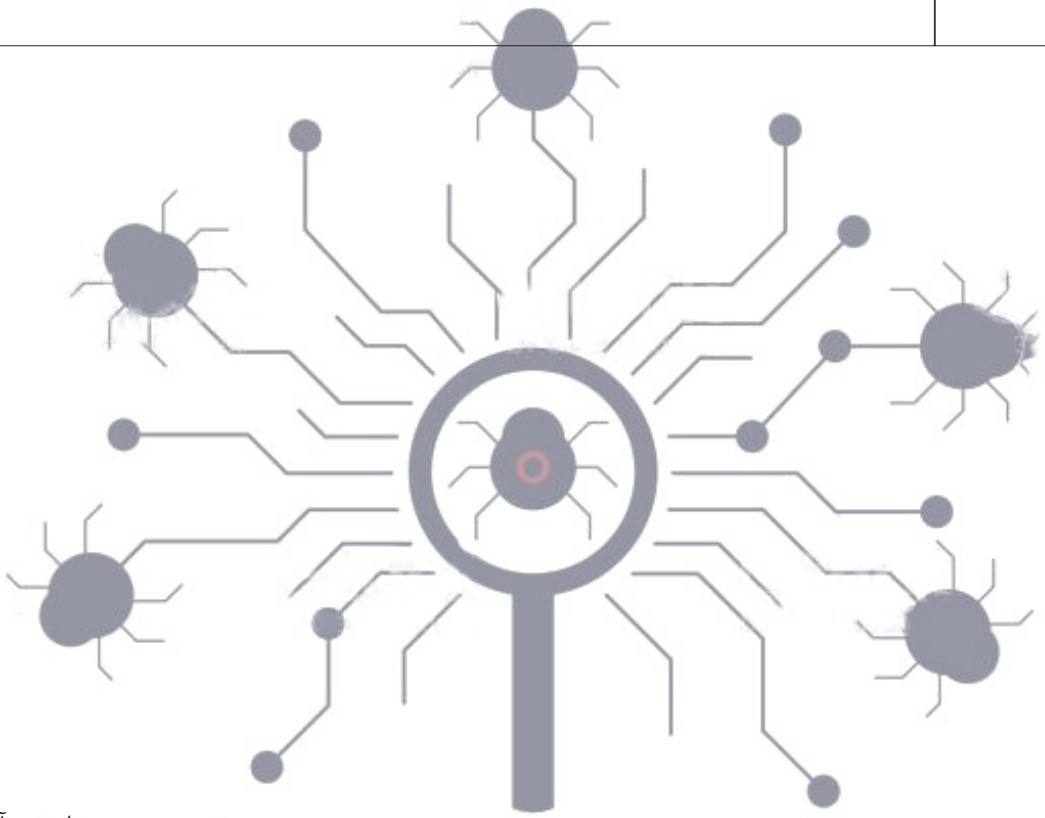
شناسه آسیب‌پذیری	CVE-2014-7169
عنوان آسیب‌پذیری	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability
توضیحات	برخی از نسخه‌های GNU Bash دارای آسیب‌پذیری اجرای کد دلخواه هستند.
محصولات آسیب‌پذیر	https://nvd.nist.gov/vuln/detail/CVE-2014-7169
منابع	https://access.redhat.com/security/cve/cve-2014-7169 https://www.cvedetails.com/cve/CVE-2014-7169/ https://nvd.nist.gov/vuln/detail/CVE-2014-7169

شناسه آسیب‌پذیری	CVE-2014-6271
عنوان آسیب‌پذیری	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability
توضیحات	برخی از نسخه‌های GNU Bash دارای آسیب‌پذیری اجرای کد دلخواه هستند.
محصولات آسیب‌پذیر	https://nvd.nist.gov/vuln/detail/cve-2014-6271
منابع	https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-6271 https://access.redhat.com/security/cve/cve-2014-6271 https://nvd.nist.gov/vuln/detail/cve-2014-6271

شناسه آسیب‌پذیری	CVE-2020-0787
عنوان آسیب‌پذیری	Microsoft Windows Background Intelligent Transfer Service (BITS) Improper Privilege Management Vulnerability
توضیحات	یک آسیب‌پذیری ارتقا سطح دسترسی در سرویس Windows Background Intelligent Transfer مربوط به ویندوز وجود دارد.
محصولات آسیب‌پذیر	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0787
منابع	https://nvd.nist.gov/vuln/detail/CVE-2020-0787 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0787 https://www.tenable.com/cve/CVE-2020-0787

شناسه آسیب‌پذیری	CVE-2014-1776
عنوان آسیب‌پذیری	Microsoft Internet Explorer Use-After-Free Vulnerability
توضیحات	آسیب‌پذیری Use-after-free در نسخه‌های ٦ تا ١١ از Internet Explorer وجود دارد، که به مهاجم از راه دور امکان اجرای کد دلخواه یا حملات منع سرویس (DoS) را می‌دهد.
محصولات آسیب‌پذیر	Microsoft Internet Explorer 6 through 11
منابع	https://nvd.nist.gov/vuln/detail/CVE-2014-1776 https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit:HTML/CVE-2014-1776&threatId=-2147280573 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776

شناسه آسیب‌پذیری	CVE-2020-5722
عنوان آسیب‌پذیری	Grandstream Networks UCM6200 Series SQL Injection Vulnerability
توضیحات	رابط کاربری HTTP مربوط به Grandstream UCM6200 series، به مهاجم احرازهویت نشده امکان انجام حملات SQL injection را می‌دهد. مهاجم با بهره برداری از این آسیب‌پذیری در نسخه‌های قبل از 1.0.19.20 امکان اجرای فرمان شل به عنوان کاربر Root را می‌دهد و در نسخه‌های قبل از 1.0.20.17 امکان تزریق یک صفحه HTML در password recovery emails را می‌دهد.
محصولات آسیب‌پذیر	HTTP interface of the Grandstream UCM6200
منابع	https://nvd.nist.gov/vuln/detail/CVE-2020-5722 https://www.tenable.com/cve/CVE-2020-5722 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5722



ژینو سفاحی
zhino.safahi@uok.ac.ir

حملات باج‌افزاری و راهکارهای جلوگیری و محافظت در مقابل آن‌ها

مقدمه

در چند سال اخیر با مراجعه به اخبار فناوری اطلاعات و حوزه امنیت سایبری تیترهایی همچون حملات باج‌افزاری و چالش‌های اصلی سازمان‌ها و کاربران درخصوص باج‌افزار همواره مطرح بوده‌اند و به یکی از مخاطرات جدی در این بستر تبدیل شده‌اند. در اصل برای تیم‌های فناوری اطلاعات و امنیت سایبری شرکت‌ها و سازمان‌ها، باج‌افزار به‌عنوان یکی از نگران‌کننده‌ترین چالش‌ها در سال‌های اخیر به شمار می‌رود. حملات باج‌افزاری در سرتاسر سال ۲۰۲۱ نیز سرفصل خبرها بود و طبق گزارش SonicWall این حملات و خسارت‌های ناشی از آن‌ها نسبت به سال ۲۰۲۰ دو برابر و نسبت به سال ۲۰۱۹ به بیش از سه برابر رسیده‌اند و پیش‌بینی‌ها درخصوص سال ۲۰۲۲ نیز این است که همچنان باج‌افزار جزء تهدیدات و چالش‌های اصلی کاربران و سازمان‌ها خواهد بود. طبق گزارش‌ها در پایان سال ۲۰۱۶، هر ۴۰ ثانیه یک کسب‌وکار قربانی حمله باج‌افزاری می‌شد و پیش‌بینی می‌شود که باج‌افزارها در سال ۲۰۲۲ بیش از ۲۰ میلیارد دلار خسارت به بار آورند و در هر ۱۴ ثانیه یک کسب‌وکار قربانی حمله باج‌افزاری شود. دیگر باید به این نکته توجه کرد که باج‌افزار تهدیدی جدی و قابل توجه برای کاربران، سازمان‌ها و شرکت‌های خصوصی است و باتوجه به سطح تهدیدی که ایجاد می‌کند، میبایستی آمادگی و روش‌های جلوگیری و حفاظتی در مقابل این حملات به شکلی جدی پیگیری و اجرا شود. البته باید دقت داشت که حتی با بهترین اقدامات احتیاطی امنیتی، هرگز نمی‌توان با قطعیت کامل احتمال آلودگی به باج‌افزار را رد کرد!

در ادامه این مطلب در مورد انواع مختلف باج‌افزار، چگونگی آلودگی و شناسایی آن‌ها، اینکه چه کسانی را هدف قرار می‌دهند، درصورت آلوده شدن به آن‌ها چه اقداماتی باید انجام شود و در نهایت، چه کاری می‌توان برای محافظت در برابر آن‌ها انجام داد، توضیحاتی ارائه خواهد شد. البته در شماره دهم همین فصل‌نامه مربوط به تابستان ۱۴۰۰ در مطلبی با عنوان «محافظت از فایل‌ها در برابر حملات باج‌افزاری» درخصوص باج‌افزار مطالبی بیان شد که مراجعه به آن می‌تواند مفید باشد.

باج‌افزار چیست؟

باج‌افزار (Ransomware) نوعی بدافزار یا برنامه مخرب محسوب می‌شود که مجرمان سایبری از آن برای قفل یا رمزگذاری فایل‌های سیستم کاربران استفاده کرده و پس از آلوده کردن سیستم، دسترسی کاربران به فایل‌ها را با چالش مواجه می‌کنند، سپس در ازای رمزگشایی، از کاربر باج می‌خواهند. همچنین با تهدید به انتشار عمومی داده‌ها و فایل‌های استخراج شده و یا مسدود کردن دائمی دسترسی به آن در صورت امتناع قربانی از پرداخت باج، فشار بیشتری بر قربانی وارد می‌کنند. تقاضاهای باج از سوی مجرمان سایبری اکنون با استفاده از رمز ارزهایی مانند بیت‌کوین انجام می‌شود به این دلیل که اساساً ردیابی پرداخت از طریق بیت‌کوین بسیار دشوار است.

شناسایی و محافظت در برابر باج‌افزار

وقتی صحبت از محافظت در برابر باج‌افزارها می‌شود، اصطلاحاً پیشگیری بهتر از درمان است، گرچه در اکثر موارد اساساً درمانی در کار نیست! برای رسیدن به این هدف، آموزش صحیح در این خصوص و استفاده از نرم‌افزارهای امنیتی مناسب بسیار مهم است. همچنین پویش مداوم آسیب‌پذیری‌های نرم‌افزارها، سیستم‌عامل‌ها و تجهیزات شبکه و انجام به‌روزرسانی و اعمال وصله‌ها به موقع می‌تواند تا حد زیادی از آلوده شدن سیستم و سازمان شما جلوگیری کند. البته همان‌طور که ذکر شد آموزش نیز دارای اهمیت است و توجه به نکاتی مانند استفاده از منابع دانلود شناخته شده، عدم دانلود پیوست هرزنامه‌ها، عدم کلیک بر روی لینک‌های موجود در ایمیل‌های مشکوک، احتیاط در خصوص اتصال فلش دیسک‌های ناشناخته به سیستم و دقت در انتخاب رمزهای عبور برای حساب‌های کاربری متعدد خود در بسترهای مختلف، اقدامات محافظتی معقول در برابر باج‌افزار است.

چند راهکار برای تشخیص باج‌افزار

- یک انتی‌ویروس به‌روزرسانی شده و قدرتمند که مجهز به ضدبدافزار است، هنگام مشاهده باج‌افزار پیام هشدار را صادر می‌کند، مگر اینکه باج‌افزار نوعی جدید و پیشرفته باشد و راهکارهای امنیتی ما را دور بزند.
- یکی دیگر از راهکارهای تشخیص آلودگی سیستم به باج‌افزار بررسی پسوند فایل‌ها است. به‌عنوان مثال، پسوند معمول یک کتاب الکترونیکی «pdf» است. اگر این پسوند به ترکیبی از حروف ناآشنا تغییر کند، ممکن است یک آلودگی باج‌افزار بوجود آمده باشد. همچنین باج‌افزار در مواردی هنگام رمزگذاری داده‌ها، نام فایل را تغییر می‌دهد. بنابراین این مورد نیز می‌تواند یک سرنخ باشد.
- افزایش غیرمعمول فعالیت CPU و دیسک یا اصطلاحاً CPU and Disk usage می‌تواند نشان‌دهنده اجرای فرآیندی مخرب مانند باج‌افزار در پس‌زمینه سیستم‌عامل باشد.
- ارتباطات شبکه مشکوک نیز سرنخی مهم است. باج‌افزار در تعامل با مجرم سایبری یا با سرور مهاجم ممکن است ارتباطات مشکوکی در شبکه ایجاد کند.

- درصورت آلودگی سیستم، در اغلب موارد فایل‌ها رمزگذاری می‌شوند و نشانه دیرهنگام برای شناسایی باج‌افزار این است که فایل‌ها باز نمی‌شوند و حمله باج‌افزاری موفق بوده است.

پس از آلودگی به باج‌افزار، پیام یا پنجره‌ای حاوی درخواست باج تایید می‌کند که آلودگی باج‌افزار وجود دارد. هرچه تهدید زودتر شناسایی شود، مبارزه با آن آسان‌تر است. تشخیص زودهنگام آلودگی می‌تواند به تعیین نوع باج‌افزاری که سیستم را آلوده کرده است کمک کند. برخی از باج‌افزارها پس از اجرای رمزگذاری، خود را حذف می‌کنند تا قابل بررسی و رمزگشایی نباشند.

انواع باج‌افزارها

همان‌طور که در مقدمه ذکر شد، تهدید ناشی از باج‌افزار منجر به رمزگذاری یا قفل‌شدن سیستم می‌شوند، پس دو دسته اصلی باج‌افزارها به‌صورت زیر هستند:

باج‌افزار قفل‌کننده (Locker ransomware)

در باج‌افزار قفل‌کننده عملکردهای اساسی کامپیوتر تحت تأثیر قرار می‌گیرند به نحوی کل صفحه را قفل می‌کند درحالی‌که موس و صفحه‌کلید تاحدی غیرفعال هستند. این به شما امکان می‌دهد به تعامل با پنجره حاوی درخواست باج ادامه دهید تا پرداخت را انجام دهید اما این نوع معمولاً فایل‌های مهم را هدف قرار نمی‌دهد. به‌طور کلی فقط عملکردهای اساسی سیستم را مسدود می‌کند، بنابراین احتمال ازبین رفتن کامل داده‌های قربانی بعید است. باج‌افزار CryptoLocker از این نوع بوده است. نمونه‌های باج‌افزار این دسته تعداد کمی از باج‌افزارها را شامل می‌شوند.

باج‌افزار رمزنگار (Crypto ransomware)

هدف باج‌افزار رمزنگار، رمزگذاری داده‌های مهم افراد، مانند اسناد، عکس‌ها و ویدیوها است، اما در کارکردهای اولیه سیستم دخالت نمی‌کند. این باعث آشفتگی کاربران می‌شود زیرا می‌توانند فایل‌های خود را ببینند اما نمی‌توانند به آن‌ها دسترسی پیدا کنند. توسعه‌دهندگان این نوع باج‌افزار اغلب یک شمارش معکوس برای باج درخواستی خود اضافه می‌کنند: «اگر تا پایان مهلت باج را پرداخت نکنید، همه فایل‌های شما حذف خواهند شد.» و با توجه به تعداد کاربرانی که از نیاز به پشتیبان‌گیری در فضای ابری یا دستگاه‌های ذخیره‌سازی فیزیکی خارجی بی‌اطلاع هستند، باج‌افزار رمزنگار می‌تواند تأثیر مخربی داشته باشد. در نتیجه، بسیاری از قربانیان صرفاً برای بازگرداندن فایل‌های خود باج می‌پردازند. باج‌افزار WannaCry از این نوع بوده است. اکثر نمونه‌های باج‌افزار از این نوع هستند.

نوع باج‌افزار در شناسایی و مقابله با آن نیز تفاوت چشم‌گیری ایجاد می‌کند. می‌توان بین انبوهی از انواع دیگر باج‌افزارها با این دو دسته اصلی تمایز قائل شد.

صرف‌نظر از نوع باج‌افزار، قربانیان معمولاً سه گزینه دارند:

- آن‌ها می‌توانند باج را بپردازند و امیدوار باشند که مجرمان سایبری به قول خود عمل کنند و کلید رمزگشایی فایل‌ها را برایشان ارسال کنند. طبق آمار فقط در حدود ۲۵ درصد قربانیانی که باج را پرداخت کرده‌اند کلید رمزگشایی برایشان ارسال شده است!

- قربانی می‌تواند با استفاده از ابزارهای موجود، فرآیند اجرایی باج‌افزار را حذف کند و از منابع مختلفی که در انتهای این مطلب به آن‌ها اشاره می‌شود برای رمزگشایی فایل‌های رمزنگاری‌شده بهره گیرد.

- در مواردی نیز، چون قربانی از فایل‌های خود نسخه پشتیبان دارد، بدون توجه به از دست رفتن فایل‌ها در سیستم آلوده، عملیات حذف فرآیند اجرایی باج‌افزار و پاک‌سازی را انجام داده و حتی با نصب سیستم‌عامل جدید و بازگردانی فایل‌ها از نسخه پشتیبان، نگرانی از آلودگی باج‌افزار رفع شود.

نکته قابل توجه این است که حتما پس از اقدامات ذکر شده، باید منشاء آلودگی به باج‌افزار شناسایی شده و به منظور عدم تکرار این رخداد، این نقص را برطرف کرد.

اقدامات پس از آلودگی به باج‌افزار

اگر مشکوک هستید که مورد حمله باج‌افزار قرار گرفته‌اید، بسیار مهم است که سریع عمل کنید. خوشبختانه چند مرحله وجود دارد که می‌توان پیگیری کرد تا حداکثر شانس ممکن را برای به حداقل رساندن آسیب و بازگشت سریع به کار معمول و احیاناً بازگردانی فایل‌های خود داشته باشید.

مرحله ۱

اتصال به اینترنت را قطع کنید.

ابتدا تمام اتصالات شبکه را قطع کنید. این موارد شامل دستگاه‌های بی‌سیم و سیمی، هارد دیسک‌های خارجی، هر بستر ذخیره‌سازی و حساب‌های ابری است. این می‌تواند از گسترش باج‌افزار در داخل شبکه جلوگیری کند.

مرحله ۲

با نرم‌افزار امنیتی و ضدباج‌افزار پویش انجام دهید.

با استفاده از نرم‌افزارهای امنیتی و ضدباج‌افزار که نصب کرده‌اید، پویش را انجام دهید. این به شما کمک می‌کند تا تهدیدات را شناسایی کنید. اگر برنامه‌های مخرب و خطرناکی شناسایی شدند، می‌توانید آن‌ها را حذف یا ایزوله کنید.

مرحله ۳

از یک ابزار رمزگشایی باج‌افزار استفاده کنید.

اگر سیستم شما به باج‌افزار آلوده شده است که داده‌های شما را رمزگذاری کرده است، برای دسترسی مجدد به فایل‌ها، به ابزار رمزگشای مناسب نیاز دارید. در انتهای این مطلب چند منبع برای دریافت رمزگشا را معرفی خواهیم‌کرد.

نکته حائز اهمیت این است که در اکثر موارد آلودگی به باج‌افزار، رمزگشا برای انجام بازگردانی فایل‌ها موجود نیست و در اصل فایل‌های رمزنگاری شده تا زمان تولید رمزگشا برای آن باج‌افزار خاص، قابل بازگردانی نخواهند بود.

مرحله ٤

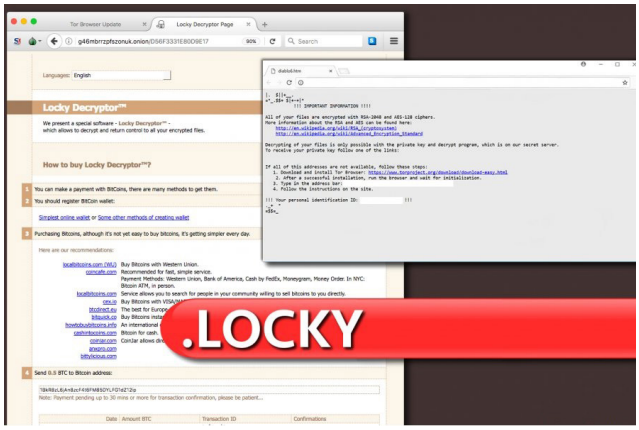
از نسخه‌های پشتیبان، فایل‌های خود را بازیابی کنید.

اگر از اطلاعات خود به‌صورت خارجی یا در فضای ذخیره‌سازی ابری نسخه پشتیبان تهیه کرده‌اید، از این نسخه، فایل‌های خود را بازگردانی کنید. اگر هیچ نسخه پشتیبان ندارید، پاک‌سازی و بازیابی سیستم شما بسیار دشوارتر است. برای جلوگیری از این وضعیت، توصیه می‌شود که به‌طور منظم از فایل‌های خود نسخه پشتیبان تهیه کنید. اگر چنین مواردی را فراموش می‌کنید، از خدمات پشتیبان‌گیری خودکار ابری استفاده کنید یا هشدارهایی را در تقویم خود تنظیم کنید تا این مورد را به شما یادآوری کنند.

چند نمونه باج‌افزار شناخته‌شده که به شما در شناسایی خطرات ناشی از باج‌افزار کمک می‌کنند عبارت‌اند از:

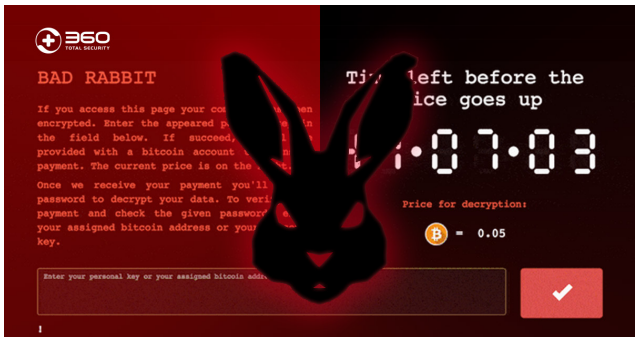
Locky

باج‌افزاری است که برای اولین بار در سال ۲۰۱٦ توسط گروهی از هکرهای سازمان یافته برای حمله مورد استفاده قرار گرفت. Locky بیش از ۱٦۰ نوع فایل را رمزگذاری کرد و از طریق ایمیل‌های جعلی با پیوست‌های آلوده منتشر شد و کاربران از طریق ایمیل گرفتار شدند و باج‌افزار را روی رایانه خود نصب کردند. این روش گسترش باج‌افزار، فیشینگ که نوعی مهندسی اجتماعی است، نامیده می‌شود. باج‌افزار Locky انواع فایل‌هایی را هدف قرار می‌دهد که اغلب توسط طراحان، توسعه‌دهندگان، مهندسان و آزمایش‌کنندگان استفاده می‌شوند.



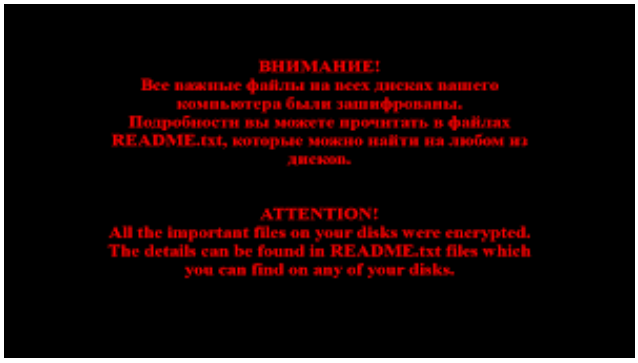
WannaCry

این باج‌افزار در بیش‌از ۱۵۰ کشور گسترش یافت. WannaCry در حدود ۲۳۰۰۰۰ کامپیوتر را در سراسر جهان تحت‌تأثیر قرار داد. این حمله یک سوم بیمارستان‌های NHS در بریتانیا را تحت‌تأثیر قرار داد و خسارتی زیادی به بار آورد.



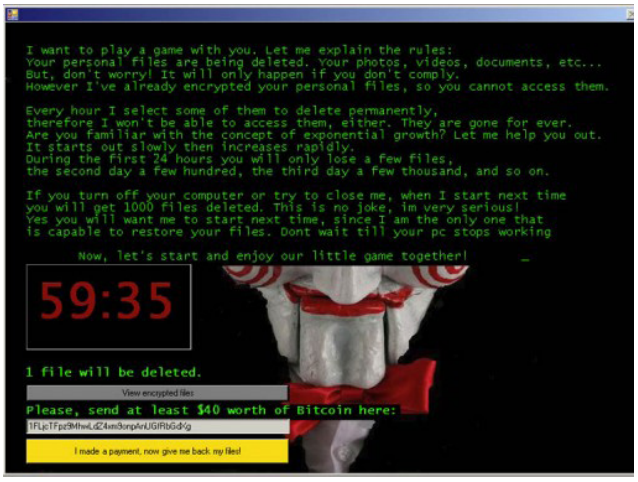
Bad Rabbit

یک نوع حمله باج‌افزاری از سال ۲۰۱۷ بود که از طریق حملات به اصطلاح Drive-by گسترش یافت. برای انجام این حملات از وب‌سایت‌های ناامن استفاده شد. در این حمله کاربر از یک وب‌سایت واقعی بازدید می‌کند، غافل از اینکه توسط هکرها به خطر افتاده است. قربانی با اجرای برنامه‌ی نصب‌کننده‌ای که بدافزار در آن پنهان شده و خواستار اجرای فرایند نصب جعلی Adobe Flash بود و در نتیجه کامپیوتر را با باج‌افزار آلوده کند.



Shade or Troldesh

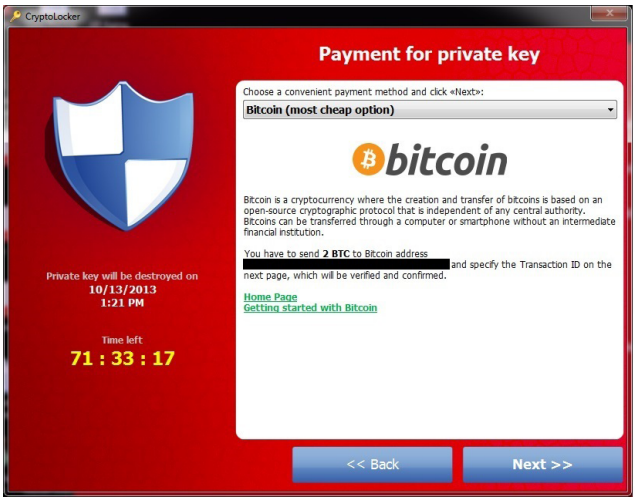
این نوع حمله باج‌افزار در سال ۲۰۱۵ رخ داد و از طریق ایمیل‌های اسپم حاوی لینک‌های آلوده یا پیوست‌های فایل منتشر شد. جالب اینجاست که مهاجمان Troldesh مستقیماً از طریق ایمیل با قربانیان خود در ارتباط بودند. قربانیانی که با آن‌ها «رابطه خوب» برقرار کرده بودند تخفیف دریافت می‌کردند. با این حال، این نوع رفتار یک استثنا است تا یک قاعده.



Jigsaw

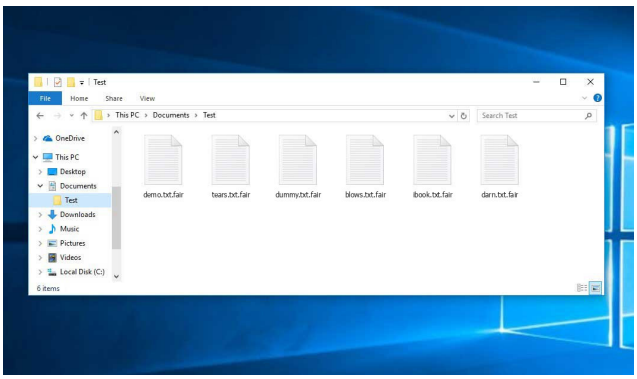
یک حمله باج‌افزاری است که در سال ۲۰۱۶ آغاز شد. نام این حمله از تصویری که از عروسک معروف مجموعه فیلم Saw نشان می‌داد، گرفته شد. با هر ساعت اضافی که باج پرداخت نمی‌شد، باج‌افزار Jigsaw فایل‌های بیشتری را حذف می‌کرد. استفاده از تصویر فیلم ترسناک باعث استرس مضاعفی در بین کاربران شد.

CryptoLocker



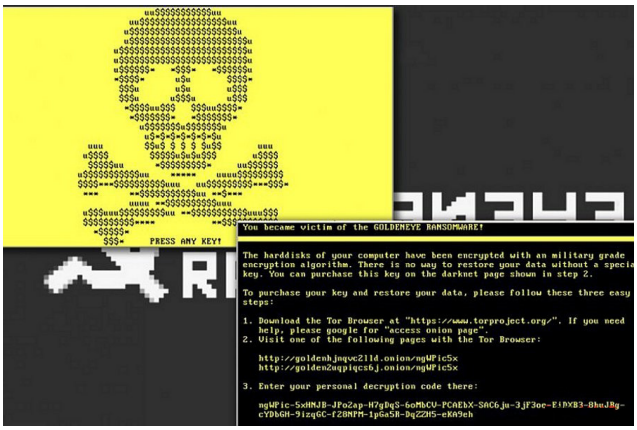
یک باج‌افزار است که برای اولین بار در سال ۲۰۰۷ مشاهده شد و از طریق پیوست‌های ایمیل آلوده منتشر شد. این باج‌افزار داده‌های مهم در رایانه‌های آلوده را جستجو و رمزگذاری کرد. تخمین زده می‌شود که ۵۰۰۰۰۰ کامپیوتر تحت‌تأثیر این باج‌افزار قرار گرفتند. سازمان‌های مجری قانون و شرکت‌های امنیتی در نهایت موفق شدند کنترل انتشار CryptoLocker را در دست بگیرند. این منجر به راه‌اندازی یک پورتال آنلاین شد که قربانیان می‌توانند کلیدی برای بازکردن قفل داده‌های خود به‌دست آورند و اطلاعات آن‌ها بدون نیاز به پرداخت باج به مجرمان قابل دستیابی شود.

FAIR



باج‌افزاری است که هدف آن رمزگذاری داده‌ها است. با استفاده از یک الگوریتم قدرتمند، تمام اسناد و فایل‌های خصوصی قربانی رمزگذاری می‌شوند. فایل‌هایی که با این بدافزار رمزگذاری شده‌اند پسوند فایل «FAIR RANSOMWARE» به آن‌ها اضافه شده است.

GoldenEye

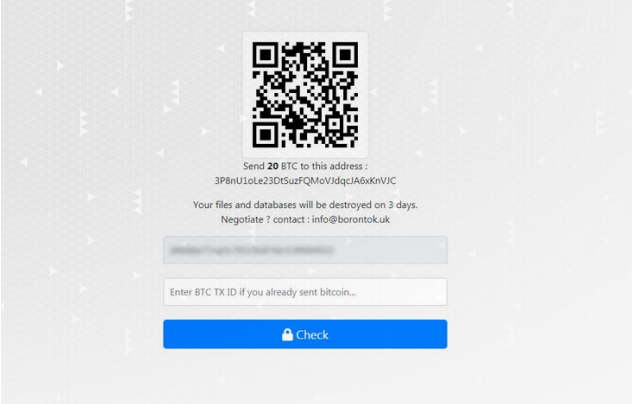


احیای Petya به‌عنوان GoldenEye منجربه یک آلودگی باج‌افزار جهانی در سال ۲۰۱۷ شد. GoldenEye که به‌عنوان «خواهر و برادر مرگبار WannaCry» شناخته می‌شود، به بیش از ۲۰۰۰ هدف « از جمله تولیدکنندگان برجسته نفت در روسیه و چندین بانک» حمله کرد.

GandCrab

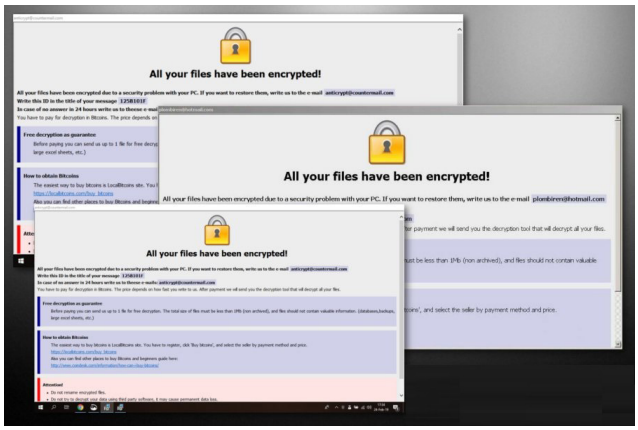
باج‌افزار ناخوشایندی است که عادات بد قربانیان خود را تهدید می‌کند. این سازمان ادعای هک وب‌کم قربانی را داشت و از آن تقاضای باج می‌کرد و درصورت عدم پرداخت تصاویر شخصی قربانی را به اشتراک می‌گذاشت. باج‌افزار GandCrab پس از اولین حضور خود در سال ۲۰۱۸ به توسعه در نسخه‌های مختلف ادامه داد. به‌عنوان بخشی از طرح «nomoreransom»، ارائه دهندگان امنیتی یک ابزار رمزگشایی باج‌افزار برای کمک به قربانیان برای بازیابی اطلاعات حساس خود از GandCrab ایجاد کردند.

B0r0nt0k



یک باج‌افزار رمزنگاری است که به‌طور خاص بر روی سرورهای مبتنی‌بر ویندوز و لینوکس تمرکز دارد. این باج‌افزار، فایل‌های سرور لینوکس را رمزگذاری و پسوند آن‌ها را به «rontok» تغییر می‌دهد. این بدافزار نه تنها فایل‌ها را تهدید، بلکه با ایجاد تغییراتی در تنظیمات startup، عملکردها و برنامه‌ها را غیرفعال می‌کند و ورودی‌های رجیستری، فایل‌ها و برنامه‌ها را نیز اضافه می‌کند.

Dharma

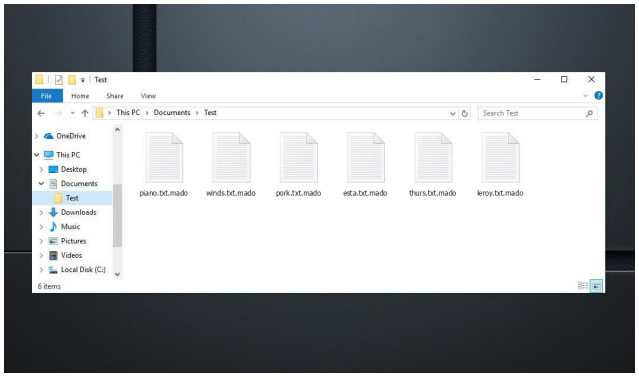


باج‌افزار جدید Dharma، به‌صورت دستی توسط هکرها نصب می‌شود و سپس سرویس‌های دسکتاپ متصل به اینترنت را هک می‌کند. به‌محض اینکه باج‌افزار توسط هکر فعال شود، شروع به رمزگذاری فایل‌هایی که پیدا شده می‌کند. به داده‌های رمزگذاری شده پسوند فایل «id-[id].[email].brrr» داده می‌شود.

Petya

یک حمله باج‌افزاری است که در سال ۲۰۱۶ رخ داد و در سال ۲۰۱۷ به عنوان GoldenEye احیا شد. این باج‌افزار مخرب به‌جای رمزگذاری فایل‌های خاص، کل هارد دیسک قربانی را با Master File Table (MFT) رمزگذاری و دسترسی به فایل‌های روی هارد دیسک را غیرممکن می‌کرد. باج‌افزار Petya از طریق یک برنامه جعلی که حاوی پیوند Dropbox آلوده بود، به بخش‌های منابع انسانی شرکت‌ها گسترش یافت.

MADO



نوع دیگری از باج‌افزار رمزنگاری است. داده‌هایی که توسط این باج‌افزار رمزگذاری شده‌اند پسوند «mado» داده می‌شود و بنابراین دیگر نمی‌توان آن‌ها را باز کرد.

ضدباج‌افزارها چه مزایایی دارند؟

علاوه‌بر این اقدامات پیشگیری از آلودگی، استفاده از نرم‌افزار مناسب برای محافظت در برابر باج‌افزار نیز ضروری است. به‌عنوان مثال، استفاده از انتی‌ویروس‌ها و فیلترهای محتوا در سرورهای ایمیل شما یک راهکار هوشمند برای جلوگیری از باج‌افزار است. این برنامه‌ها خطر ارسال هرزنامه را با پیوست‌های مخرب یا پیوندهای آلوده به صندوق پستی شما را کاهش می‌دهند. به‌طور کلی ضد باج‌افزار یک راه حل حفاظت از باج‌افزار است و از سازمان‌ها در برابر پیچیده‌ترین حملات باج‌افزار محافظت می‌کند. اگر به‌طور دقیق‌تر به برخی از انتی‌ویروس‌های مهم و قدرتمند دقت کنیم درمیابیم که در زیرمجموعه این انتی‌ویروس‌ها نوعی ضدباج‌افزار نیز قرار دارد. البته ضدباج‌افزارهایی به‌صورت مستقل نیز توسعه داده شده‌اند. به‌عنوان مثال چند مورد از ضدباج‌افزارها عبارت‌اند از:

Bitdefender

چندین لایه محافظت در برابر باج‌افزار، تجزیه‌وتحلیل و رهگیری برنامه‌های مخرب در هنگام دسترسی و در حین اجرا را فراهم می‌کند. از رمزگذاری داده‌های شخصی یا حساس توسط بدافزارها جلوگیری کرده و سازمان‌ها را ایمن نگه می‌دارد. این راه‌حل همچنین با ایجاد خودکار یک نسخه پشتیبان از فایل‌های هدف که پس از مسدود شدن بدافزار بازیابی می‌شوند، به‌طور فعال از کاربر محافظت می‌کند.

Kaspersky

ابزار جدید و بهبود یافته ضدباج‌افزار Kaspersky که رایگان است. این ابزار از Cloud برای تشخیص رفتار، اسکن و مسدودکردن فوری باج‌افزارها و بدافزارهای رمزنگاری شده استفاده می‌کند. این نسخه برای کاربران خانگی و مشاغل قابل استفاده است. آخرین نسخه Kaspersky Security Cloud Free شامل ابزاری به نام System Watcher است که حملات باج‌افزاری را رصد می‌کند.

Avast

باج‌افزارهای جدید و بهبودیافته هر روز به اینترنت هجوم می‌آورد اما Avast انتی‌ویروس خود را به صورت مداوم ارتقا می‌دهد تا کاربران را درمقابل این جریان ایمن‌تر نگه دارد. ابزار رایگان ضد باج‌افزار Avast برای iOS و Android موجود است و باج‌افزارهای خطرناک و انواع دیگر تهدیدات را قبل از اینکه به فایل‌های شما آسیب برسانند، متوقف می‌کند.

Check Point

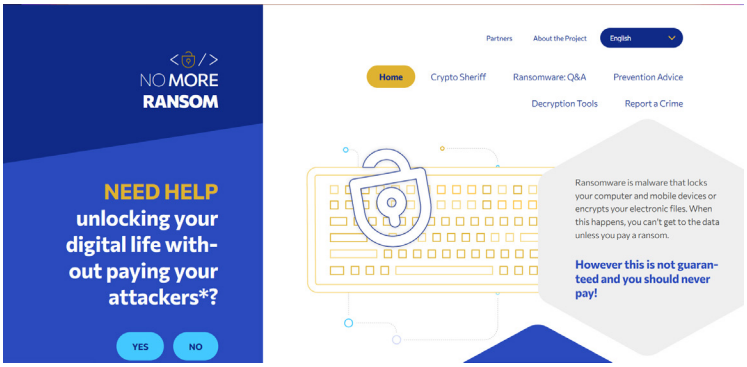
باج‌افزار بدون هشدار از طریق وب، ایمیل، یا دستگاه‌های رسانه‌ای قابل جابجایی به سازمان شما نفوذ می‌کند. ضدباج‌افزار Check Point از سازمان‌ها در برابر پیچیده‌ترین حملات باج‌افزار محافظت می‌کند و تداوم و بهره‌وری کسب‌وکار را تضمین می‌کند. Anti-Ransomware به‌عنوان بخشی از Harmony Endpoint–Check Point یک راه‌حل کامل امنیتی نقطه‌پایانی ارائه شده‌است. Harmony Endpoint حفاظت جامعی از نقطه‌پایانی را در بالاترین سطح امنیتی فراهم می‌کند که برای جلوگیری از نقض امنیت و به خطر افتادن داده‌ها ضروری است.

Cisco Ransomware Defense

Cisco Ransomware Defense معماری امنیتی سیسکو است، با استفاده از دفاع‌هایی در سطح شبکه، DNS، ایمیل و نقطه‌پایانی را شامل می‌شوند. این معماری توسط تحقیقات پیشرو در صنعت Talos برای پاسخگویی نهایی در برابر باج‌افزار پشتیبانی می‌شود. Cisco Umbrella از دستگاه‌ها در داخل و خارج از شبکه شرکت محافظت می‌کند. قبل از اینکه دستگاه بتواند به سایت‌های مخرب میزبان باج‌افزار متصل شود، درخواست‌های DNS را مسدود می‌کند. محافظت از بدافزار پیشرفته AMP Cisco برای نقاط‌پایانی مانع از باز شدن فایل‌های باج‌افزار در نقاط‌پایانی می‌شود. Cisco ISE از طریق شبکه Cisco برای تقسیم‌بندی پویا شبکه شما، بنابراین دسترسی به سرویس‌ها و برنامه‌ها بسیار امن می‌ماند و باج‌افزار نمی‌تواند به‌صورت جانبی پخش شود.

پس از بررسی ضدباج‌افزارها و ارائه راهکارهایی برای جلوگیری از آلودگی به باج‌افزار، حال بررسی می‌کنیم که اگر سیستم دچار آلودگی باج‌افزار شد و فایل‌ها رمزنگاری شدند برای رمزشگایی فایل‌ها چه فعالیتی باید صورت گیرد. استفاده از برخی از رمزگشاها آسان است اما برخی نیاز به دانش فنی دارند. به‌همان اندازه که ما می‌خواهیم این فرآیند آسان‌تر باشد، همیشه این اتفاق نمی‌افتد. در ادامه چند مورد رایج از مراجع و پایگاه‌داده‌هایی که رمزگشاهای باج‌افزار را منتشر کرده‌اند را بررسی خواهیم کرد.

- No More Ransom با آدرس nomoreransom.org
- Kaspersky با آدرس noransom.kaspersky.com
- Emsisoft با آدرس emsisoft.com/ransomware-decryption-tools
- و غیره



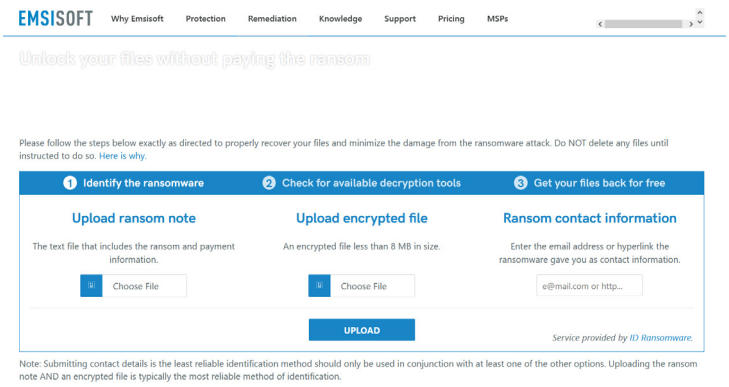
No More Ransom

وب‌سایتی است که توسط مرکز جرایم سایبری اروپا یوروپل، واحد ملی جرایم فناوری پیشرفته پلیس هلند و McAfee طراحی‌شده و به قربانیان باج‌افزار کمک می‌کند تا داده‌های رمزگذاری شده خود را بدون پرداخت هزینه به مجرمان بازیابی کنند. یکی از اهداف این است که قربانیان دیگر نباید مجبور به پرداخت باج یا از دست رفتن فایل‌هایشان شوند. با بازگرداندن رایگان دسترسی به فایل‌های آلوده آن‌ها، گزینه سومی را در اختیار کاربران قرار می‌دهند.

Kaspersky

قادراست برنامه‌های آلوده را هنگام دانلود یا تکثیر در شبکه مسدود کند و در نتیجه محافظت بلادرنگ را ارائه دهد. این کار از آلوده‌شدن سیستم شما جلوگیری می‌کند با انجام اسکن به شناسایی و مسدودکردن باج‌افزار کمک می‌کند و از داده‌های شما در برابر حملات باج‌افزاری محلی و دسترسی از راه دور محافظت می‌کند. همچنین این شرکت پایگاهی را برای انتشار رمزگشاهای مربوط به باج‌افزارها در نظر گرفته است که اگر در زمانی برای یک باج‌افزار خاص رمزگشایی توسعه یابد و تست‌های لازم این شرکت را با موفقیت پشت سر بگذارد در این پایگاه به صورت عمومی منتشر شده و کاربران به‌راحتی می‌توانند به آن دسترسی داشته باشند.

Emsisoft



یکی دیگر از پایگاهایی که منبع قرارگیری رمزگشاهای مربوط به باج‌افزارها هستند سایت Emsisoft است. برخی از باج‌افزارهای رمزنگار، دارای رمزگشا هستند و در صورت آلودگی سیستم با این دسته از باج‌افزارها، قربانی می‌تواند با مراجعه به این سایت از طریق مراحلی که توضیح داده خواهد شد برنامه رمزگشا را دانلود کرده و فرایند رمزگشایی فایل‌های آلوده خود را انجام دهد. در این سایت مراحل زیر را دقیقاً مطابق دستورالعمل دنبال کنید تا بتوانید فایل‌های خود را به‌درستی بازیابی کنید و آسیب ناشی از حمله باج‌افزار را به حداقل برسانید.

همان‌طور که در عکس بالا مشخص است، روش‌های مختلفی برای شناسایی نوع باج‌افزاری که سیستم شما را آلوده کرده است وجود دارد. در بخش اول می‌توان فایل متنی که باج‌افزار بر روی صفحه نمایش شما نشان می‌دهد را آپلود کنید، در بخش دوم می‌توان یک فایل رمزگذاری شده را با حجم کمتر از ۸ مگابایت آپلود کنید و در بخش سوم آدرس ایمیل یا لینکی را که باج‌افزار به‌عنوان اطلاعات تماس به شما داده است را وارد کنید. پس از آپلود هر یک از موارد قید شده، این سایت در بانک اطلاعاتی خود جستجو می‌کند که آیا برای این نمونه باج‌افزار، رمزگشایی در بانک اطلاعاتی خود می‌یابد یا خیر. اگر در آن زمان هنوز رمزگشایی برای این نمونه باج‌افزار موجود نباشد پیامی حاوی این مطلب به کاربر نشان داده خواهد شد. باید توجه داشت که ممکن است در آینده‌ای نزدیک یا دور برای این نمونه باج‌افزار، رمزگشا توسعه یابد پس می‌توان فایل‌های آلوده حساس و مهم را حذف نکرد و در حافظه‌ای جداگانه نگهداری کرد که شاید در آینده با توسعه رمزگشا بتوان فایل‌ها را بازگردانی کرد اما این امر قطعی نیست!

در حالتی دیگر اگر اطلاعات آپلود شده توسط کاربر حاکی از آن باشد که برای باج‌افزار، رمزگشا موجود باشد برنامه رمزگشا بایستی توسط کاربر دانلود شود و طبق دستورالعمل‌های داده شده عملیات رمزگشایی و بازگردانی فایل‌ها انجام شود. در زیر یک رمزگشا برای باج‌افزار خانواده STOP را مشاهده می‌کنید که از طریق این سایت قابل دانلود است.

هادی گلباغی
h.golbaghi@uok.ac.ir

دفترچه تقلب

دفترچه تقلب فریمورک Volatility

Volatility - An advanced Open Source Memory Forensics Framework

مقدمه

فریمورک Volatility یک مجموعه ابزار متن باز GPLv2 تحت لایسنس GNU توسعه‌داده شده با زبان پایتون است. این ابزار به‌منظور جرم‌شناسی و تحلیل حافظه، استخراج اطلاعات و مستندات دیجیتال از حافظه موقت یا RAM مورد استفاده است. همچنین از این ابزار برای تحلیل بدافزار و مهندسی معکوس نیز استفاده می‌کنند. اولین نسخه این ابزار در سال ۲۰۰۷ به‌صورت عمومی در Black Hat DC منتشر شد که حاصل سال‌ها تحقیق آکادمیک و عملی درخصوص تحلیل پیشرفته حافظه و جرم‌شناسی بوده است. روش‌ها و تکنیک‌های مورد استفاده در این ابزار به‌طور کاملاً مستقل از سیستم مورد بررسی انجام می‌شوند اما در زمان اجرای آن در سیستم قابل مشاهده هستند. این ابزار سیستم‌عامل‌های ویندوز، لینوکس، مک و اندروید را پشتیبانی کرده و به‌دلیل طراحی ماژولار آن، به راحتی قابلیت پشتیبانی از سیستم‌عامل‌ها و معماری‌های جدید را دارد. این ابزار دارای قابلیت توسعه افزونه و اسکریپت در خود است که کار کاربران را برای خودکارسازی و سفارشی کردن امور آسان‌تر می‌کند. این ابزار فعالیت‌های زیر را شامل می‌شود:

- لیست‌کردن تمامی فرآیندهای (Process) در حال اجرا
- لیست‌کردن کانکشن‌های شبکه فعال و بسته شده
- نمایش تاریخچه استفاده از اینترنت در سیستم
- شناسایی فایل‌های سیستم و بازیابی آن‌ها از طریق دامپ حافظه (Memory Dump)
- خواندن محتوای اسناد
- بازیابی دستورات اجرا شده در محیط CMD ویندوز
- پویش برای بدافزارهای موجود بر طبق قواعد YARA
- بازیابی اسکرین‌شات‌ها و محتوای کلیپ‌بورد
- بازیابی رمزهای عبور هش شده
- بازیابی کلیدهای SSL و گواهی‌نامه‌های آن‌ها
- تحلیل ریجستری، DLL ها و هوک API
- انجام مهندسی معکوس، تحلیل و شناسایی بدافزار

در ادامه دفترچه تقلب یا Cheat Sheet از قابلیت‌های این ابزار ارائه می‌شود.

استفاده اولیه

دستورات معمول کامپوننت‌ها	vol.py -f [image] --profile=[profile] [plugin]
نمایش پروفایل، اطلاعات آدرس و پلاگین‌ها	vol.py --info
نمایش مشخصات دستورات	vol.py --help
نمایش پارامترهای پلاگین‌ها	vol.py [plugin] --help
لود کردن پلاگین‌ها از دایرکتوری خارجی	vol.py --plugins=[path] [plugin]
مشخص نمودن آدرس DTB یا KDBG	vol.py --dtb=[addr] --kdbg=[addr]
مشخص نمودن خروجی فایل	vol.py –output-file=[file]

شناسایی Image

به‌دست‌آوردن اطلاعات سیستم‌عامل و معماری آن	imageinfo
شناسایی و تجزیه دیباگر بلاک داده	kdbgscan

هوک API

پویش برای هوک API	apihooks

پویش بر طبق YARA

پویش برای امضاهای YARA	yarascan

لیست‌کردن فرآیندها و اطلاعات آن‌ها

لیست‌کردن فرآیندهای فعال	pslist
پویش برای فرآیندهای پنهان یا متوقف شده	psscan
نمایش مراجع فرآیندها با لیست‌های مختلف	psxveiw
نمایش فرآیندها به شکل درخت والد-فرزند	Pstree
مشخصات بیشتر فرایندها با PID خاص	Specify –o/--offset=OFFSET or -p/--pid=1,2,3
نمایش DLL ها	dlllist
نمایش پارامترهای دستورات	cmdline
نمایش جزئیات VAD	Vadinfo [--addr]
دامپ‌کردن تخصیص‌ها به فایل‌های شخصی	Vaddump --dump-dir=PATH [--base]
دامپ‌کردن همه صفحات معتبر یک فایل	Memdump --dump-dir=PATH
نمایش هندل‌ها	handles
نمایش مجوزها	Privs
نمایش SID ها	getsids
نمایش متغیرهای محیطی	envars

کدهای تزریق شده

شناسایی و استخراج بلاک‌های کد تزریق‌شده	malfind
مراجع DLL ها با فایل‌های اختصاص‌داده‌شده حافظه	ldrmodules
پویش یک بلاک از کد در فرآیند یا حافظه کرنل برای API های ورودی	impscan

لاگ‌ها و تاریخچه‌ها

بازیابی رخدادهای لاگ	evtlogs
بازیابی تاریخچه دستورات	Cmdscan and consoles
بازیابی کش IE تاریخچه اینترنت	Iehistory
نمایش سرویس‌های در حال اجرا	svcscan

استخراج فایل PE

دامپ یک ماژول کرنل	moddump
دامپ یک فرآیند	procdump
دامپ DLL های حافظه فرآیند	dlldump

تحلیل ریجستری

نمایش hive های کش شده	hivelist
نمایش مقدار کلیدها و اطلاعات	printkey
دامپ داده‌های userassist	userassist
دامپ اطلاعات shellbag	Shellbags
دامپ the shimcache	shimcache

اشیاء کرنل

پویش برای درایور اشیاء	driverscan
پویش برای متغیرها	mutantscan
پویش برای تاریخچه فایل اشیاء	Filescan
پویش برای لینک اشیاء	symlinkscan

حافظه کرنل

modules	نمایش ماژول‌های لود شده در کرنل
modscan	پویش برای مابقی ماژول‌ها
Unloadedmodules	نمایش ماژول‌هایی که اخیراً لود نشده‌اند
timers	نمایش تایمر و DPC های مرتبط
Callbacks	نمایش بازگشت‌های از فراخوانی در کرنل
ssdt	وارسی SSDT
idt , gdt	وارسی IDT و GDT
driverirp	وارسی جداول IRP
Devicetree	نمایش درخت مربوط به دستگاه‌ها
pooltracker	نمایش وضعیت استفاده pool tag کرنل

اطلاعات شبکه

Connections and sockets	اطلاعات شبکه در ویندوز XP و ۲۰۰۳
Connscan and sockscan	پویش برای مابقی اطلاعات
netscan	اطلاعات شبکه در ویندوز ۷ و ویستا

Volshell

>>> ps()	لیست فرآیندها
>>> cc(pid=3028)	فیلتر کردن خروجی به ازای نام، pid و غیره
>>> process_space=	به‌دست‌آوردن آدرس فضای یک فرآیند
>>> dis(address, length, space)	دیس‌اسمبل کردن داده در فضای آدرس

>>> db(address, length, space)
>>> dd(address, length, space)
>>> dq(address, length, space)
	دامپ بایت‌ها، dwords و یا qwords

>>> dt("_EPROCESS", recursive = True)	نمایش یک ساختار
>>> dt("_EPROCESS", 0x820c92a0)	نمایش یک نمونه ساختار
>>> thread = obj.Object("_ETHREAD", offset=0x820c92a0, vm = addrspace())	ایجاد یک شی در فضای کرنل

دامپ کردن

Imagecopy –O/--output-image=FILE	ایجاد یک دامپ raw حافظه از hibernation، crash dump, firewire acquisition, virtualbox,Vmware snapshot, hpak, or EWF file
raw2dmp –O/--output-image=FILE	تبدیل نوع فایل aforementioned به Windows crash dump با ابزار Windbg

رشته‌ها

Strings -a -td FILE>strings.txt	استفاده از رشته‌های GNU و یا string.exe از مجموعه SYSInternal
strings	ترجمه آدرس‌های رشته‌ای

شناسایی بدافزار

دامپ کلیدهای RC4 مربوط به ZEUS/Citadel	Zeusscan and citadelscan
شناسایی و رمزگشایی پیکربندی‌های Poison Ivy	poisonivyconfig
رمزگشایی پیکربندی JAVA RAT	Javaratscan (github.com/Rurik)
شناسایی فرآیند hollowing	hollowfind

منابع فایل‌های سیستمی

پویش برای رکوردهای MFT	mftparser
استخراج فایل‌های کش شده	dumpfiles
تجزیه رکوردهای USN Journal	Usnparser (github.com/tomspencer)

حافظه GUI

نشست‌ها (نمایش لاگین‌های RDP)	sessions
نمایش مالکین کلیپ‌بورد در ویندوز	wndscan
شناسایی باج‌افزار در دسکتاپ	Deskscan
نمایش جداول نشست‌ها	Atoms and atomscan
دامپ محتوای کلیپ‌بورد	clipboard
دامپ محتوای USB	usbstor
شناسایی پیام هوک‌ها مانند کی‌لاگر	messagehooks
گرفتن یک اسکرین‌شات از دامپ حافظه	Screenshot --dump-dir=PATH
نمایش ویندوزهای پنهان و آشکار	Windows and wintree

بازیابی رمزهای عبور

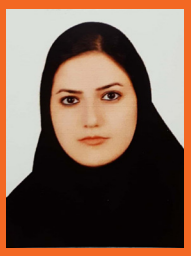
دامپ LSA secrets	lsadump
دامپ هش‌های دامنه کش شده	cachedump
دامپ هش‌های LM و NTLM	hashdump
استخراج اطلاعات کاربری از OpenVPN	Openvpn (github.com/Phaeilo)
استخراج کلیدهای خصوصی RSA و گواهی‌ها	dumpcerts

رمزنگاری دیسک

بازیابی TrueCrypt passphrases کش شده	truecryptpassphrase
مشخصات TrueCrypt	truecryptsummary
استخراج کلیدهای TrueCrypt	truecryptmaster

Volatility

- Some Notes
  - Declare Variables
  - Adding KDBG
- Identifying Image
  - imageinfo
- List Processes
  - pslist
  - psscan
  - psxview
  - pstree
- YARA
  - Scanning Against specific string with Rules
    - yarascan
- Analysing Registry
  - Find and list available registry hives
    - hivelist
  - Print all keys and subkeys in a hive
    - hivedump
  - Output a registry key, subkeys, and values
    - printkey
  - Extract all available registry hives
    - dumpregistry
  - Find and parse userassist key values
    - userassist
  - Dump user NTLM and Lanman hashes
    - hashdump
  - Map ASEPs to running processes
    - autoruns
  - Extracting Shellbags
    - shellbags
- Time-based objects found in memory
  - timeliner
- Network Scan
  - Scan for TCP Connections & Sockets
    - netscan
  - Scanning in XP Systems
    - connscan
- Find Malware
  - Find API Hooking
    - apihooks
  - Find Process Hollowing
    - hollowfind
  - Find unlinked DLLs
    - ldrmodules
  - Find injected code and dump sections
    - malfind
  - Find R00tkits
    - modscan
    - ssdt
    - driverirp
    - idt
- Analyzing DLLs & Handles
  - DLLs
    - dlllist
  - ProcessSID
    - getsids
  - Handles
    - handles
  - Drivers
    - driverscan
    - modules
- Dumpping
  - DLLs
    - List dll
      - dlllist
    - Dump DLLs
      - dlldump
  - Kernel Drivers
    - moddump
  - Processes
    - procdump
  - Memeory
    - memdump
  - Scan Object File&User Handles
    - filescan
    - userassist
    - windows.filescan
  - Extract Object File Handles
    - dumpfiles
  - Win Services
    - svcscan
  - CMD History
    - cmdscan
    - consoles
  - Console Information Output
    - consoles
  - Clipboard
    - clipboard
  - USB
    - usbstor



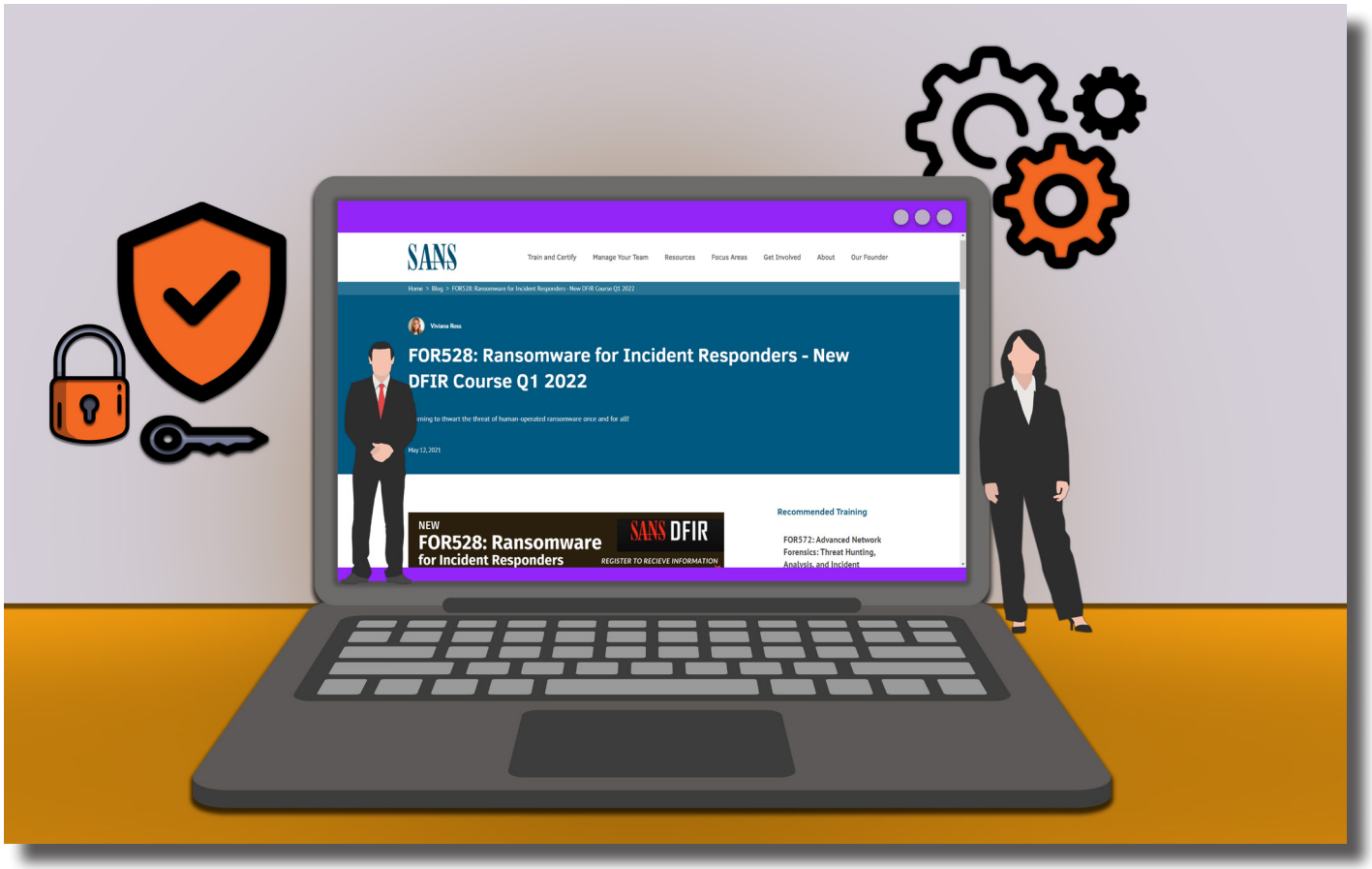
منا علی‌اکبری

aliakbarimona@gmail.com

معرفی دوره

FOR528

Ransomware for Incident Responders - New DFIR Course Q1 2022



مقدمه

موسسه SANS به‌عنوان پیشروترین سازمان در امر ارائه آموزش‌های گسترده و جامع در زمینه امنیت اطلاعات در دنیا شناخته شده است. دوره‌های طراحی شده توسط SANS به فراگیران می‌آموزد که چگونه از سیستم‌ها و شبکه‌های خود در برابر خطرات بالقوه امنیتی دفاع کنند. تدوین دوره‌های SANS به کمک متخصصان و محققانی در سراسر دنیا انجام می‌شود که هر یک در زمینه امنیت اطلاعات در سازمان‌های دولتی، شرکت‌ها و دانشگاه‌ها همه ساله زمان بسیاری را به تحقیق و انجام پروژه در زمینه امنیت اطلاعات اختصاص می‌دهند. دوره‌های موسسه SANS در سه سطح مقدماتی، متوسط و پیشرفته ارائه می‌شوند که نوع آموزش دوره‌های SANS از نظر نوع کاربرد به‌نحوی می‌باشد که شرکت‌کنندگان و فراگیران بلافاصله با گذراندن دوره این مهارت‌ها را می‌توانند در محیط‌های کاری خود، به کار ببرند.

در این مطلب، دوره آموزشی FOR528 با موضوع پاسخگویی به حوادث و حملات باج افزاری، توسط موسسه SANS ارائه شده است که در ادامه به آن پرداخته می‌شود.

مشخصات دوره

- ناشر: SANS
- مدرس: Ryan Chapman
- سطح: پیشرفته
- مدت زمان: چهار روز
- زبان: انگلیسی

مخاطبان دوره

- مدیران شبکه سازمانی
- تحلیلگران امنیت فناوری اطلاعات
- تیم‌های مدیریت پروژه
- دانشجویان و علاقه‌مندان

لینک

توضیح در خصوص دوره

امروزه آلودگی توسط باج‌افزار و خبر درخصوص این نوع حملات به یک امر رایج تبدیل شده است که در زندگی روزانه درباره آن می‌شنویم. از یک طرف تهدید باج‌افزار بسیار جدی و خطرناک بوده و کاربران و سازمان‌ها را با چالش‌های جدی مواجه کرده است اما از طرفی دیگر به یک بستر پررونق با سوددهی بالا برای تیم‌های باج‌افزاری تبدیل شده است. درخصوص باج‌افزار و شیوه‌های محافظت در برابر این حملات در شماره دهم همین فصل‌نامه به‌طور کامل توضیحاتی ارائه شده است.

حال درخصوص دوره FOR528 با عنوان پاسخگویی به حوادث و حملات باج‌افزاری اگر توضیح دهیم، هدف این دوره چهار روزه این است که به مخاطبان آموزش دهد که چگونه کنترل‌های حفاظتی را درخصوص این حملات فعال کنند و اطمینان حاصل کنند که نسخه‌های پشتیبان در مواجهه با یک حمله باج‌افزاری تا چه سطحی ایمن هستند. چک‌لیست‌های مربوطه برای حفاظت از منابع و بسترها در این دوره بررسی خواهند شد و اقدامات مهم و فوری نیز فراگرفته می‌شوند. به این ترتیب، مخاطبین نحوه پاسخگویی به حوادث در مواقعی که باج‌افزار در محیط به‌صورت فعال در حال گسترش است را فرا می‌گیرند.

آنچه خواهید آموخت:

- چگونه باج‌افزار تبدیل به یک تجارت بزرگ شده است.
- چگونه اپراتورهای باج‌افزارهای human-operated یا (HumOR) به تیم‌های باج‌افزاری تبدیل شده‌اند.
- چه کسانی بیشتر در معرض تهدید یک باج‌افزار هستند.
- چگونه اپراتورهای باج‌افزاری وارد محیط قربانیان خود می‌شوند.
- چگونه سازمان خود را در برابر تهدید HumOR آماده کنید.
- نحوه شناسایی ابزارهایی که اپراتورهای HumOR اغلب برای نفوذ به محیط و انجام فعالیت‌های post-exploitation در طول یک حمله باج‌افزار استفاده می‌کنند.
- چگونه اپراتورهای باج‌افزاری را در شبکه خود شناسایی کنید.
- زمانی‌که باج‌افزار به‌طور فعال در سیستم شما اجرا می‌شود، چگونه پاسخ دهیم.
- پس از حمله باج‌افزار چه اقداماتی باید انجام داد.
- نحوه شناسایی data exfiltration

نازیلا خسروی
n.khosravi@uok.ac.ir

معرفی کتاب

مشخصات

نام کتاب	Ransomware Protection Playbook
نویسنده	Roger A. Grimes
زبان	English
تعداد صفحات	320
ناشر و سال انتشار	Wiley; 1st edition (August 2021 ,27)

در دنیای دیجیتال امروزی، با شناسایی و یادگیری مراحلی ساده و اقداماتی عملی، می‌توان از تبدیل‌شدن به قربانی بعدی باج‌افزار پیشگیری کرد.

معرفی

لیست قربانیان باج‌افزار در سراسر دنیا روزبه‌روز بیشتر می‌شود و به همان اندازه که طولانی است، ناامیدکننده نیز می‌باشد اما خبر خوب این است که اقدامات زیادی می‌توان انجام داد تا خود و سیستم‌هایتان را در برابر نفوذگران و برنامه‌های مخرب ایمن کنید.

در این کتاب، راجر آ. گریمز، کهنه‌کار امنیت سایبری و ارزیاب امنیتی، یک نقشه‌ی راه عملی را برای سازمان‌هایی که به‌دنبال محافظت از شبکه‌های خود در برابر یکی از موذیانه‌ترین و مخرب‌ترین تهدیدات سایبری حال حاضر یعنی باج‌افزارها هستند، ارائه می‌دهد. با مطالعه‌ی این کتاب می‌توان گام‌های مشخصی را برای افزایش امنیت خود و آماده‌شدن در برابر حملات برداشت.

این نویسنده اقدامات پیشگیرانه‌ای برای جلوگیری از آلودگی به باج‌افزار، پیش از انجام آن را شرح می‌دهد. همچنین درخصوص چگونگی شناسایی سریع یک حمله، محدودکردن آسیب‌ها در صورت وقوع و نحوه‌ی تصمیم‌گیری در مورد پرداخت باج نیز بحث می‌کند.

این کتاب شما را آماده خواهد کرد تا درصورتی‌که در معرض تهدیدات امنیت قرار گرفتید، یک برنامه از پیش تعیین شده را اجرا کنید و آسیب مالی و اعتباری که سازمان شما متحمل می‌شود را محدود کنید. همچنین یاد خواهید گرفت که چگونه یک چهارچوب استاندارد از امنیت سایبری و حفاظت قانونی برای کاهش اختلالات احتمالی در فعالیت‌های تجاری خود را ایجاد کنید. با این چهارچوب امنیتی همچنین می‌توانید:

- طرح‌های از پیش ساخته‌ای در پاسخ به بحران در زمان حمله، ایجاد کنید.
- طرح‌های بیمه امنیت سایبری و حفاظت قانونی را ارزیابی و انتخاب کنید.
- از برخی از برجسته‌ترین و رایج‌ترین حملات باج‌افزاری انجام شده، درس بگیرید.
- احتمال تبدیل‌شدن به درس عبرت برای نسل‌های بعدی را کاهش دهید.

لینک

فهرست مطالب

Acknowledgments xi
Introduction xxi
Part I: Introduction
Chapter 1: Introduction to Ransomware
Chapter 2: Preventing Ransomware
Chapter 3: Cybersecurity Insurance
Chapter 4: Legal Considerations
Part II: Detection and Recovery 133
Chapter 5: Ransomware Response Plan
Chapter 6: Detecting Ransomware
Chapter 7: Minimizing Damage
Chapter 8: Early Responses
Chapter 9: Environment Recovery
Chapter 10: Next Steps
Chapter 11: What Not to Do
Chapter 12: Future of Ransomware

نویسنده

ROGER A. GRIMES نویسنده ۱۳ کتاب و بیش از ۱۱۰۰ مطلب و مقاله در حوزه امنیت رایانه، حملات نفوذگران و بدافزارها می‌باشد. ایشان از سخنرانان همیشگی در کنفرانس‌های امنیت رایانه می‌باشند و در سال‌های ۲۰۰۵ تا ۲۰۱۹ به‌عنوان نویسنده حوزه امنیت در مجلات CSO و InfoWorld بوده‌اند.

مطالعه‌ی کتاب برای چه کسانی مفید است؟

- متخصصان امنیت سایبری و اطلاعات
- مسئولین حفظ حریم خصوصی سازمان‌ها
- مدیران ریسک و تهدیدات
- مدیران ارشد فناوری اطلاعات
- تمامی علاقه‌مندان امنیت و افرادی که نگران امنیت داده‌های خود یا سازمانشان هستند.

مقاله تحقیقاتی

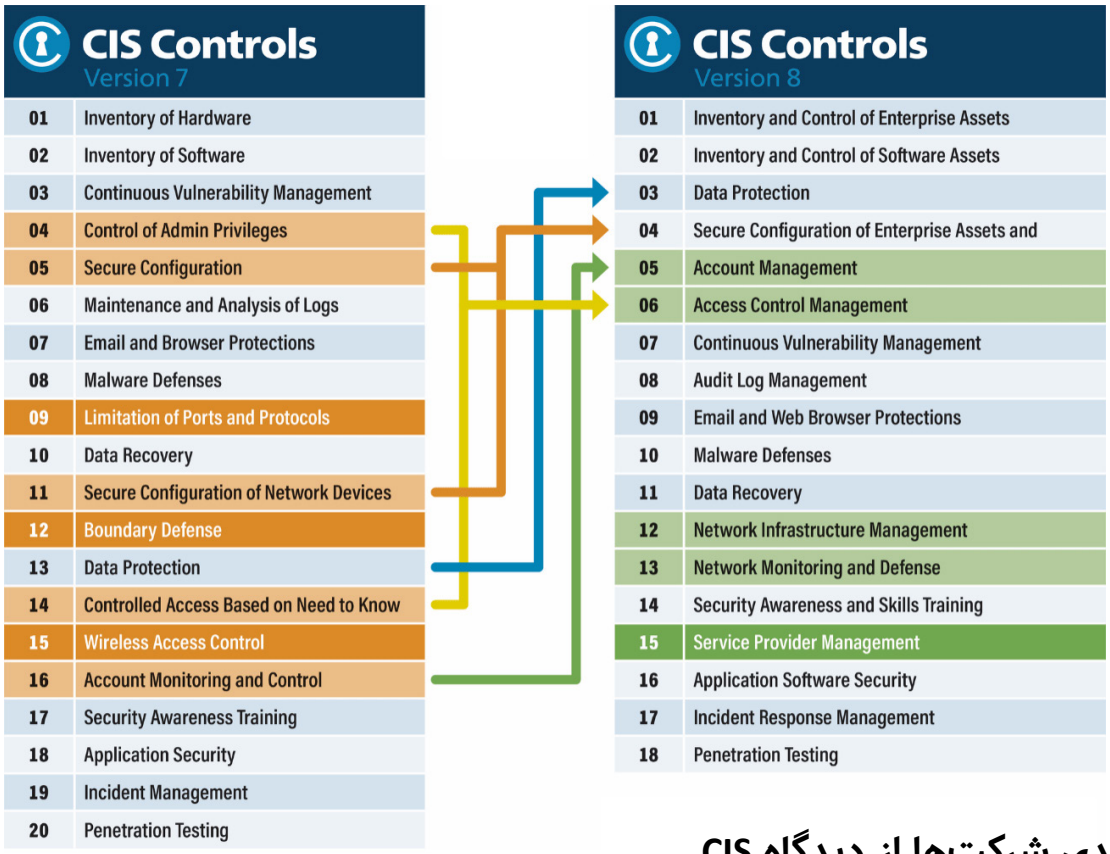
آرین فقیراللهی
Aryan.faghirollahy@gmail.com

پدرام قاسمی
ipedram91@gmail.com

چک‌لیست هجده کنترل بحرانی CIS در سازمان

مقدمه

حملات سایبری به‌سرعت در حال افزایش و تحول هستند به‌طوری که امروزه جلوگیری و دفاع در برابر آن‌ها دشوارتر از همیشه شده است. در اوایل سال ۲۰۰۸ در پاسخ به نشت داده‌های شرکت‌ها و سازمان‌ها، CIS در پایگاه صنعتی دفاعی ایالات متحده شروع به‌کار کرد. کنترل‌های آن که قبلاً به‌عنوان کنترل‌های امنیتی حیاتی شناخته می‌شدند، مجموعه‌ای از اقدامات توصیه‌شده برای دفاع سایبری هستند که راه‌های مشخص و عملی را برای توقف فراگیرترین و خطرناک‌ترین حملات امروزی ارائه می‌دهند. در ۱۸ می ۲۰۲۱، Center for Internet Security (CIS) نسخه ۸ را در کنفرانس جهانی RSA 2021 منتشر کرد.



طبقه‌بندی شرکت‌ها از دیدگاه CIS

IG1

یک شرکت IG1، شرکتی کوچک تا متوسط با تخصص محدود در زمینه فناوری اطلاعات و امنیت سایبری است که به حفاظت از دارایی‌ها و پرسنل فناوری اطلاعات اختصاص دارد. دغدغه اصلی این شرکت‌ها، عملیاتی نگه‌داشتن کسب‌وکارهایی است که تحمل محدودی برای خرابی دارند. حساسیت داده‌هایی که آن‌ها سعی در محافظت از آن‌ها دارند کم است و اصولاً اطلاعات مالی و کارمندان را شامل می‌شود.

IG2 (شامل IG1)

یک سازمان IG2 دارای افرادی است که به‌صورت ویژه مسئولیت مدیریت و حفاظت از زیرساخت فناوری اطلاعات آن سازمان را برعهده دارند. چنین سازمان‌هایی از بخش‌های مختلفی تشکیل شده‌اند. هر بخش دارای عملکرد، هدف و قوانین متفاوت و در نتیجه شرایط مخاطرات مختلف است. سازمان‌های IG2 معمولاً داده‌های سازمانی یا اطلاعات مهم مشتریان را ذخیره و پردازش نموده و می‌توانند در برابر وقفه‌های کوتاه‌مدت مقاومت کنند. با این وجود احتمال از دست‌دادن اعتماد عمومی در صورت وقوع رخنه‌های امنیتی وجود دارد. پیاده‌سازی و پیکربندی سازوکارهای امنیتی و حفاظتی منتخب در IG2 نیازمند فناوری سازمانی و تخصص‌های ویژه‌ای هستند. استفاده از چنین سازوکارهایی در سازمان‌ها امکان مقابله با پیچیدگی‌های روزافزون عملیاتی را فراهم می‌کند.

IG3 (شامل IG2 و IG1)

یک سازمان IG3 دارای کارشناسان امنیتی است که در حوزه‌های مختلف امنیت سایبری مانند مدیریت مخاطرات، آزمون نفوذپذیری و امنیت برنامه‌های کاربردی متخصص هستند. داده‌ها و دارایی‌های IG3 شامل اطلاعات یا عملکردهای حیاتی است که تحت نظارت‌های قانونی قرار داشته و مقررات خاصی بر روی آن‌ها اعمال می‌شود. چنین سازمانی باید دسترس‌پذیری یک مجموعه از خدمات و همچنین محرمانگی و جامعیت داده‌های حساس را تضمین کند. وقوع حملات موفق بر ضد این سازمان‌ها می‌تواند آسیب جدی به رفاه عمومی وارد کند. راهکارهای حفاظتی منتخب برای IG3 باید مانع از اجرای حملات هدفمند از سوی مهاجمان پیشرفته شده و پیامدهای منفی ناشی از وقوع حملات روز صفر را کاهش دهند.

۱ موجودی و کنترل دارایی‌های شرکت

CONTROL 01 Inventory and Control of Enterprise Assets

5 Safeguards | IG1 2/5 | IG2 4/5 | IG3 5/5

هر شرکتی نیازمند مدیریت فعال شامل موجودی، پیگیری و اصلاح دارایی‌های سازمانی خود است. دارایی‌های سازمانی شامل سیستم‌های کاری و شخصی مانند تلفن همراه یا لپ تاپ، تجهیزات شبکه، تجهیزات مربوط به اینترنت اشیا (IOT) و سرورها می‌شوند. این کار به شرکت‌ها کمک می‌کند تا لیست کامل و دقیقی از دارایی‌هایی بیابند که نیاز به کنترل و رصد شدن دارند. به‌علاوه، این کنترل به شرکت‌ها کمک می‌کند دارایی‌های ثبت نشده و مدیریت نشده خود را حذف یا اصلاح کنند. این دارایی‌ها شامل هر دستگاه یا سیستمی که به زیرساخت‌های فیزیکی یا مجازی سازمان متصل یا از راه دور (Remote) و یا ابری (cloud) به‌نحوی با سازمان در ارتباط هستند، می‌شوند.

۲ موجودی و کنترل دارایی‌های نرم‌افزاری

CONTROL 02 Inventory and Control of Software Assets

7 Safeguards | IG1 3/7 | IG2 6/7 | IG3 7/7

شرکت‌ها نیازمند مدیریت فعال کلیه نرم‌افزارهای خود (سیستم عامل‌ها و برنامه‌های کاربردی) در شبکه هستند، به‌گونه‌ای که تنها نرم‌افزارهای مجاز نصب شده و قابل اجرا باشند. در این نوع کنترل نرم‌افزارهای غیرمجاز و مدیریت نشده شناسایی شده و از نصب و اجرا آن‌ها جلوگیری می‌شود.

۳ حفاظت از داده‌ها

CONTROL 03 Data Protection

14 Safeguards | IG1 6/14 | IG2 12/14 | IG3 14/14

در اکثر شرکت‌ها و سازمان‌های توسعه فرآیندها و کنترل‌های فنی برای شناسایی، طبقه‌بندی، حفظ و آگاهی از داده‌ها به شکل صحیح انجام نمی‌شود. حفاظت از داده‌ها به ما کمک می‌کند کنترل بیشتری بر آن‌ها داشته باشیم و از وقوع حوادث مربوط به داده‌ها مانند نشت اطلاعات جلوگیری کنیم.

٤ پیکربندی امن دارایی‌ها و نرم‌افزارهای سازمانی

CONTROL 04 Secure Configuration of Enterprise Assets and Software

12 Safeguards | IG1 7/12 | IG2 11/12 | IG3 12/12

پیکربندی ایمن دارایی‌های سخت‌افزاری سازمانی و سیستم‌های شخصی مانند لپ‌تاپ‌ها و تلفن‌های همراه، تجهیزات شبکه، تجهیزات مربوط به اینترنت اشیاء (IOT) و سرورها و دارایی‌های نرم‌افزاری مانند سیستم‌عامل‌ها و نرم‌افزارها باید بسیار مورد توجه قرار گیرد.

۵ مدیریت حساب‌های کاربری

انجام روال‌هایی برای اختصاص‌دادن و مدیریت احراز هویت‌هایی که منجر به اعطا اعتبارنامه برای حساب‌های کاربری مانند حساب Administrator یا هر نوع دسترسی دیگر، مدیریت حساب‌های کاربری نام دارند. این مدیریت به ما کمک می‌کند به هر فردی به اندازه نیازش دسترسی بدهیم و از دسترسی خارج از اندازه افراد به بسترها و داده‌ها جلوگیری کنیم.

CONTROL 05 Account Management

6 Safeguards | IG1 4/6 | IG2 6/6 | IG3 6/6

٦ مدیریت کنترل دسترسی

استفاده از فرآیندها و ابزارها برای ایجاد، اختصاص، مدیریت و حتی لغو اعتبار و امتیازات دسترسی برای حساب‌های مختلف کاربری در ارتباط با دارایی‌ها و نرم‌افزارهای سازمانی، مدیریت کنترل دسترسی است که در یک شرکت یا سازمان دارای اهمیت بالایی است.

CONTROL 06 Access Control Management

8 Safeguards | IG1 5/8 | IG2 7/8 | IG3 8/8

۷ مدیریت مستمر آسیب‌پذیری

میبایستی برنامه‌ای برای ارزیابی و ردیابی مستمر آسیب‌پذیری‌ها در تمام دارایی‌های سازمانی، درون زیرساخت‌های شرکت طراحی کنید که هدف آن اصلاح و به حداقل رساندن نقص‌های امنیتی باشد که می‌توانند منجر به حملات شوند. همچنین در برنامه‌ریزی‌ها باید یافتن تهدیدات و آسیب‌پذیری‌های جدید نیز مدنظر قرار گیرد.

CONTROL 07 Continuous Vulnerability Management

7 Safeguards | IG1 4/7 | IG2 7/7 | IG3 7/7

۸ مدیریت و بررسی گزارش‌های لاگ‌ها

گزارش‌های مربوط به لاگ‌ها را می‌توان برای شناسایی تهدیدات و مخاطرات بررسی و رصد کرد و در سرورها، سیستم‌عامل‌ها و نرم‌افزارهای مختلفِ مورد استفاده، اطلاعات مربوط به لاگ‌ها جمع‌آوری، بررسی و نگهداری شوند.

CONTROL 08 Audit Log Management

12 Safeguards | IG1 3/12 | IG2 11/12 | IG3 12/12

CIS Controls

۹ حفاظت از ایمیل و مرورگر وب

CONTROL 09 Email and Web Browser Protections

7 Safeguards | IG1 2/7 | IG2 6/7 | IG3 7/7

حفاظت و شناسایی تهدیدات از طریق ایمیل و وب را بهبود دهید زیرا این دو فرصت‌های خوبی برای مهاجمان ایجاد می‌کنند تا از طریق فعالیت‌هایی که در این دو بستر دارند رفتارهایشان را شناسایی و از نقاط ضعف آن‌ها سوءاستفاده کنند. مرورگرهای وب و حساب‌های ایمیل به‌دلیل تعامل مستقیم آن‌ها با کاربران داخل یک سازمان، نقاط بسیار رایج ورود مهاجمان هستند. محتوای ارائه شده به کاربران در این دو بستر را می‌توان به گونه‌ای تولید کرد که کاربران را به افشای اطلاعات، ارائه داده‌های حساس یا فراهم آوردن بستری برای دسترسی مهاجمان و در نتیجه افزایش خطر برای شرکت، ترغیب کرد. از آنجایی که ایمیل و وب، ابزار اصلی تعامل کاربران و بسترهای خارج از سازمان است، این موارد اهداف اصلی برای کدهای مخرب و مهندسی اجتماعی خواهند بود. طبق آمارها درصد بالایی از حملات نیز نشات گرفته از این دو بستر است.

۱۰ بدافزارها

CONTROL 10 Malware Defenses

7 Safeguards | IG1 3/7 | IG2 7/7 | IG3 7/7

باید از دانلود، پخش و اجرای بدافزارها و کدهای مخرب بر روی بسترهای مختلف سازمانی خود جلوگیری کنید یا با یک برنامه دقیق، کنترل کاملی بر آن‌ها داشته باشید.

۱۱ بازیابی اطلاعات

CONTROL 11 Data Recovery

5 Safeguards | IG1 4/5 | IG2 5/5 | IG3 5/5

روش‌های کافی و مختلفی برای حفظ و نگهداری از داده‌ها و دارایی‌های سازمانی ایجاد کنید تا حوادث غیرمترقبه (عمدی یا سهوی) باعث ازدست‌رفتن داده‌ها نشوند و یک وضعیت امن در این بستر ایجاد کنید.

۱۲ مدیریت زیرساخت شبکه

CONTROL 12 Network Infrastructure Management

8 Safeguards | IG1 1/8 | IG2 7/8 | IG3 8/8

برای پیشگیری از بهره‌برداری از نقاط ضعف سرویس‌های شبکه و نقاط دسترسی شما توسط مهاجمان، دستگاه‌های شبکه و زیرساخت را از این منظر به‌صورت فعال مانیتور و مدیریت کنید.

۱۳ نظارت و دفاع از شبکه

CONTROL 13 Network Monitoring and Defense

11 Safeguards | IG1 0/11 | IG2 6/11 | IG3 11/11

روال‌ها و ابزارهایی برای مانیتور کردن و دفاع جامع از شبکه خود در برابر تهدیدات امنیتی در کل زیرساخت و کاربران ایجاد کنید.

۱۴ آگاهی‌رسانی و مهارت‌های امنیتی

برای کاهش خطرات امنیت سایبری در شرکت، دوره‌ها و کلاس‌های آموزشی امنیت برای ارتقاء دانش کارمندان خود برگزار کنید تا از اطلاعاتی درخصوص امنیت سایبری و مهارت کافی در این زمینه برخوردار باشند. اقدامات افراد نقش مهمی در موفقیت یا شکست برنامه امنیتی یک شرکت دارد. برای مهاجم آسان‌تر است که کاربر را به کلیک‌کردن بر روی یک لینک یا بازکردن یک پیوست ایمیل برای نصب بدافزار به‌منظور ورود به یک شرکت، ترغیب کند تا اینکه یک اکسپلویت را برای انجام مستقیم آن بیابد.

CONTROL 14 Security Awareness and Skills Training

9 Safeguards | IG1 8/9 | IG2 9/9 | IG3 9/9

۱۵ مدیریت ارائه‌دهنده خدمات

فرآیندی برای ارزیابی ارائه‌دهندگان خدماتی که داده‌های حساس را در اختیار دارند، یا مسئول پلتفرم‌ها یا فرآیندهای فناوری اطلاعات حیاتی یک سازمان هستند، ایجاد کنید تا مطمئن شوید که این ارائه‌دهندگان از آن پلتفرم‌ها و داده‌ها به‌طور مناسب محافظت می‌کنند.

CONTROL 15 Service Provider Management

7 Safeguards | IG1 1/7 | IG2 4/7 | IG3 7/7

۱۶ امنیت نرم‌افزار کاربردی

چرخه عمر امنیتی نرم‌افزارهای داخلی توسعه‌یافته، میزبانی شده یا به دست آمده را مدیریت کنید تا از ضعف‌های امنیتی پیش از تأثیرگذاری بر سازمان جلوگیری کرده و آن‌ها را شناسایی و اصلاح کنید.

CONTROL 16 Applications Software Security

14 Safeguards | IG1 0/14 | IG2 11/14 | IG3 14/14

۱۷ مدیریت واکنش به حوادث

برنامه‌ای برای ارتقاء مهارت و قابلیت واکنش به حوادث مانند سیاست‌ها، طرح‌ها، نقش‌های تعریف شده، آموزش و ارتباطات برای آماده‌سازی، شناسایی و پاسخ سریع به حملات مختلف را ایجاد کنید.

CONTROL 17 Incident Response Management

9 Safeguards | IG1 3/9 | IG2 8/9 | IG3 9/9

۱۸ تست نفوذ

یکی از فعالیت‌های مهم در یک سازمان، ارزیابی امنیتی سامانه‌ها و نرم‌افزارها، شبکه و سیستم‌عامل‌ها و بررسی پیکربندی‌ها است. از طریق شناسایی نقاط ضعف در کنترل‌ها (افراد، فرآیندها و فناوری) و شبیه‌سازی حملات و اقدامات مهاجم، اثربخشی و انعطاف‌پذیری راهکارهای امنیتی شرکت را آزمایش کنید. تمامی این اقدامات از طریق اجرای تست نفوذ در بسترهای مختلف و به‌صورت دوره‌ای امکان‌پذیر است.

CONTROL 18 Penetration Testing

5 Safeguards | IG1 0/5 | IG2 3/5 | IG3 5/5

مقاله تحقیقاتی

آرین فقیراللهی
Aryan.faghirollahy@gmail.com

ژوان عبدمؤخر
jowanaabdmoakher.apa@gmail.com

آمار حملات سایبری در سال ۲۰۲۲

مقدمه

حملات سایبری در سال ۲۰۲۰ با کسب رتبه پنجم در لیست رتبه‌بندی تهدیدات جهانی، در میان مهم‌ترین و جدی‌ترین موارد قرار گرفتند و تلنگرهای جدیدی را به بخش‌های دولتی و خصوصی وارد کردند. پیش‌بینی‌ها و شواهد موجود نشان می‌دهند که این صنعت مخاطره‌آمیز در سال ۲۰۲۲ هم به رشد خود ادامه خواهد داد. یکی از این پیش‌بینی‌ها، مربوط به حملات سایبری در حوزه اینترنت اشیاء است که انتظار می‌رود تا سال ۲۰۲۵ به تنهایی دو برابر شود. مشکل بسیار مهم دیگر در حوزه امنیت سایبری، نرخ ناچیز شناسایی و پیگیری جرایم سایبری است. طبق گزارش the World Economic Forum's 2020 Global Risk Report نرخ شناسایی و یا تعقیب قضائی حملات سایبری در آمریکا رقم ناچیز ۰٫۰۵٪ است.

اگر شما یکی از افراد زیادی هستید که یک استارت‌آپ در حال رشد را اداره می‌کنید، لازم است بدانید که چشم اندازها همواره در حال تغییر است، همان‌گونه که سال ۲۰۲۰ تغییرات بسیاری را با خود به همراه داشت، شرایط همه‌گیری کووید-۱۹، همه کسب‌وکارهای کوچک و بزرگ را تحت تأثیر قرار داده است. به‌دلیل انجام گسترده فعالیت‌ها به‌صورت دورکاری در دو سال گذشته، شک و تردیدهای پیرامون آن و نحوه محافظت از داده‌ها، نرخ حملات سایبری رشد کرده‌اند. این جرایم سایبری بازه گسترده‌ای را شامل می شوند (از سرقت پول گرفته تا کلاهبرداری در فضای سایبری و نشت داده‌ها). آمارها نشان می‌دهند که این حملات در نتیجه همه‌گیری ویروس کرونا تا ٦٠٠٪ افزایش یافته‌اند. این امر تقریبا تمام کسب‌وکارها و صنایع را مجبور به پذیرش راه‌حل‌های جدید و سازگار سریع با آن‌ها کرده است. در این میان سؤالی که مطرح می‌شود این است که، شما چگونه می‌توانید استارت‌آپ خود را برای امن نگه داشتن داده‌ها در سال ۲۰۲۲ آماده کنید؟

در این مطلب، مهم‌ترین آمارها، هشدارها، نکات و توصیه‌های امنیت‌سایبری در حوزه استارتاپ‌ها بررسی و تشریح می‌شوند.

رشد هزینه‌های جرایم سایبری

هزینه‌های مربوط به جرایم سایبری برای کسب‌وکارها و صنایع در سال ۲۰۲۵، سالانه تقریبا ۱۰٫۵ تریلیون دلار تخمین زده شده است. این رقم در سال ۲۰۱۵ تنها ۳ تریلیون دلار بوده است. آمارها نشان می‌دهد که هزینه‌های مربوط به جرایم سایبری سالانه نرخ رشد ۱۵٪ را تجربه می‌کنند. براساس گزارش شرکت cybersecurity ventures جرایم سایبری بزرگ‌ترین انتقال دهنده ثروت اقتصادی در تاریخ هستند.

تأثیر جرایم سایبری بر کسب‌وکارهای کوچک و متوسط

حملات سایبری همه کسب‌وکارها را تهدید می‌کنند اما در این میان کسب‌وکارهای کوچک و متوسط هدف حملات بیشتر و پیچیده‌تر قرار می‌گیرند. طبق گزارش Accenture's Cost of Cybercrime Study، با وجود اینکه کسب‌وکارهای کوچک هدف ٤٣٪ حملات سایبری هستند اما تنها ١٤٪ آن‌ها راهکارهای مناسب دفاع سایبری برای خود آماده کرده‌اند.

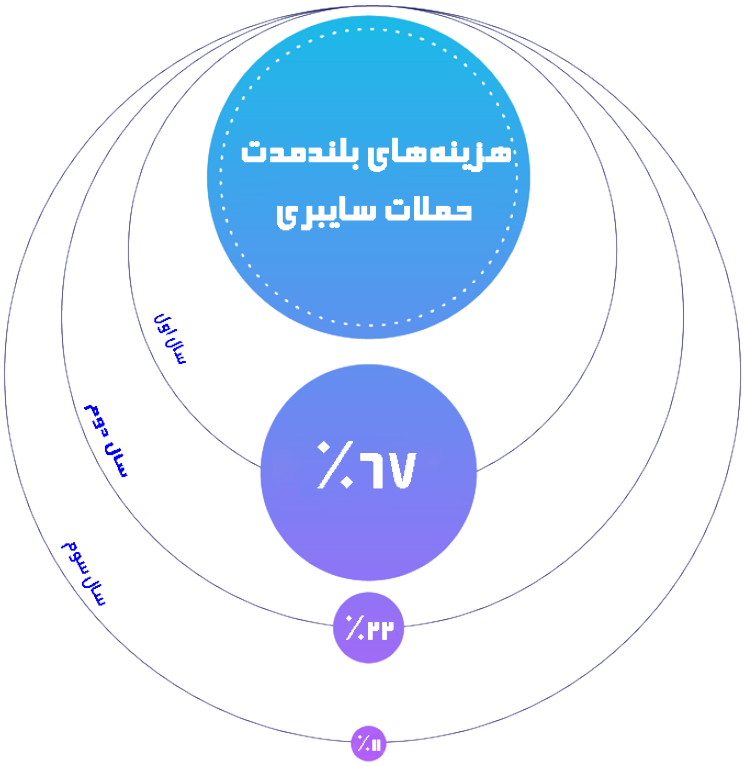
حملات سایبری نه تنها باعث اختلال در عملکردهای عادی شرکت می‌شوند بلکه صدمات زیادی را به زیرساخت‌های فنی و سیستمی وارد می‌کنند، صدماتی که بدون صرف هزینه‌های فراوان و منابع مورد نیاز، گاهاً غیرقابل بازگشت هستند. شایان ذکر است به‌عنوان رهبر یک کسب‌وکار، با درک اهداف حملات و پیامدهای آن، می‌توانید شدت حملات و آسیب‌های احتمالی را به حداقل برسانید و امنیت سایبری خود را بهبود ببخشید.

به نقل از گزارش وضعیت امنیت سایبری موسسه phonemon، کسب‌وکارهای کوچک و متوسط بر اساس تجربیات اخیر خود در مورد حملات سایبری، وضعیت امنیتی خود را به شکل زیر تعریف می‌کنند:

- **اقدامات امنیتی ناکافی:** ٤٥٪ معتقدند که فرآیندهای آن‌ها در کاهش حملات سایبری غیرموثر بوده است.
- **فراوانی حملات:** ٦٦٪ در ١٢ ماه گذشته حمله سایبری را تجربه کرده‌اند.
- **حملات هدفمند:** ٦٩٪ بر این باورند حملات سایبری هدفمندتر شده‌اند.

رایج‌ترین انواع حملات به کسب‌وکارهای کوچک

- حملات بر پایه مهندسی اجتماعی و سرقت اطلاعات به کمک صفحات جعلی (فیشینگ): ٥٧٪
- سرقت داده‌ها و ایجاد چالش فنی و غیرفنی: ٣٣٪
- سرقت اعتبارات و اطلاعات حساب‌های کاربری: ٣٠٪



هزینه‌های بلندمدت حملات سایبری

هزینه‌های بلند مدت حملات سایبری می‌توانند چندین ماه یا حتی چندین سال شرکت شما را درگیر کنند. اگر شرکت از وجود حملات و نفوذها بی‌اطلاع باشد و آن‌ها را در برنامه‌ریزی‌هایش پیش‌بینی نکرده باشد، این هزینه‌ها می‌توانند به طرز قابل توجهی افزایش یابند. از دست دادن داده‌ها، اختلال در کسب‌وکار، از دست دادن درآمد در اثر غیرفعال بودن سیستم‌ها و یا حتی صدمه زدن به شهرت و اعتبار برند تجاری می‌توانند شامل این هزینه‌ها باشند. تصویر روبرو، میزان تأثیراتی که یک کسب‌وکار ممکن است در سه سال بعد از یک حمله سایبری با آن مواجه شود را به‌تصویر کشیده است.

تأثیر و شدت حملات سایبری

حملات سایبری می‌توانند با توجه به شدت حمله، به شکل‌های مختلف بر یک سازمان تأثیر بگذارند. این تاثیرات بازه گسترده‌ای را شامل می‌شوند (از کم خطرترین آن‌ها یعنی اختلالات جزئی در عملیات روزانه و معمولی گرفته تا خطرناک‌ترین آن‌ها یعنی خسارات مالی بزرگ). اما نکته حائز اهمیت این است که تمام حملات سایبری بدون در نظر گرفتن نوع آن‌ها، هزینه‌های مالی یا غیرمالی به همراه خواهند داشت.

پنج زمینه‌ای که کسب‌وکار شما ممکن است آسیب ببیند به شرح مقابل است:

- زیان‌های مالی
- از دست دادن بهره‌وری
- صدمه به اعتبار
- مسئولیت‌های قانونی در برابر یک شرکت ثانوی
- تداوم مشکلات شرکت (عدم وجود منابع و
- پشتیبانی‌های لازم مالی یا فنی)

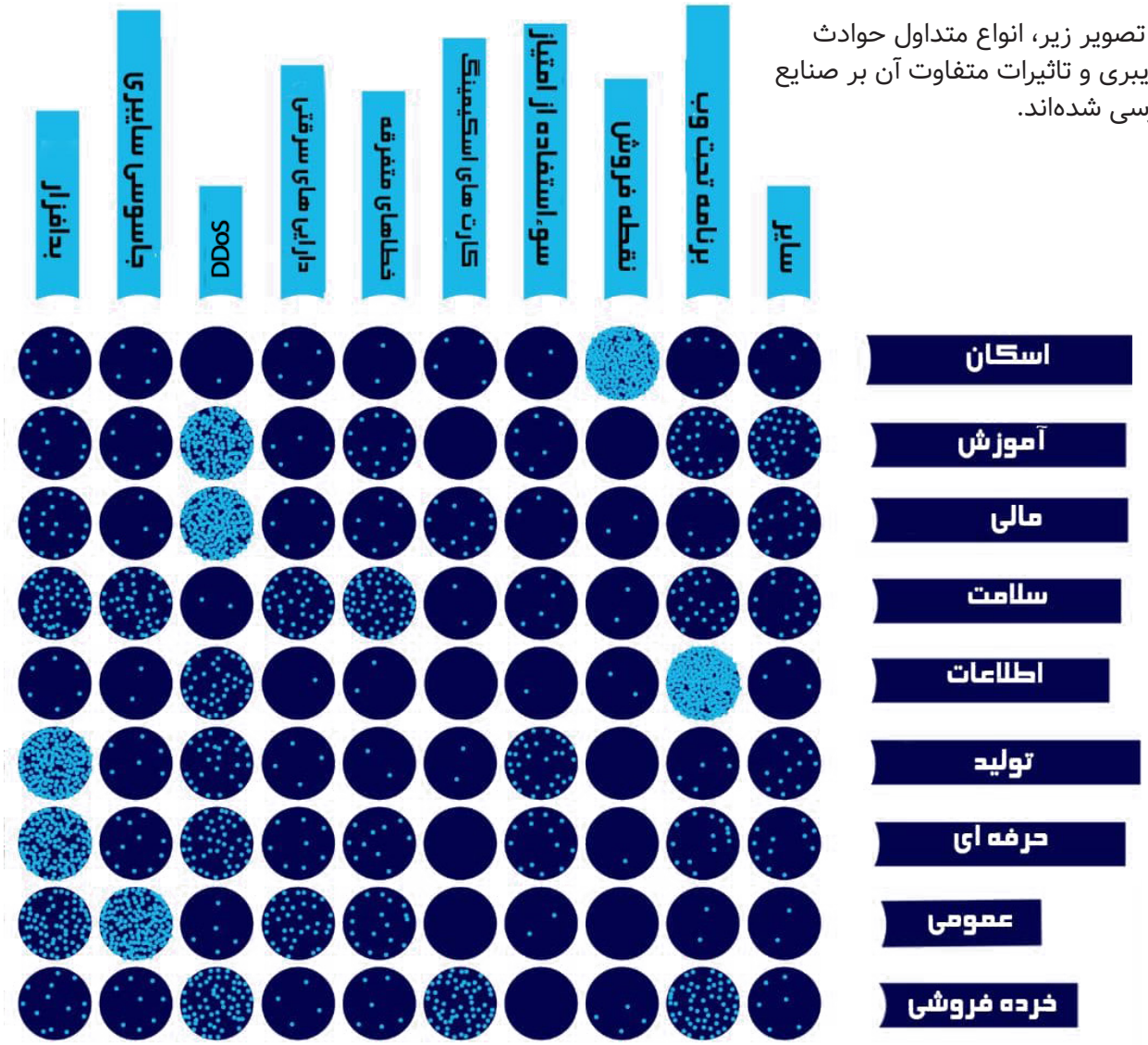
حملات باج‌افزاری به‌عنوان نگران‌کننده‌ترین چالش در سال‌های اخیر به شمار می‌رود. در پایان سال ۲۰۱۶، هر ۴۰ ثانیه یک کسب‌وکار قربانی یک حمله باج‌افزاری می‌شد. طبق گزارش Cybersecurity Ventures، این میزان در سال ۲۰۲۱ به ۱۱ ثانیه کاهش پیدا کرده است. این نوع حملات به وسیله یک برنامه مخرب، دسترسی به اطلاعات یا کامپیوترها را از طریق قفل یا رمزگذاری آن‌ها محدود می‌کنند و تا زمانی که شرکت قربانی به مجرمان باج موردنظر را نپردازد، داده‌ها و سیستم‌ها از دسترس خارج خواهند بود. در این میان، حتی با پرداخت مبلغ مورد نظر باج‌افزار، هیچ تضمینی برای بازگشت اطلاعات وجود ندارد. بهترین دفاع درباره باج‌افزارها پیشگیری از طریق روش‌های مختلف و داشتن نسخه‌های متعدد پشتیبان از اطلاعات حیاتی است.

صنایع آسیب‌پذیر در برابر حملات سایبری

در حالی که هر صنعتی ممکن است در معرض حملات سایبری باشد، اما برخی از آن‌ها به دلیل ماهیت تجاری خود بیشتر در معرض خطر هستند. این کسب‌وکارها، مشاغلی هستند که از نزدیک با زندگی روزمره مردم درگیر هستند و یا اطلاعات حساس و هویتی را نگهداری می‌کنند. طبق بررسی‌ها این کسب‌وکارها اهداف جذاب‌تری برای هکرها هستند. این مشاغل عبارتند از:

- **بانک‌ها و موسسات اعتباری:** به‌دلیل نگهداری اطلاعات حساب‌های بانکی، کارت‌های اعتباری و اطلاعات شخصی مشتری‌ها.
- **موسسات حوزه سلامت:** به‌دلیل نگهداری‌کردن اطلاعات مربوط به سلامت افراد، تحقیقات کلینیکی، اطلاعات شخصی و اطلاعات مربوط به پرداخت‌ها و بیمه‌ها.
- **شرکت‌ها:** به‌دلیل نگهداری اطلاعاتی همچون طرح‌های تجاری، دارایی‌های فکری، استراتژی‌های فروش، اطلاعات مربوط به مشتری‌ها و کارمندان، قرارداد معاملات مالی و اطلاعات گوناگون دیگر.
- **موسسات علمی و دانشگاهی:** به‌دلیل نگهداری اطلاعات مربوط به ثبت‌نامی‌ها، تحقیقات علمی و دانشگاهی، اطلاعات مالی و اطلاعات هویتی.

در تصویر زیر، انواع متداول حوادث سایبری و تاثیرات متفاوت آن بر صنایع بررسی شده‌اند.

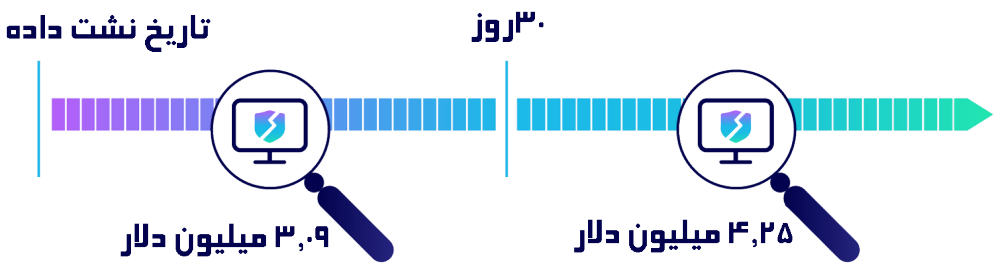


نشت داده

نشت داده به معنای دسترسی پیدا کردن به اطلاعات خصوصی و محرمانه توسط افرادی است که مجوز این کار را ندارند.کشف نشت داده زمانی صورت می‌گیرد، که شرکت یا کسب‌وکار از وقوع حادثه آگاه می‌شود. به گفته IBM ، کشف نشت داده توسط یک شرکت به صورت میانگین ۱۹۷ روز و برای مهار آن تا ٦٩ روز دیگر زمان لازم است. در این میان شرکت‌هایی که در کمتر از ۳۰ روز موفق به مهار نشت داده می‌شوند، به‌طور میانگین بیش از یک میلیون دلار صرفه‌جویی خواهند کرد. هر تاخیری در این فرایند هزینه‌های سنگینی مانند از دست‌دادن مشتری‌های بیشتر، کاهش اعتماد عمومی و جریمه‌های سنگین‌تر طبق قوانین GDPR را در پی خواهد داشت.

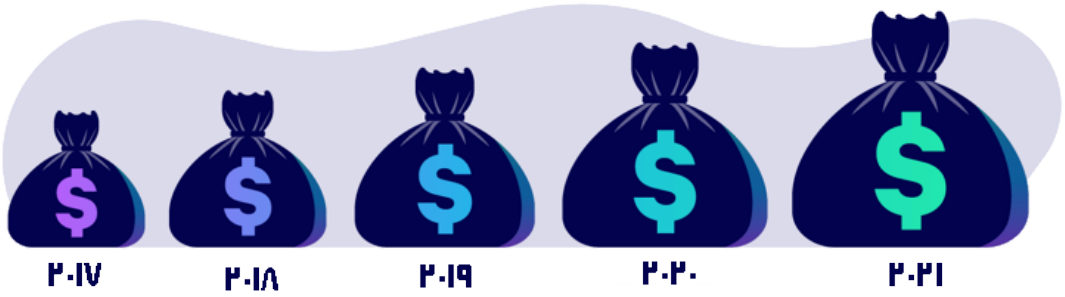
داشتن یک برنامه و سیاست درخصوص مسئولیت‌ها و فعالیت‌ها در نشت داده یک راهکار عملی برای آمادگی در زمان‌هایی است که نشت داده رخ می‌دهد. این برنامه سندی است که در آن واکنش‌های فوری و اطلاعات مورد نیاز برای مدیریت یک نشت داده با جزییات تشریح شده است. این سند راهنمایی برای تیم شما در جریان عملیات کشف، تحقیق و بررسی، اصلاح، مهار و بازیابی حالت اولیه در حادثه نشت داده است. داشتن یک استراتژی مدیریت خطر هم در جایگاه مقابله با حوادثی مثل نشت داده می‌تواند تاثیرات مخرب آن را به حداقل برساند.

کشف نشت داده به طور متوسط ۱۹۷ روز طول می‌کشد



میزان هزینه جهانی برای امنیت سایبری

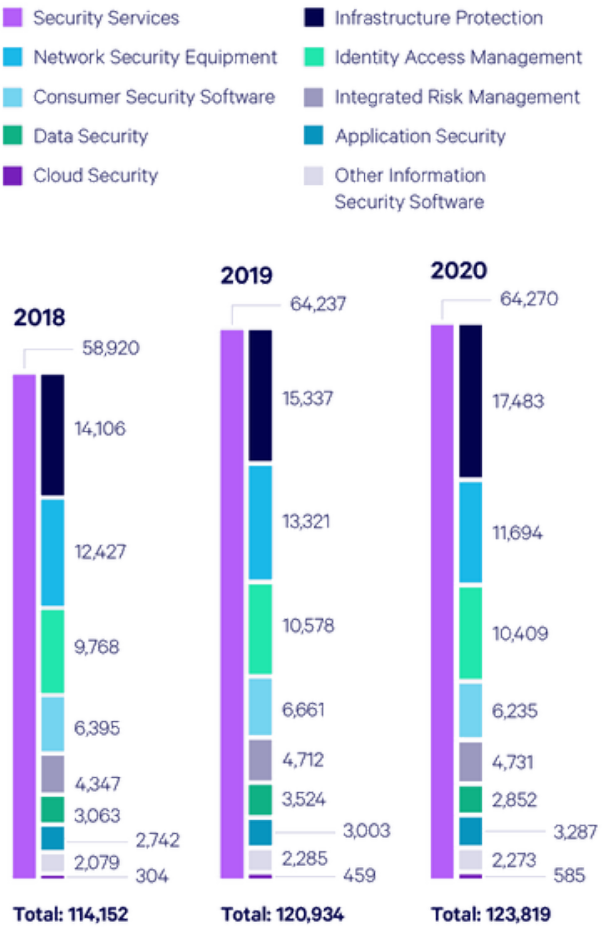
پیش‌بینی می‌شود که هزینه‌های جهانی برای محصولات و خدمات امنیت سایبری در دوره پنج ساله ۲۰۱۷ تا ۲۰۲۱ در مجموع از ۱ تریلیون دلار فراتر رفته و این رقم ۱۲ تا ۱۵٪ رشد سود سالانه بازار امنیت سایبری از سال ۲۰۲۱ است



پیش‌بینی می شود بودجه امنیت سایبری در سه سال آینده افزایش پیدا کند

٪۷۱

در این نمودار به تفکیک بخش، می توان میزان این رشد را در یک بازه زمانی سه ساله (از ۲۰۱۸ تا ۲۰۲۰) مشاهده کرد و نگاهی به نحوه رشد هزینه‌های امنیت سایبری به تفکیک محصول یا خدمت در سراسر جهان انداخت.



چه کسانی مسئول نشت داده هستند؟

مردم گمان می‌کنند اطلاعات ذخیره شده در پایگاه داده شرکت‌ها، صرفاً اسناد و اطلاعاتی درباره شرکت‌ها هستند اما هکرها و مهاجمین ارزش واقعی این اطلاعات را می‌دانند. به‌همین دلیل برای به‌دست‌آوردن آن‌ها تلاش می‌کنند اما همیشه هکرها نیستند که مسبب لو رفتن اطلاعات می‌شوند؛ بنابه گزارش شرکت Verizon's data breach investigation، اکثر حملات سایبری توسط افراد خارجی، افراد داخلی، شرکای شرکت، گروه‌های هکری سازمان‌یافته و گروه‌های وابسته انجام می‌شوند. میزان انجام حملات توسط این افراد را می‌توان به صورت زیر دسته بندی کرد. مسبب ۷۰٪ حملات سایبری افراد خارج از سازمان هستند؛ این یعنی کارمندان و افراد داخلی شرکت در لو رفتن داده‌ها ۳۰٪ سهم دارند که این رقم قابل توجه‌ای است. به‌دلیل همین سهم قابل توجه افراد داخلی سازمان و درصد بالای نفوذها بر پایه مهندسی اجتماعی، باید بر روی آموزش افراد داخلی سازمان بیشتر تمرکز کرد. در این آموزش‌ها باید آن‌ها را با انواع روش‌های فریب و نفوذ بر پایه مهندسی اجتماعی آشنا کرد تا بتوان خطرات قابل توجه این دسته از حملات را کاهش داد. در شکل پایین می‌توان علاوه‌بر گروه‌های بزرگی که سهم قابل توجهی در زمینه نشت داده دارند، گروه‌های دیگر، با سهم‌های کوچک‌تر را نیز مشاهده کرد.

چگونه خطر حملات سایبری را کاهش دهیم؟

با افزایش تهدیدات مربوط به سوءاستفاده هکرها از داده‌های کاربران، پس از اجرای فرآیندهایی برای جلوگیری از نشت داده، بهترین کار، داشتن یک سیاست در زمینه نشت داده است. قوانین مربوط به نشت داده با توجه به قوانین کشورها، مختلف هستند. شما باید با توجه به موقعیت جغرافیایی کسب‌وکار خود، عوامل مختلفی را مد نظر قرار دهید. این عوامل می‌توانند مواردی از قبیل اعلانات مربوط به نشت داده، چه چیزی نشت داده محسوب می‌شود و چه مجازات‌هایی را در پی دارد، باشند. در ادامه به شش قدم مهم برای کاهش خطرات ناشی از حملات سایبری می‌پردازیم. اقدامات دیگری هم وجود دارند که می‌توانند خطر حملات و خطاها را کاهش دهند، مانند برگزاری دوره‌های منظم آموزشی برای کارمندان داخلی اما این شش گام، قدم‌های بسیار مهم و حیاتی در کاهش خطرات سایبری هستند.

۱ ارتباط سیستم‌های کاری و شخصی را محدود کنید.

به‌دلیل افزایش تعداد کارمندانی که از راه دور کار می‌کنند، انتقال داده‌ها بین دستگاه‌های شخصی و کاری اغلب اجتناب‌ناپذیر شده است و نگهداری اطلاعات حساس در کامپیوترهای شخصی موجب افزایش آسیب‌پذیری در برابر حملات سایبری می‌شود. بنابراین، برای جلوگیری و کاهش این خطرات باید انتقال داده‌ها را تا حد امکان کاهش دهید.

۲ هرگونه دانلودی با آگاهی صورت گیرد.

شرکت‌ها نیازمند مدیریت فعال کلیه نرم‌افزارهای خود (سیستم عامل‌ها و برنامه‌های کاربردی) در شبکه هستند، به‌گونه‌ای که تنها نرم‌افزارهای مجاز نصب شده و قابل اجرا باشند. در این نوع کنترل نرم‌افزارهای غیرمجاز و مدیریت نشده شناسایی شده و از نصب و اجرا آن‌ها جلوگیری می‌شود.

۳ امنیت رمز عبور را بهبود بخشید.

قدرت و میزان پیچیدگی رمز عبور شما، اولین سد میان دسترسی به حساب‌های کاربری و داده‌ها و هکرها است پس همواره سعی کنید رمزهای عبور پیچیده با طول کافی انتخاب کنید. می‌توان این انتخاب را با به کاربردن کاراکترهای خاص (مانند !@#$٪)، نامفهوم‌بودن رمز (عدم استفاده از اعدادی مانند تاریخ تولد و اسامی مانند نام خود، خانواده یا حیوان خانگی)، طول بیش از ۸ کاراکتر، ترکیبی از حروف بزرگ و کوچک و اعداد و کاراکترها و تعویض منظم رمز و افشا نکردن آن به هر صورتی مانند، به اشتراک گذاشتن یا حتی نوشتن آن، انجام دهید.

٤ به‌روزرسانی‌ها را به‌صورت مرتب انجام دهید.

شرکت‌های ارائه‌دهندگان نرم‌افزار و سیستم‌عامل، سخت تلاش می‌کنند تا به‌طور منظم نرم‌افزار و سیستم‌عامل خود را از طریق ارائه بسته‌هایی، به‌روزرسانی کرده و با رفع نقص‌ها و آسیب‌پذیری‌ها، ایمن‌تر کنند. شما با انجام این به‌روزرسانی‌ها و اعمال وصله‌های منتشر شده، می‌توانید آسیب‌پذیری‌های متعدد در بسترهایی که مورد استفاده شما است را کاهش دهید.

۵ نظارت خود بر داده‌ها را افزایش دهید.

به‌طورمنظم بسترها و داده‌های خود را برای یافتن هرگونه نشت اطلاعات تحت‌نظر بگیرید. این کار به شما کمک می‌کند خطر نشت داده‌ها در طولانی مدت را کاهش دهید. ابزارهایی که در این زمینه وجود دارند می‌توانند فعالیت‌های رصد را خودکار و مجتمع کرده و در صورت مشاهده هرگونه فعالیت مشکوک، به شما هشدار دهند.

انتقال داده‌ها را کاهش دهید

با احتیاط دانلود کنید

امنیت رمز عبور خود را ارتقا دهید

نرم‌افزار خود را آپدیت کنید

بر نشت داده‌ها نظارت کنید

برنامه‌ای را برای مسئولیت نشت داده توسعه دهید

٦ سیاست‌ها و برنامه‌های مربوط نشت داده را توسعه دهید.

باید توجه داشت که نشت داده حتی می‌تواند برای منظم‌ترین و محافظه‌کارترین شرکت‌ها هم رخ دهد اما با داشتن سیاست‌ها و برنامه‌هایی در هر سازمانی می‌توان پاسخی مناسب برای حملات واقعی و صدمات احتمالی پس از آن آماده کرد.

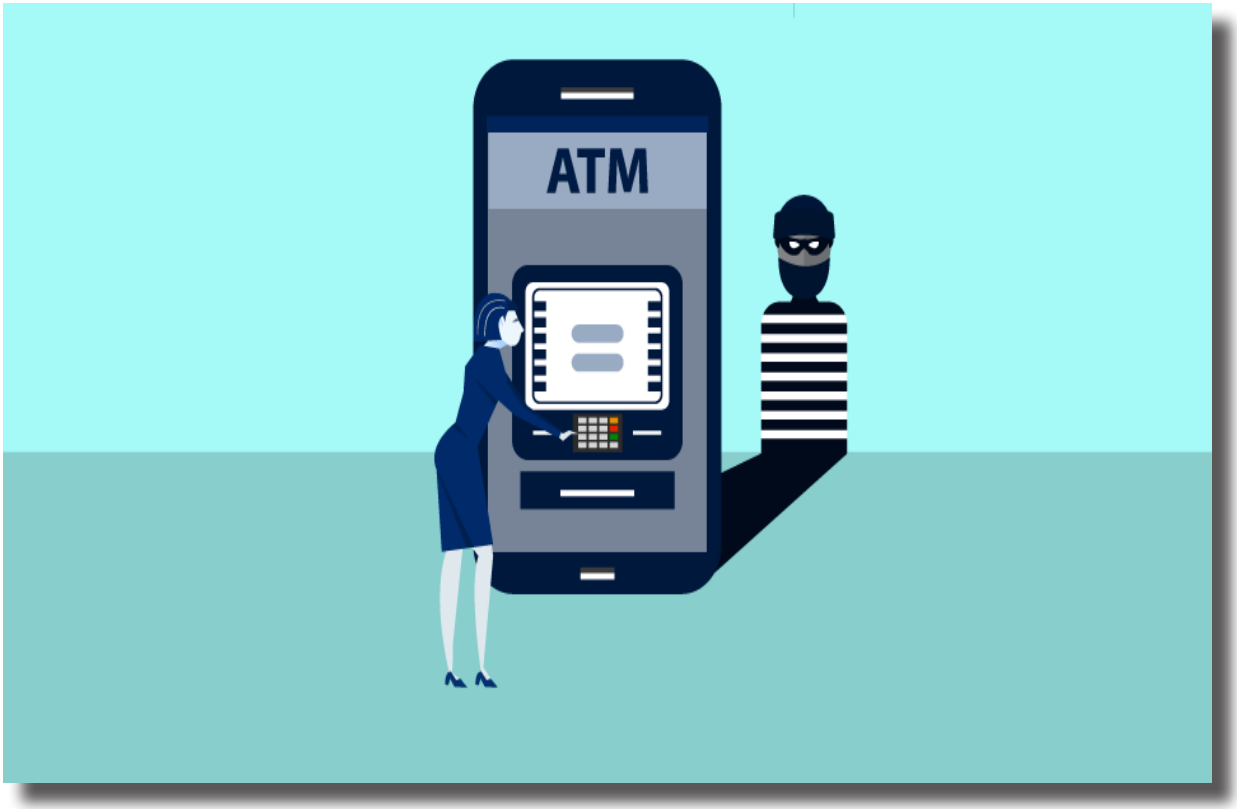
کلام پایانی

واضح است که همه کسب‌وکارهای کوچک و بزرگ در هر لحظه در معرض تهدیدات سایبری هستند پس زمان را از دست ندهید و از همین امروز قدم‌های اولیه را برای جلوگیری از حملات، نشت داده و حوادث احتمالی بعد از آن بردارید. داشتن حفاظت‌های کافی از داده‌ها پایه‌ای‌ترین فعالیت است و البته می‌توانید با داشتن یک سیاست و برنامه در حوزه امنیت سایبری، شرکت خود را از حوادث احتمالی محافظت کنید. اما به یاد داشته باشد، مهم‌ترین نکته در زمینه امنیت سایبری این است که امنیت کامل هیچگاه محقق نمی‌شود پس شما باید همواره برای ارتقای امنیت سازمان و شرکت خود تلاش کنید و هزینه‌های مربوط به این امر را در اولویت قرار دهید.

ژینو سفاحی
zhino.safahi@uok.ac.ir

امنیت اطلاعات

هشدار درخصوص اسکیمرها



مقدمه

در برهه‌ی کنونی خرید با پول نقد خیلی کم و به ندرت انجام می‌شود. اکثر افراد برای خرید از کارت‌های اعتباری استفاده می‌کنند. در کنار مزیت‌هایی که خرید با کارت اعتباری در اختیار مردم قرار می‌دهد، چالش‌هایی را نیز ایجاد می‌کند. یکی از این چالش‌ها مربوط به امنیت استفاده از کارت‌های اعتباری، سرقت اطلاعات و برداشت بخشی یا کل موجودی حساب به‌وسیله اسکیمر (Skimmer) است. اسکیمر دستگاهی است که مشخصات کارت اعتباری یا حساب‌بانکی شخص را کپی می‌کند تا بتواند از حساب‌بانکی او به‌طور غیرقانونی استفاده کند. کلاهبرداران یا مجرمان از اسکیمر تعبیه‌شده در دستگاه عابربانک یا کارت‌خوان برای شبیه‌سازی و کپی‌کردن کارت اعتباری قربانیان استفاده می‌کنند. اسکیمر دستگاهی کوچک به اندازه یک پیجر است که اطلاعات نوارمغناطیسی روی کارت اعتباری را می‌خواند و ذخیره می‌کند.

اسکیمینگ کارت اعتباری چیست؟

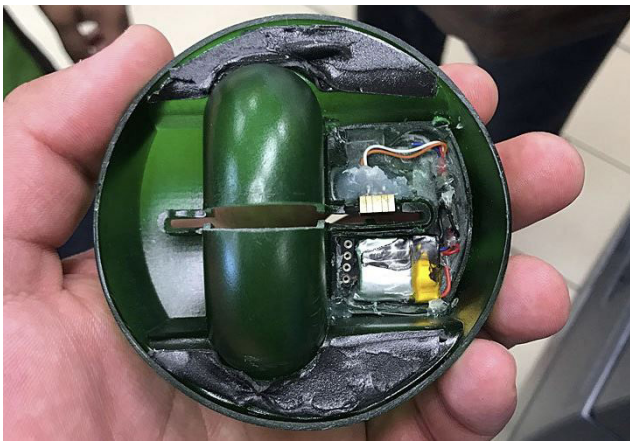
اسکیمینگ کارت اعتباری نوعی کلاهبرداری از کارت اعتباری است که در آن فرد اطلاعات شخصی کارت مانند شماره‌کارت، نام دارنده‌کارت و رمزکارت را با استفاده از یک دستگاه Skimming به سرقت می‌برد. سپس سارق به‌طور غیرقانونی از موجودی حساب پول برداشت می‌کند یا داده‌های به‌دست آمده از آن را می‌فروشد.

اسکیمینگ کارت اعتباری چگونه انجام می‌شود؟

در یک کارت اعتباری، نوارمغناطیسی (نوارسیاه یا magstripe) در طرف مقابل کارت اعتباری، تمام اطلاعات مورد نیاز یک کلاهبردار برای سرقت پول شما را ذخیره می‌کند. نوار شامل نام دارنده کارت، شماره‌کارت، تاریخ انقضا و کد CVV2 است.

اسکیمینگ کارت اعتباری

در قلب یک عملیات اسکیمینگ یک اسکیمر وجود دارد. اسکیمر یک دستگاه اسکن است که بر روی اسکنر کارت در یک دستگاه خودپرداز نصب شده است. اکثر دستگاه‌های خودپرداز در سراسر کشور از یک طرح مشترک استفاده می‌کنند و در نتیجه، بازار سیاه مملوء از دستگاه‌های اسکیمر مشابه با دستگاه‌های قانونی نصب شده در خودپرداز است که مجرمان و کلاهبرداران از آن استفاده می‌کنند. این اسکیمرها به قدری باکیفیت و مشابه نمونه اصلی تولید شده‌اند که مردم اکثراً نمی‌توانند وجود آن‌ها بر روی دستگاه ATM را تشخیص دهند، بنابراین هر زمان در هر تراکنش بانکی، چه آنلاین و چه در دستگاه خودپرداز، افراد به‌صورت پیش‌فرض از نظر امنیتی دارای تشویش و اضطراب هستند که اطلاعات کارت اعتباری و حساب آن‌ها سرقت نشود و مبالغی از حساب آن‌ها به‌صورت غیرقانونی برداشت نشود. تراکنش آنلاین به یک گذرواژه یکبار مصرف برای اجرا نیاز دارد، این مورد در دستگاه‌های خودپرداز صادق نیست. هرکسی که شماره‌کارت و رمزکارت شما را داشته باشد می‌تواند از حساب شما پول برداشت کند و شما را بسیار بیشتر از قبل متضرر و مضطرب کند. اما سوال اصلی این است که چگونه یک فرد ناشناس اطلاعات کارت اعتباری شما را به‌دست می‌آورد؟ برای این مورد، راه‌های متعددی وجود دارد که اسکیمینگ کارت اعتباری رایج‌ترین روش است.



که شخصی کارت خود را در دستگاه خودپرداز وارد می‌کند، ندانسته آن را از اسکیمر عبور می‌دهد.
اسکیمر قادر به خواندن نوارمغناطیسی بر روی کارت‌های‌اعتباری و ذخیره اطلاعات رمزگذاری شده در آن‌ها است. برخی از اسکیمرها می‌توانند داده‌های صدها کارت را ذخیره‌کنند. اطلاعات اسکیمرهای اصلی باید به‌صورت دستی و بدون تجهیزات استخراج شوند و خطر گرفتارشدن در این فرآیند را افزایش می‌دهد. بااین‌حال، برخی از اسکیمرهای پیشرفته از راه دور قابل دسترس هستند و قادر به انتقال داده‌ها به‌صورت بی‌سیم می‌باشند.

اسکیمر دستگاه‌های POS

دستگاه‌های کارت‌خوان (POS) یا خودپرداز انجام تراکنش‌های بانکی را برای مشتریان بانکی در هر ساعت از شبانه روز بدون اینکه به ساعات کاری دفتر بانک وابسته باشند بسیار آسان می‌کند. در یک فروشگاه مواد غذایی، پمپ بنزین یا مطب پزشک، پایانه‌های POS به‌عنوان یک دستگاه مناسب تلقی می‌شوند و راه‌حل پرداخت قابل اعتماد و سریع بوده و به‌طور گسترده‌ای توسط عموم مردم مورداستفاده است. برای استفاده از این دستگاه‌ها مشتریان فقط باید از کارت استفاده کنند و شماره رمزکارت را بر روی دستگاه وارد کنند و تراکنش‌های غیر نقدی انجام دهند و پول برداشت کنند. با این حال، استفاده از دستگاه‌های کارت‌خوان دارای چالش‌های متعدد امنیتی است. یکی از این چالش‌ها، کلاهبرداری و کپی کارت توسط اسکیمر است. در این روش اطلاعات کارت مشتری با استفاده از اسکیمر نصب شده در جایگاه قرارگیری کارت دستگاه کپی می‌شود. اسکیمر برای سرقت اطلاعات مشتری از جمله شماره حساب، مبالغ موجودی و شماره رمزکارت ذخیره شده روی نوار مغناطیسی الکترونیکی (در پشت کارت) استفاده می‌شود. کلاهبردار با استفاده از اطلاعات ثبت شده، کارت مشتری را کپی‌کرده و قادر است حساب را خالی کند.

دوربین مخفی کوچک یا یک صفحه‌کلید تقلبی

اطلاعات کارت اعتباری بدون رمزکارت دارای ارزش زیادی نیست. برای به‌دست آوردن رمزکارت روش‌های مختلفی وجود دارد که به‌عنوان‌مثال با استفاده از یک دوربین کوچک یا یک صفحه‌کلید تقلبی می‌توان رمز را به‌دست آورد. سارقان معمولاً یک دوربین را در مکان‌هایی مخفی که تشخیص و شناسایی آن با چشم غیر مسلح سخت است نصب می‌کنند تا رمزکارت را ثبت کنند. برخی حتی تا آنجا پیش می‌روند که برای ثبت اعداد وارد شده توسط کاربر، از یک روکش تقلبی صفحه‌کلید ATM که برای کاربر قابل تشخیص نیستند، استفاده می‌کنند. همچنین در دستگاه‌های کارت‌خوان؛ یک جایگاه جاگذاری کارت حجیم یا عریض‌تر از حد معمول نشان می‌دهد که ممکن است یک دستگاه اسکیمر در جایگاه جاگذاری کارت قرار داشته باشد.

در چند سال اخیر اسکیمینگ در فروشنده‌های دوره‌گرد و در خرده‌فروشی‌ها در حال گسترش است و روش کار آن‌ها بر فرض مثال این‌گونه است که بعد از عبور کارت از دستگاه، اطلاعات کارت را ذخیره می‌کنند و اگر حتی رمز کارت شما را ندانند، طبق روش رایجی که اغلب فروشندگان استفاده می‌کنند رمز را از مشتری سوال کرده و برای خود ثبت می‌کنند و می‌توانند به کارت شما دسترسی داشته باشند.

هنگامی که یک کلاهبردار تمام اطلاعات مربوط به کارت اعتباری را دارد، ممکن است اقدام به ساخت یک کارت اعتباری تقلبی رمزگذاری شده با استفاده از اطلاعات سرقت‌شده کند و سپس از آن پول برداشت کند!

چگونه از اسکیم کارت اعتباری جلوگیری کنیم؟

خوشبختانه شما می‌توانید تشخیص دهید که آیا یک دستگاه خودپرداز با اسکیمر دستکاری شده است یا خیر.

قدم اول

قبل از قراردادن کارت خود در اسکنر کارت، اسکنر را کمی تکان دهید. اسکنرهای کارت معتبر قوی هستند و در دستگاه به خوبی ایمن شده‌اند، بنابراین تکان جزئی نباید بر روی آن‌ها تأثیر بگذارد، اما ممکن است در هنگام تکان‌دادن اسکیمرها شل و سست شوند. اگر به نظر می‌رسد که جایگاه جا انداختن کارت ضعیف و لرزان است، می‌توانید از دستگاه خودپرداز استفاده نکنید.

قدم دوم

قبل از واردکردن رمزکارت، به‌دنبال دوربین‌های مخفی اطراف دستگاه بگردید. متداول‌ترین قسمت‌هایی که شخصی در آن دوربین مخفی نصب می‌کند عبارت است از بالای صفحه‌کلید، بالای دستگاه خودپرداز و نواحی نزدیک به صفحه. همچنین، اگر صفحه‌کلید شل و سست به‌نظر می‌رسد یا کلیدها ضعیف و لرزان هستند، از دستگاه استفاده نکنید.

قدم سوم

سعی کنید که در هیچ شرایطی رمز کارت خود را در اختیار شخص دیگری قرار ندهید، پیشنهاد ما برای ایمن نگه‌داشتن و جلوگیری از اسکیمینگ این است که سعی کنید خودتان کارت اعتباری‌تان را از جایگاه کارت دستگاه بکشید و اگر در شرایط ضروری قرار داشتید و این امکان وجود نداشت حتماً خودتان رمز کارت را وارد کنید.

رایج‌ترین دستگاه‌های خودپرداز مستعد دستکاری، آن‌هایی هستند که در پمپ بنزین‌ها یا آن‌هایی که دور از مناطق شلوغ هستند و ازاین‌رو توسط مسئولان، نظارت و مراقبت جدی ندارند. از استفاده از چنین دستگاه‌های خودپردازی خودداری کنید مگر اینکه کاملاً ضروری باشد. همچنین، در صورت امکان، چند دقیقه اضافی وقت بگذارید و به‌جای استفاده از این نوع دستگاه‌ها، از کارت‌خوان‌های روی میز صندوق‌دار پول پرداخت کنید، زیرا احتمال آن که به اسکیمر مجهز شوند کمتر است. اگر کارت اعتباری‌تان مشکوک اسکیم شدن بود بلافاصله کارت خود را از طریق بانک صادرکننده بسوزانید و یا حسابتان را مسدود کنید.

کلام پایانی

خوشبختانه، شرکت‌های بانکی شروع به نصب اقدامات امنیتی بیشتری برای جلوگیری از دستکاری کارت اعتباری کرده‌اند. جایگاه جا انداختن کارت ساده و قدیمی با طرح‌های دقیق‌تر و پیچیده‌تر تعویض شده‌اند و قراردادن اسکیمرها بر روی آن‌ها را برای کلاهبرداران سخت‌تر می‌کند. از نوار و برچسب‌های امنیتی در دستگاه‌های خودپرداز استفاده می‌کنند برای تشخیص اینکه آیا توسط شخصی این دستگاه‌ها دستکاری شده‌است یا خیر! بیشتر کارت‌ها از تراشه‌های EMV (تراشه‌های مربعی کوچک رایانه‌ای در جلوی کارت شما) استفاده می‌کنند، که نسبت به نوارمغناطیسی مقاوم‌تر هستند. داده‌های ذخیره شده در یک تراشه EMV برای هر تراکنش منحصر به فرد است و به ایمن‌تر شدن کارت در برابر تقلب و کلاه‌برداری کمک می‌کند. به‌طور کلی فرایند اسکیمینگ فقط مختص کارت اعتباری نیست! اسکیمینگ بر روی هر نوع کارتی می‌تواند اجرا شده و امنیت افراد را به خطر بیاندازد و در این زمینه آموزش بهترین کارکرد را دارد که هدف اصلی نوشتار این مطلب بوده است.

مرکز آپا دانشگاه کردستان

cert.uok.ac.ir