بررسی روش‌های مقابله با حملات باج‌افزاری در چارچوب پیش‌گیری از جرایم سایبری

پوهنمل عصمت الله ناشر
نویسنده *
تکنالوژی معلوماتی، پوهنحی کمپیوترساینس، پوهنتون بدخشان
نشانی برقی nashirasmatullah@gmail.com
نشانی ارکاید https://orcid.org/0009-0004-9976-4461

پوهنمل محمد الله شیرپور
نویسنده
تکنالوژی معلوماتی، پوهنحی کمپیوترساینس، پوهنتون بدخشان
نشانی برقی shirpor528@gmail.com
نشانی ارکاید https://orcid.org/0009-0001-2115-1217

چکیده

باج‌افزار یکی از خانواده‌ی بدافزارها است که با استفاده از روش‌های امنیتی مانند رمزنگاری، فایل‌ها و منابع کاربر را گروگان گرفته و در عوض بازگرداندن دسترسی به اطلاعات قفل‌شده، درخواست ارز دیجیتال یا پول می‌کند. هیچ محدودیتی برای قربانیان این نوع حمله وجود ندارد، چرا که باج‌افزار می‌تواند از طریق انترنت منتقل شود. هدف این تحقیق بررسی روش‌های مقابله با حملات باج‌افزاری از طریق روش کتاب خانه‌ی مطالعات علمی منتشرشده در بخش امنیت سایبری می‌باشد. یافته‌ها نشان داد که آموزش مستمر استفاده کننده‌ها، استفاده از الگوریتم‌های رمزنگاری قوی، تطبیق روش‌های چندلایه‌یی امنیتی، پشتیبان‌گیری منظم و بهره‌گیری از پلتفورم‌های تشخیص نفوذ مبتنی بر هوش مصنوعی از مهم‌ترین و مؤثرترین راه‌کارها برای کاهش تأثیر حملات باج‌افزاری هستند.

کلید واژه‌ها: امنیت سایبری، باج‌افزار، جرایم سایبری، حملات سایبری، رمزنگاری

* **نویسنده مسئول:** nashirasmatullah@gmail.com

A Study on Countermeasures against ransomware Attacks within the Framework of Cybercrime Prevention

Asmatullah Nashir
Author * Information Technology Computer Science Faculty, Badakhshan
Email University, Badakhshan, Afghanistan
Orcid Email:nashirasmatullah@gmail.com
https://orcid.org/0009-0004-9976-4461

Mohammadullah Shirpoor
Author Information Technology Computer Science Faculty, Badakhshan
Email University, Badakhshan, Afghanistan
Orcid shirpor528@gmail.com
https://orcid.org/0009-0001-2115-1217

Abstract
Ransomware is a category of malicious software that encrypts users' files and system resources, thereby restricting access to data and demanding a ransom, typically in the form of digital currency, in exchange for data recovery. This type of attack can target any individual or organization, as ransomware can be widely distributed through the internet. The aim of this study is to examine effective methods for mitigating ransomware attacks through a library-based review of published scientific research in the field of cybersecurity. The findings indicate that continuous user awareness and training, the use of strong encryption algorithms, the implementation of multi-layered security mechanisms, regular data backup practices, and the adoption of artificial intelligence–based intrusion detection platforms are among the most significant and effective strategies for reducing the impact of ransomware attacks.

Keywords: Cybercrime, Cybersecurity, Cyberattack, Encryption Ransomware ,

Pamir Academic & Research Journal - مجله‌ی علمی-تحقیقی پامیر / - دپامیر علمی څېړنیزه مجله

* Corresponding Author: nashirasmatullah@gmail.com

مقدمه

در سال‌های اخیر، حملات باج‌افزاری به یکی از جدی‌ترین تهدیدات سایبری برای کاربران و سازمان‌ها تبدیل شده است. این نوع بدافزار با استفاده از روش‌های امنیتی مانند رمزنگاری، فایل‌ها و منابع دیجیتال قربانی را گروگان گرفته و در ازای بازگرداندن دسترسی، درخواست ارز دیجیتال یا وجه نقد می‌کند. ویژگی خطرناک باج‌افزارها این است که می‌توانند به سرعت و بدون محدودیت از طریق اینترنت منتشر شده، افراد و سازمان‌ها را هدف قرار دهند. نمونه‌هایی حملات گسترده WannaCryو Petya نشان داده‌اند که این تهدیدها قادر به ایجاد خسارات مالی گسترده و اختلال در خدمات یا سرویس‌های دیجتالی‌هستند.

تحقیقات اخیر نشان می‌دهد که مقابله با باج‌افزار تنها با ابزارهای امنیتی سنتی کافی نیست. روش‌های مؤثر شامل آموزش مستمر کاربران، استفاده از الگوریتم‌های رمزنگاری قوی، پیاده‌سازی پالیسی امنیتی چندلایه، پشتیبان‌گیری منظم و بهره‌گیری از پلتفورم های تشخیص نفوذ مبتنی بر هوش مصنوعی هستند. علاوه بر این، به‌کارگیری مدل‌های امنیتی نوین مانند مدل اعتماد صفر و کنترل‌های دقیق دسترسی می‌تواند میزان تأثیر مقابله با این تهدیدات را افزایش دهد.

تحقیق نشان داده است که آموزش کاربران و به‌روزرسانی مستمر سیستم‌ها، همراه با پشتیبان‌گیری منظم و استفاده از ابزارهای امنیتی پیشرفته، می‌تواند اثرات حملات باج‌افزاری را به میزان قابل توجهی کاهش دهد. هم‌چنین بررسی‌ها نشان می‌دهد که مجرمان سایبری همواره با بهره‌گیری از آسیب‌پذیری‌های جدید و روش‌های نوین، قابلیت انتشار و تخریب باج‌افزارها را افزایش می‌دهند، که ضرورت توسعه‌ی راه‌کارهای پیش‌گیرانه و مقاوم‌تر را بیش از پیش آشکار می‌سازد.

هدف این تحقیق فراهم کردن راه‌کارهای است که علاوه بر کاهش خسارات، توانمندی کاربران و سازمان‌ها در مواجه با این تهدیدات را ارتقا دهد و بستر امن‌تری برای فعالیت‌های دیجیتال فراهم نماید.

تبیین مسأله

باج‌افزار نوعی حمله باج‌خواهانه و کُد مخرب یا نرم‌افزار مخرب است که سیستم را آلوده کرده و دسترسی کاربر به فایل‌ها، پوشه‌ها یا حتی کل سیستم را محدود یا غیرممکن می‌سازد تا زمانی که مبلغی به‌عنوان باج پرداخت شود. این نوع حملات معمولاً با رمزنگاری فایل‌های کاربر و قفل‌کردن دسکتاپ شخص قربانی آن‌جام می‌شود. در برخی موارد، باج‌افزار منابع دیجیتالی را قفل‌کرده و سپس برای‌آزادسازی آن‌ها درخواست پول می‌کند. یکی از مهم‌ترین و مخرب‌ترین مصادیق این تهدیدات، حملات باج‌افزاری است که از طریق رمزنگاری داده‌های کاربران و مطالبه باج،

دسترسی به اطلاعات را محدود ساخته و خسارات گسترده، جدی و گاه جبران‌ناپذیر مالی و امنیتی به افراد و سازمان‌ها وارد می‌کند.

نمونه‌هایی مانند حملات گسترده WannaCry و Petya نشان دهنده‌ی قدرت تخریب بالا و قابلیت انتشار سریع این نوع بدافزارها هستند. با وجود پیشرفت در ابزارهای امنیتی، مجرمان سایبری همواره با بهره‌گیری از آسیب‌پذیری‌های جدید، روش‌های خود را به‌روزرسانی می‌کند و مسیرهای تازه‌ای برای نفوذ پیدا می‌نمایند. افزایش مفاد مالی این حملات و رشد صنعت باج‌افزار به میلیاردها دالر، انگیزه‌ی مجرمان برای ادامه این نوع حملات را تقویت کرده است. از این‌رو، شناخت عمیق سازوکار حملات باج‌افزاری و شناسایی روش‌های مؤثر برای پیش‌گیری و کاهش آثار آن‌ها، به ضرورت اجتناب ناپذیر در حوزه‌ی امنیت سایبری تبدیل شده است. این تحقیق با مطالعه دقیق منابع علمی، مهم‌ترین راه‌کارهای پیش‌گیرانه و واکنشی در برابر باج‌افزارها را استخراج و تحلیل نماید تا از این طریق، بستر امن‌تری برای کاربران و سازمان‌ها فراهم گردد.

پرسش‌های تحقیق

پرسش اصلی: کدام نوع روش‌ها و تکنیک‌هایی برای شناسایی و پیش‌گیری از حملات باج‌افزاری مؤثرتر هستند؟

پرسش‌های فرعی

۱. باج‌افزارها چگونه سیستم‌ها و داده‌های سازمانی را هدف قرار می‌دهند و چه روش‌هایی برای نفوذ به سیستم‌ها به کار می‌برند؟

۲. چگونه می‌توان پس از وقوع حمله باج‌افزاری سیستم‌ها را بازیابی و خسارات ناشی از آن را کاهش داد؟

اهمیت تحقیق

در عصر تحول دیجیتال، اطلاعات و منابع دیجیتال حیاتی‌ترین دارایی‌های هر سازمان، نهادهای دولتی و حتی افراد به‌شمار می‌آیند. باج‌افزار به‌عنوان یکی از خطرناک‌ترین انواع بدافزارها، با بهره‌گیری از تکنیک‌های رمزنگاری، این دارایی‌ها را هدف قرار داده و در ازای بازگرداندن دسترسی، درخواست پرداخت ارز دیجیتال می‌کند. گستردگی و سهولت انتشار این تهدید از طریق اینترنت و ابزارهایی چون مهندسی اجتماعی، تبلیغات آلوده، ایمیل‌های فیشینگ و بهره برداری از آسیب‌پذیری‌های سیستم، موجب شده که هر کاربر یا سازمانی در معرض آن قرار گیرد.

آن‌چه این تهدید را متمایز و نگران‌کننده می‌سازد، تأثیرات جبران ناپذیر آن حتی پس از حذف نرم افزار مخرب است. برخلاف بدافزارهای سنتی، بازگشت کامل داده‌ها بدون کمک سازنده

مجله‌ی علمی-تحقیقی پامیر / - Pamir Academic & Research Journal - دپامیر علمی څېړنیزه مجله

باج‌افزار تقریباً غیرممکن است. بر اساس گزارش‌های منتشرشده از طرف "Cybersecurity Ventures"، باج‌افزار سریع‌ترین نوع در حال رشد جرایم سایبری است، به‌طوری‌که میزان خسارت ناشی از آن از ۳۲۵ میلیون دالر در سال ۲۰۱۵ به ۲۰ میلیارد دالر در سال ۲۰۲۱ رسیده است. افزایش چشم‌گیر حملات باج‌افزاری به زیرساخت‌های حیاتی مانند خدمات درمانی، حمل‌ونقل، تولید، مالی و دولتی، نیاز فوری به توسعه‌ی تکنیک‌های پیش‌گیرانه و واکنشی را ایجاد کرده است. ابزارهای هک و باج‌افزارها با قیمتی ناچیز در بازارهای زیرزمینی اینترنت در دسترس قرار دارند که ورود به دنیای جرایم سایبری را برای افراد کم تجربه نیز آسان ساخته است.

از طرف دیگر، مدل جدیدی از باج‌افزار به نام (Ransomware-as-a-Service) باعث گسترش سازمان‌یافته این نوع حملات شده و نشان دهنده‌ی رشد یک اکوسیستم سایبری مجرمانه پیچیده است. رمزنگاری پیشرفته، ارز دیجیتال ناشناس و دسترسی آسان به کدهای باج‌افزار، این تهدید را به یک تجارت پرسود برای مهاجمان تبدیل کرده است.

در نتیجه، تحقیق در زمینه‌ی شناسایی، پیش‌گیری، کاهش خسارات و بازیابی پس از حملات باج‌افزاری نه تنها برای ارتقای امنیت سایبری حیاتی است، بل‌که برای حفاظت از اقتصاد، اطلاعات شخصی و زیرساخت‌های سازمان‌ها نیز مهم می‌باشد. این تحقیق گامی اساسی در جهت تدوین و تقویت راهبردهای مقابله با این تهدید رو به رشد در سطح جهانی به‌شمار می‌رود.

اهداف تحقیق

هدف اصلی: هدف اصلی این تحقیق، بررسی روش‌های مقابله با حملات باج‌افزاری در چارچوب پیش‌گیری از جرایم سایبری می‌باشد.

اهداف فرعی

۱. شناسایی مهم‌ترین روش‌های مقابله با حملات باج‌افزاری در حوزه‌ی امنیت سایبری؛

۲. بررسی نقش آموزش کاربران و راه‌کارهای فنی در پیش‌گیری از حملات باج‌افزاری؛

۳. تحلیل تأثیر راه‌کارهای multiple-layer security، پشتیبان‌گیری و تشخیص نفوذ هوشمند در کاهش خسارات باج‌افزار؛

پیشینه‌ی تحقیق

تحقیقات متعددی برای پیش‌گیری از حملات باج‌افزاری آن‌جام شده‌اند که هرکدام با بهره‌گیری از رویکردهای مختلف، به‌دنبال شناسایی وجود این نوع بدافزار در سیستم‌ها بوده‌اند.

در این تحقیق، با ترکیب روش‌های تحلیل استاتیک و دینامیک، مجموعه‌ای فشرده و نوآورانه از ویژگی‌ها استخراج شده است که توصیف‌کننده الگوهای رفتاری باج‌افزارها می‌باشند. یافته‌ها

نشان می‌دهد که استفاده از تحلیل چندلایه و ترکیبی موجب بهبود دقت و سرعت در شناسایی باج‌افزارهای رمزنگاری شده و می‌تواند مبنایی برای طراحی پلتفورم‌های دفاعی هوشمند در برابر تهدیدات سایبری فراهم سازد (Kashif Shaukat & Ribeiro,2018).

چین در مقاله‌ی خود از پیشنهاد روشی برای شناسایی و رتبه‌بندی ویژگی‌های متمایز باج‌افزارها از طریق تحلیل خودکار لاگ‌های سیستمی بحث نموده است تا فرآیند زمان‌بر تحلیل دستی در مقابله با حملات باج‌افزاری کاهش یابد . (Chen & Bridges, 2017)

داسیر و همکاران ان با معرفی پلتفورم به نام Redemption که با ایجاد مقاومت بیش تر در سطح سیستم‌عامل در برابر حملات باج‌افزاری، قادر است تحقیق نموده است و رفتار مخرب برنامه‌ها را شناسایی و از تخریب داده‌ها جلوگیری می‌کند. این پلتفورم با نظارت بر الگوهای ورودی و خروجی داده‌ها (I/O) و ایجاد یک بافر شفاف برای ذخیره‌سازی موقت اطلاعات، در صورت شناسایی رفتار مشکوک، فرآیند آلوده را متوقف کرده و داده‌های آسیب‌دیده را بازیابی می‌نماید. (Dacier et al, 2017).

هدف این مقاله ارایه‌ی مروری بر پژوهش‌های اخیر در زمینه‌ی پیش‌گیری از حملات باج‌افزاری و معرفی بهترین روش‌ها و راه‌کارهای کاهش تأثیر این نوع حملات است (Alshaikh et al, 2020).

هدف این تحقیق مدل‌سازی حملات چندمرحله‌ای باج‌افزارهای رمزنگاری شده علیه زیرساخت‌های حیاتی و پلتفورم‌های کنترل صنعتی (ICS/SCADA) است. در این پژوهش، با تحلیل ایستای باج افزار WannaCry، روش‌های مورد استفاده برای شناسایی گره‌های آسیب‌پذیر و گسترش در شبکه بررسی شده است (Zimba, Wang, & Chen, 2018).

روش تحقیق

روش تحقیق در این تحقیق از نوع کتاب‌خانه‌ای و توصیفی-تحلیلی استفاده شده است. در این تحقیق، اطلاعات و داده‌های مورد نیاز از طریق بررسی منابع دومی شامل مقالات علمی، کتاب‌ها، کنفرانس‌های تحقیقی در بخش امنیت سایبری و باج‌افزارها جمع‌آوری شده است.

در مرحله‌ی نخست، با استفاده از پایگاه‌های علمی معتبر مانند: IEEE Xplore ، سپرینگر، گوگل سکالر و ساینس دایریکت مقالات مرتبط با کلیدواژه‌هایی هم‌چون باج‌افزار، رمزنگاری، جرایم سایبری، امنیت سایبری و حملات سایبری جستجو گردید.

در مرحله‌ی دوم، منابع جمع‌آوری شده از نظر اعتبار علمی، سال انتشار، و میزان ارتباط با موضوع تحقیق مورد ارزیابی قرارگرفتند و تنها تحقیقات که دارای داده‌های معتبر و قابل استناد بودند، در تحلیل نهایی استفاده شدند. سپس با استفاده از روش تحلیل محتوا، داده‌های

مجله‌ی علمی-تحقیقی پامیر / - دپامیر علمی څېړنیزه مجله - Pamir Academic & Research Journal

۱۰ فایل، از گسترش آن جلوگیری نماید، ضمن آن‌که فایل‌هایی خارج از پوشه‌ی اسناد کاربر را بررسی نمی‌کند(Scaife et al., 2016).

کانتینلا و همکاران تکنیکی به نام ShieldFSپیشنهاد کردند که هنگام تغییر فایل‌ها، یک نسخه‌ی پشتیبان از آن‌ها در یک ناحیه‌ی محافظت شده ذخیره می‌کند. این روش به فایل اصلی اجازه می‌دهد که تغییرات روی آن اعمال شود، در حالی‌که سیستم تمام تغییرات را ردیابی می‌نماید. سیستم تشخیص ShieldFS بر پایه‌ی تحلیل ترکیبی عواملی مانند آنتروپی عملیات نوشتن، فراوانی عملیات خواندن و نوشتن، فهرست‌سازی پوشه‌ها، درصد فایل‌های تغییرنام‌یافته، و آمار نوع فایل‌ها عمل می‌کند. اگر ShieldFS تشخیص دهد که فرآیند آن‌جام‌شده طبیعی است، نسخه‌ی پشتیبان ذخیره‌شده حذف می‌شود، زیرا فایل اصلی توسط باج‌افزار رمزگذاری نشده است. اما اگر سیستم رفتار مخرب را شناسایی کند، فرآیند مشکوک فوراً متوقف شده و نسخه‌های پشتیبان بازیابی می‌شوند تا جایگزین فایل‌های تغییریافته یا رمزگذاری‌شده گردند. بدین ترتیب، ShieldFSروش کارآمد برای تشخیص و بازیابی فایل‌ها در برابر حملات باج‌افزاری فراهم می‌سازد (Continella et al., 2016).

خاراز و کردا روش به نام Redemption معرفی کردند که برای جلوگیری از آسیب باج‌افزار، تمام عملیات رمزگذاری را به نسخه‌های موقت فایل‌ها هدایت می‌کند و بدین ترتیب فایل‌های اصلی بدون آسیب باقی می‌مانند. این سیستم با استفاده از چارچوب کرنل ویندوز، درخواست‌های نوشتن را به‌صورت شفاف به ناحیه‌ای محافظت‌شده منتقل می‌کند. هرچند Redemption در حفظ امنیت فایل‌ها مؤثر است، اما هنگام کار با تعداد زیاد فایل‌های کوچک، عمل‌کرد آن تا حدود ۷ تا ۹ درصد کاهش می‌یابد (Dacier et al., 2017).

رفتار شبکه‌ای: رفتار شبکه‌ای باج‌افزارها، به خصوصWannaCry، نشان دادند که تقسیم‌بندی شبکه و اولویت‌بندی امنیت دستگاه‌های تولیدی می‌تواند انتشار باج‌افزار را محدود کند و با تحلیل کد منبع، روش‌های شناسایی نقاط آسیب‌پذیر شبکه توسط باج‌افزار را شناسایی کردند (Zimba et al., 2018).

اکبانو و همکاران با تحلیل دینامیک WannaCry نشان دادند که این باج‌افزار شامل دو بخش بوده که یک ان انتشار شبکه‌ای به‌عنوان کرم با اسکن آسیب‌پذیری‌ها و دومی ان رمزگذاری فایل‌ها با استفاده از کلیدهای RSA داخلی. هم‌چنین WannaCry از طریق آدرس‌های Onion و پورت‌های امن Tor با سرورهای C&C ارتباط برقرار می‌کند. این یافته‌ها می‌تواند به طراحی مکانیزم‌های مؤثر مقابله با WannaCry و باج‌افزارهای مشابه کمک کند (Akbanov et al., 2019).

مجله‌ی علمی-تحقیقی پامیر / - دپامیر علمی څېړنیزه مجله - Pamir Academic & Research Journal

روش‌های پیش‌گیری معاصر: راجپوت با بررسی انواع خانواده‌های باج‌افزار و ویژگی‌های آن‌ها نشان داد که بسیاری از باج‌افزارها رفتارها و ویژگی‌های مشابهی دارند، که این امر می‌تواند به بهبود روش‌های شناسایی و پیش‌گیری کمک کند (Singh Rajput, 2017). هول و همکاران با ایجاد مدل Randep ویژگی‌های رفتاری باج‌افزار را بر اساس مراحل اجرای آن‌ها دسته‌بندی کردند و با تحلیل فراخوانی‌های API ویندوز، رفتار احتمالی هر نمونه را پیش‌بینی نمودند. این مدل می‌تواند در شناسایی و مدیریت مؤثر باج‌افزارها کمک کند، هرچند همه‌ی نمونه‌ها تمام مراحل مدل را طی نمی‌کند(Hull et al., 2019).

لی و همکاران با استخراج شاخص‌های نفوذ از طریق Cuckoo Sandbox، نمونه‌های باج‌افزار را با استفاده از یادگیری ماشین نظارت‌شده به ۷ خانواده دسته‌بندی کردند و این روش می‌تواند پایه‌ای برای تحلیل و شناسایی باج‌افزارهای جدید بر اساس رفتار آن‌ها باشد (Lee, 2018).

بازیابی پس از آلودگی: زیمپا با استفاده از مهندسی معکوس و تحلیل دینامیک، ساختارهای حمله و تکنیک‌های حذف داده‌ای که باج‌افزارها به کار می‌برند را بررسی کردند. آن‌ها نتیجه گرفتند که کلید بازیابی داده‌ها به طراحی حمله و روش حذف داده‌های اعمال شده بستگی دارد، صرف نظر از میزان تخریب باج‌افزارهای رمزنگار. با این حال، برخی باج‌افزارها اثرات غیرقابل بازگشت دارند، مانند NotPetya که هیچ راه واقعی برای رمزگشایی هارد دیسک‌های رمزگذاری شده آن وجود ندارد(Zimba, Wang, & Simukonda, 2018).

دام‌گذاری مهاجم: با استفاده از فایل‌های طعمه (کاناری) در لینوکس می‌توان رخ‌دادهای باج‌افزاری را هنگام دسترسی به این فایل‌ها تشخیص داده و اجرای باج‌افزار را متوقف کرد و بدین‌ترتیب بقیه‌ی داده‌ها را مصون نگه داشت؛ این پلتفورم حتی قادر است به‌صورت خودکار اقدامات پاک‌سازی را آغاز کند، اما محدودیت هایی دارد. حفاظت فقط برای بخش‌هایی از سیستم فایل اعمال می‌شود، توزیع ناکافی تله‌ها و حذف فایل کاناری می‌تواند کارایی را کاهش دهد، و در حالت هایی که باج‌افزار فایل‌های یک پوشه را به‌صورت تصادفی رمزگذاری می‌کند ممکن است پیش از متوقف سازی تمام فایل‌ها آسیب ببینند (Gómez-Hernández et al., n.d).

تحقیقات متعددی در زمینه‌ی پیش‌گیری و مقابله با حملات باج‌افزاری آن‌جام شده است که هر کدام با بهره‌گیری از رویکردهای مختلف، به دنبال شناسایی، جلوگیری و کاهش اثرات این تهدیدات بوده‌اند. روش‌های مبتنی بر امضا به شناسایی نمونه‌های شناخته شده با دقت بالا کمک می‌کند، اما در برابر نسخه‌های جدید یا کدهای مبهم محدودیت دارند. در مقابل، رویکردهای مبتنی بر رفتار با بررسی تعامل بدافزار با فایل‌ها و سیستم، امکان شناسایی زودهنگام و جلوگیری از رمزگذاری گسترده داده‌ها را فراهم می‌کند. هم‌چنین تحلیل رفتار شبکه‌ای باج‌افزارها نشان داده

است که با شناسایی مسیرهای انتشار و نقاط آسیب پذیر شبکه می‌توان از گسترش آن‌ها جلوگیری کرد. روش‌های پیش‌گیری معاصر شامل دسته‌بندی ویژگی‌های رفتاری باج‌افزار، کنترل دسترسی، بازیابی پس از آلودگی و دام‌گذاری مهاجم است که به کاهش اثرات حمله و محافظت از داده‌ها کمک می‌کند. مجموع این یافته‌ها نشان می‌دهد که ترکیبی از روش‌های تشخیص امضایی و رفتاری، فناوری‌های نوین مانند یادگیری ماشین، و تطبیق پالیسی‌های امنیتی چندلایه برای مقابله مؤثر با باج‌افزارها ضروری است و می‌تواند آسیب‌های ناشی از این تهدیدات را به حداقل برساند.

نتیجه‌گیری

تحقیقات حاضر نشان می‌دهد که مقابله با حملات باج‌افزاری نیازمند رویکردی چندلایه و جامع است که ترکیبی از روش‌های شناسایی، پیش‌گیری و بازیابی را شامل می‌شود. روش‌های مبتنی بر امضا با دقت بالا قادر به شناسایی نمونه‌های شناخته‌شده باج‌افزار هستند، اما در برابر نسخه‌های جدید یا باج‌افزارهای پیچیده محدودیت دارند. از طرف دیگر، روش‌های مبتنی بر رفتار با تحلیل تعامل باج‌افزار با فایل‌ها، سیستم و شبکه، امکان شناسایی زودهنگام و جلوگیری از رمزگذاری گسترده داده‌ها را فراهم می‌کند. تحلیل رفتار شبکه‌ای باج‌افزارها نیز نشان می‌دهد که شناسایی مسیرهای انتشار و نقاط آسیب‌پذیر شبکه می‌تواند از گسترش آن‌ها جلوگیری کند و به طراحی مکانیزم‌های مؤثر مقابله کمک کند.

روش‌های پیش‌گیری مدرن، از جمله دسته‌بندی ویژگی‌های رفتاری باج‌افزارها، کنترل دسترسی کاربران، بازیابی داده‌ها پس از آلودگی و دام‌گذاری مهاجم، نقش مهمی در کاهش اثرات حملات و محافظت از داده‌ها ایفا می‌کند. استفاده از فناوری‌های نوین مانند یادگیری ماشین، محیط‌های شبیه سازی شده، الگوریتم‌های پیش‌رمزگذاری دو مرحله‌ای و سیستم‌های هشدار دهنده زودهنگام، کارایی روش‌های پیش‌گیرانه و واکنشی را بهبود می‌بخشد.

مجله‌ی علمی-تحقیقی پامیر / - دپامیر علمی څېړنیزه مجله - Pamir Academic & Research Journal

منابع

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *Journal of Telecommunications and Information Technology*, *1*, 113–124. https://doi.org/10.26636/jtit.2019.130218

Alshaikh, H., Ramadan, N., & Hefny, H. A. (2020). Ransomware Prevention and Mitigation Techniques General Terms. In *International Journal of Computer Applications* (Vol. 177, Issue 40).

Chen, Q., & Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. *Proceedings - 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017*, *2017-December*, 454–460. https://doi.org/10.1109/ICMLA.2017.0-119

Continella, A., Guagnelli, A., Zingaro, G., De Pasquale, G., Barenghi, A., Zanero, S., & Maggi, F. (2016). ShieldFS: A self-healing, ransomware-aware file system. *ACM International Conference Proceeding Series*, *5-9-December-2016*, 336–347. https://doi.org/10.1145/2991079.2991110

Dacier, M., Bailey, M., Polychronakis, M., & Antonakakis, M. (Eds.). (2017). *Research in Attacks, Intrusions, and Defenses* (Vol. 10453). Springer International Publishing. https://doi.org/10.1007/978-3-319-66332-6

Gómez Hernández, J. A., García Teodoro, P., Magán Carrión, R., & Rodríguez Gómez, R. (2023). Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges. In *Electronics (Switzerland)* (Vol. 12, Issue 21). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics12214494

Gómez-Hernández, J. A., Alvarez-González, L. ´, & García-Teodoro, P. (n.d.). *R-Locker: Thwarting Ransomware Action through a Honeyfile-based Approach*. https://nesg.ugr.es

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, *8*(1). https://doi.org/10.1186/s40163-019-0097-9

Kashif Shaukat, S., & Ribeiro, V. J. (n.d.). *RansomWall: A Layered Defense System against Cryptographic Ransomware Attacks using Machine Learning*.

Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Prevention of crypto-ransomware using a pre-encryption

detection algorithm. *Computers*, *8*(4). https://doi.org/10.3390/computers8040079

Lee, Dongwon. (2018). *IEEE ISI2018 : IEEE International Conference on Intelligence and Security Informatics : November 8-10, 2018, Florida International University, Miami FL*. IEEE.

Parkinson, S., Crampton, A., & Hill, R. (n.d.). *Computer Communications and Networks Guide to Vulnerability Analysis for Computer Networks and Systems An Artificial Intelligence Approach*. http://www.springer.com/series/4198

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *Proceedings - International Conference on Distributed Computing Systems*, *2016-August*, 303–312. https://doi.org/10.1109/ICDCS.2016.46

Singh Rajput, T. (2017). Evolving Threat Agents: Ransomware and their Variants. In *International Journal of Computer Applications* (Vol. 164, Issue 7).

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, *4*(1), 14–18. https://doi.org/10.1016/j.icte.2017.12.007

Zimba, A., Wang, Z., & Simukonda, L. (2018). Towards Data Resilience: The Analytical Case of Crypto Ransomware Data Recovery Techniques. *International Journal of Information Technology and Computer Science*, *10*(1), 40–51. https://doi.org/10.5815/ijitcs.2018.01.05