Information Technology Innovations and Applied Communication
Vol. 3, No. 4, Winter, 2026, Serial No. 8,pp.39-51

Improving situational awareness in detecting cyber attacks aimed at cyber espionage with evidence-based statistics based on the process of maitre attacks

Ali Khajeh Hasani[1]; Hamid Akbari[2]*

* Assistant Professor, Imam Hossein University, Tehran, Iran.

(**Received:** 14 November 2025, **Revised:** 20 December 2025, **Accepted:** 06 January 2026, **Published:** 21 January 2026)

Abstrac

In today's digital information age, cyber espionage attacks cause great damage to the privacy of organizations and individuals. Therefore, it is essential to provide an effective and appropriate solution for detecting such attacks and identifying attackers. The aim of this research is to improve situational awareness in detecting cyber espionage attacks by collecting evidence based on the Maitre attack process. In this research, the Endesley situational awareness model and the Maitre matrix have been used as a comprehensive guide in the areas of situational awareness and detecting cyber attacks. The most important steps of this research are: designing the cyber espionage process, extracting attacker steps from the Maitre matrix, collecting attack actions and evidence, and validating attack detection methods with the opinions of experts in the field of cyber defense. This research not only helps organizations and individuals to become familiar with existing threats, but also allows them to design and implement appropriate security programs and measures to detect cyber espionage attacks. Given the importance and prevalence of cyber espionage attacks, this research can be used as a practical and comprehensive guide for organizations and individuals interested in detecting and preventing cyber espionage attacks. The results of this method, which is a combination of 14 steps, 37 attacker actions, 190 clues and evidence, and 36 suggested solutions, can be effective and useful in detecting cyber attacks with the aim of espionage and information theft. In this method, Cronbach's alpha, which is the most common statistical method, has been used to examine the internal consistency (reliability) of surveys. In the Cronbach's alpha study, the average of all survey questions is 0.982, which indicates that the reliability of the surveys is within an acceptable range.

Keywords: Situation awareness, Cyber espionage, Cyber attacker, Andesley model, Attack detection, Maitre matrix

* Corresponding Author: E-mail: g9920134713@ihu.ac.ir

«نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال سوم، شماره 4، فصل زمستان، 1404؛ ص 51-39.

مروری - ترویجی

بهبود آگاهی وضعیتی در تشخیص حملات سایبری باهدف جاسوسی سایبری با احصای قرائن و شواهد مبتنی بر فرایند حملات مایتره

علی خواجه حسنی*[1]، حمید اکبری[2]

۱- دانشجو کارشناسی‌ارشد، ۲- استادیار،دانشگاه جامع امام حسین ع، تهران ایران

(**دریافت**: 23 آبان 1404؛ **بازنگری**: 29 آذر 1404؛ **پذیرش**: 16 دی 1404؛ **انتشار**: 11 بهمن 1404)

چکیده

امروزه در عصر اطلاعات دیجیتالی بر اثر حملات جاسوسی سایبری، به حریم خصوصی سازمان‌ها و اشخاص آسیب زیادی واردشده است؛ بنابراین، ارائه راهکارهای مؤثر و مناسب برای تشخیص این‌گونه حملات و شناسایی مهاجمان امری ضروری است. هدف این پژوهش، بهبود آگاهی وضعیتی در تشخیص حملات جاسوسی سایبری با احصای قرائن و شواهد مبتنی بر فرایند حملات مایتره است. در این پژوهش، از مدل آگاهی وضعیتی اندلسی و ماتریس مایتره، به‌عنوان یک راهنمای جامع در حوزه‌های آگاهی وضعیتی و تشخیص حملات سایبری استفاده‌شده است. اهم اقدامات این پژوهش عبارت‌اند از: طراحی فرایند جاسوسی سایبری، استخراج گام‌های مهاجمین از ماتریس مایتره، احصاء اقدامات و قرائن و شواهد حمله و اعتبارسنجی روش‌های تشخیص حمله با نظر خبرگان حوزه پدافند سایبری.

این پژوهش نه‌تنها به سازمان‌ها و افراد کمک می‌کند تا با تهدیدات موجود آشنا شوند، بلکه به آن‌ها امکان می‌دهد تا برنامه‌ها و اقدامات امنیتی مناسبی را برای تشخیص حملات جاسوسی سایبری طراحی و پیاده‌سازی کنند. باتوجه‌به اهمیت و شیوع حملات جاسوسی سایبری، این تحقیق می‌تواند به‌عنوان یک راهنمای عملی و جامع برای سازمان‌ها و افراد علاقه‌مند به تشخیص و پیشگیری از حملات جاسوسی سایبری، مورداستفاده قرار گیرد.

نتایج حاصل از این روش که تلفیقی از ۱۴ گام، ۳۷ اقدام مهاجم، ۱۹۰ قرائن و شواهد، ۳۶ راهکار پیشنهادی است می‌تواند در تشخیص حملات سایبری باهدف جاسوسی و سرقت اطلاعات مؤثر و مفید باشد. در این روش برای بررسی سازگاری داخلی (پایایی) نظرسنجی‌ها، از آلفای کرونباخ که رایج‌ترین روش آماری است، استفاده‌شده است. در بررسی آلفای کرونباخ، میانگین تمام سؤالات نظرسنجی برابر ۰.۹۸۲ شده که نشان‌دهنده پایایی نظرسنجی‌ها در محدوده قابل‌قبولی است.

کلیدواژه‌ها: آگاهی وضعیتی، جاسوسی سایبری، مهاجم سایبری، مدل اندلسی، تشخیص حمله، ماتریس مایتره

* رایانامه نویسنده مسئول E-mail: g9920134713@ihu.ac.ir

۱. مقدمه

در دنیای دیجیتالی امروزی که فناوری اطلاعات و ارتباطات در تمامی شئون زندگی بشر حضور مستمر دارد، مسئله امنیت اطلاعات یکی از چالش‌های اساسی است. در عصر فناوری اطلاعات و ارتباطات، تهدیدات سایبری به امنیت سازمان‌ها و ساختارهای مختلف حمله می‌کنند. این تهدیدات می‌توانند شامل جاسوسی سایبری باشند که به‌منظور دسترسی غیرمجاز به اطلاعات حساس و محرمانه انجام می‌شود. برای تشخیص این تهدیدات، استفاده از روش‌های پیشرفته مبتنی بر رفتار است. حملات سایبری به‌عنوان یکی از چالش‌های مهمی است که خطرهای جدی برای امنیت داده‌ها، سیستم‌ها و شبکه‌های رایانه‌ای در سطح سازمان و کشور ایجاد می‌کند؛ لذا حملات پیشرفته سایبری باهدف جاسوسی، خطرهای جدی را برای اقتصاد و امنیت ملی کشورها پدید می‌آورند. متأسفانه اغلب مهاجمین و بدافزارهای رایانه‌ای یک‌قدم از سیستم‌های امنیتی جلوتر هستند. ازاین‌رو باید به‌جای انتظار برای مواجهه با تهدیدات و هجمه‌های احتمالی، یعنی همان روش‌های پیشین دفاع سایبری، به دنبال راه‌حلی قوی‌تر و هوشمندانه‌تر برای ازمیان‌بردن آن خطر احتمالی باشیم. اینجاست که نظریه «دفاع سایبری فعال» که بخش اساسی آن آگاهی وضعیتی سایبری است مطرح می‌شود. در سال‌های اخیر متخصصان و پژوهشگران همواره به دنبال یک مدل آگاهی وضعیتی فعال، مؤثر و هوشمند برای دستیابی به دفاع مطلوب در مقابل حملات پیچیده امروزی بوده‌اند. با ظهور دفاع سایبری فعال و اثبات اثربخشی و بازدارندگی بالای آن در بهبود دفاع سایبری، دستیابی به یک مدل مطلوب آگاهی وضعیتی بر مبنای مفاهیم و رویکردهای این نوع دفاع، از اصلی‌ترین موضوعات تحقیقاتی در این مسئله است. در این مقاله با ارائه یک مدل پیشنهادی گسترده و جامع آگاهی وضعیتی سایبری به همراه زیر بخش‌های آن بر مبنای راهبردها و فن‌های دفاع سایبری فعال در مقایسه با سایر مدل‌ها، تغییر اساسی در بهبود دفاع سایبری خصوصاً در زیرساخت‌های حیاتی و حساس ایجاد خواهد شد.

دراین‌خصوص یکی از راهکارهای مفید برای بهبود آگاهی وضعیتی در شناسایی و تشخیص حملات جاسوسی سایبری، تلفیق دو مدل مهم آگاهی وضعیتی اندلسی[1] و ماتریس مایتره[2] است. مدل آگاهی وضعیتی اندلسی با تحلیل داده‌های جمع‌آوری‌شده، به تشخیص حملات سایبری و شناسایی رفتارهای غیرمعمول کمک می‌کند. دومین مدل که در اینجا مورد بحث قرار می‌گیرد، ماتریس مایتره است. ماتریس مایتره یک ابزار تصمیم‌گیری است که برای تحلیل و ارزیابی ریسک‌ها و تهدیدات امنیتی استفاده می‌شود. این مدل بر اساس دو پارامتر اصلی، یعنی احتمال و تأثیر، میزان ریسک را برای هر تهدید یا حمله مشخص می‌کند. با استفاده از این ابزار، می‌توان تهدیدات را در یک مقیاس قابل‌اندازه‌گیری قرار داده و اولویت‌بندی کرد.

تلفیق مدل آگاهی وضعیتی اندلسی و ماتریس مایتری در تشخیص حملات سایبری باهدف جاسوسی سایبری، به ما امکان می‌دهد تا بهبود چشمگیری در آگاهی وضعیتی حاکم بر سیستم‌ها و شبکه‌ها داشته باشیم. با تلفیق این دو مدل، می‌توانیم تهدیدات جاسوسی سایبری را شناسایی کرده و تأثیر آن‌ها را در سطح سیستم‌ها ارزیابی کنیم. این رویکرد به ما امکان می‌دهد تا با تمرکز بیشتر منابع و زمان خود به طور هوشمندانه در نقاط ضعف امنیتی، بتوانیم پاسخگویی سریع‌تری برای مقابله با حملات جاسوسی سایبری داشته باشیم. در ادامه بحث دو مفهوم مدل اندلسی و ماتریس مایتره را شرح داده می‌شوند.

شناختی و سازوکارهایی را که افراد برای ارزیابی شرایط برای توسعه آگاهی وضعیتی به‌کارگیری می‌کنند و همچنین کار و عوامل محیطی که بر توانایی آن‌ها برای دریافت آگاهی وضعیتی تأثیر می‌گذارد را توصیف می‌کند [۱]. ماتریس مایتره ابزاری برای تحلیل و ارزیابی ریسک‌ها و تهدیدات امنیتی است. این مدل بر اساس دو پارامتر اصلی احتمال و میزان تأثیر، مقدار ریسک را برای هر تهدید یا حمله مشخص می‌کند.

هدف مقاله این است که با ترکیب دو مدل آگاهی وضعیتی اندلسی و ماتریس مایتره یک روش مؤثر برای تشخیص حملات جاسوسی سایبری بر اساس آگاهی وضعیتی حاکم بر سیستم‌ها و شبکه‌ها ارائه دهد.

ساختار مابقی مقاله بدین شرح است که در بخش دوم روش تحقیق و راهکار مؤثر برای بهبود آگاهی وضعیتی معرفی‌شده است. در بخش سوم پیشینه و سوابق موضوع بیان‌شده است. در بخش چهارم روش پیشنهادی و نتایج آن شرح داده شده است. در بخش پنجم ارزیابی روش پیشنهادی ارائه‌شده و درنهایت در بخش ششم نتیجه‌گیری آمده است.

۲. روش تحقیق

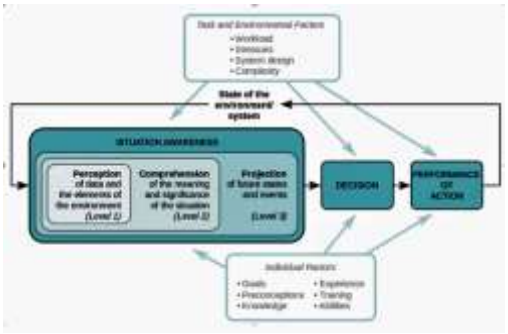
یکی از راهکارهای مؤثر برای بهبود آگاهی وضعیتی در تشخیص حملات سایبری باهدف جاسوسی سایبری، تلفیق دو مدل مهم است. اولین مدل، مدل آگاهی وضعیتی اندلسی است که این مدل با تحلیل داده‌های جمع‌آوری‌شده، به تشخیص حملات سایبری و شناسایی رفتارهای غیرمعمول کمک می‌کند. دومین مدل که در اینجا مورد بحث قرار می‌گیرد، ماتریس مایتره است. ماتریس مایتره یک ابزار تصمیم‌گیری است که برای تحلیل و ارزیابی ریسک‌ها و تهدیدات امنیتی استفاده می‌شود. این مدل بر اساس دو پارامتر اصلی، یعنی احتمال و تأثیر، میزان ریسک را برای هر تهدید یا حمله مشخص می‌کند. با استفاده از این ابزار، می‌توان تهدیدات را در یک مقیاس قابل‌اندازه‌گیری قرار داده و اولویت‌بندی کرد.

تلفیق مدل آگاهی وضعیتی اندلسی و ماتریس مایتری در تشخیص حملات سایبری باهدف جاسوسی سایبری، به ما امکان می‌دهد تا بهبود چشمگیری در آگاهی وضعیتی حاکم بر سیستم‌ها و شبکه‌ها داشته باشیم. با تلفیق این دو مدل، می‌توانیم تهدیدات جاسوسی سایبری را شناسایی کرده و تأثیر آن‌ها را در سطح سیستم‌ها ارزیابی کنیم. این رویکرد به ما امکان می‌دهد تا با تمرکز بیشتر منابع و زمان خود به طور هوشمندانه در نقاط ضعف امنیتی، بتوانیم پاسخگویی سریع‌تری برای مقابله با حملات جاسوسی سایبری داشته باشیم. در ادامه بحث دو مفهوم مدل اندلسی و ماتریس مایتره را شرح داده می‌شوند.

[1] Endesley
[2] Maitre Matrix

۲-۱- مدل اندلسی

مدل اندلسی فرایندهای شناختی و سازوکارهایی را که افراد برای ارزیابی شرایط برای توسعه آگاهی وضعیتی به‌کارگیری می‌کنند و همچنین کار و عوامل محیطی که بر توانایی آن‌ها برای دریافت آگاهی وضعیتی تأثیر می‌گذارد را توصیف می‌کند. این مدل سه سطح تشکیل آگاهی وضعیتی (ادراک، درک و تجسم حملات آینده.) را برابر شکل ۲-۱ با جزئیات توصیف می‌کند:



شکل (۱). مدل آگاهی وضعیتی اندلسی [۱]

الف) ادراک (سطح ۱ آگاهی وضعیتی): اولین گام در دستیابی به آگاهی وضعیتی درک وضعیت، ویژگی‌ها و پویایی عناصر مربوطه در محیط است؛ بنابراین، سطح ۱ آگاهی وضعیتی، اساسی‌ترین سطح آگاهی وضعیتی، شامل فرایندهای نظارت، تشخیص نشانه و تشخیص ساده است که منجر به آگاهی از عناصر موقعیتی متعدد (اشیا، رویدادها، افراد، سیستم‌ها، عوامل محیطی) و وضعیت فعلی آن‌ها (مکان‌ها، شرایط، حالت‌ها، اقدامات) می‌شود.

ب) درک (سطح ۲ آگاهی وضعیتی): گام بعدی در تشکیل آگاهی وضعیتی شامل سنتز عناصر سطح ۱ آگاهی وضعیتی از طریق فرایندهای تشخیص الگو، تفسیر و ارزیابی است. سطح ۲ آگاهی وضعیتی نیاز به یکپارچه‌سازی این اطلاعات برای درک چگونگی تأثیر آن بر اهداف و اهداف فرد دارد. این شامل توسعه یک تصویر جامع از جهان یا آن بخش از جهان است که برای فرد نگران‌کننده است.

ج) تجسم حالات آینده (سطح ۳ آگاهی وضعیتی): سومین و بالاترین سطح آگاهی وضعیتی شامل توانایی تجسم حالات آینده عناصر در محیط است. سطح ۳ آگاهی وضعیتی از طریق آگاهی از وضعیت و پویایی عناصر و درک وضعیت (سطوح ۱ و ۲ آگاهی وضعیتی) و سپس برون‌یابی این اطلاعات به‌موقع برای تعیین چگونگی تأثیر آن بر وضعیت‌های آینده محیط عملیاتی به دست می‌آید.

۲-۲- ماتریس مایتره:

ماتریس مایتره (تاکتیک‌های خصمانه، فن‌ها و دانش مشترک) یک چارچوب و پایگاه دانش شناخته‌شده در سطح جهانی است که در مورد تاکتیک‌ها، فن‌ها و روش‌هایی که توسط مهاجمین سایبری در طول حملات سایبری استفاده می‌شود بینش ارزشمندی را فراهم می‌کند. روش - های توسعه‌یافته و نگهداری شده توسط شرکت مایتره به‌عنوان یک منبع جامع برای درک و طبقه‌بندی روش‌های مختلف مورداستفاده توسط بازیگران تهدید است.

هدف اصلی مایتره افزایش درک جامعه امنیت سایبری از تهدیدات دنیای واقعی با سازمان‌دهی و فهرست‌بندی رفتارهای خصمانه است. این یک‌زبان و ساختار استاندارد برای توصیف کل چرخه عمر یک حمله، از شناسایی اولیه و بهره‌برداری به حرکت جانبی، استقامت و خروج ارائه می‌دهد. با نقشه‌برداری از این فن‌های حمله، سازمان‌ها می‌توانند تهدیدات سایبری تشخیص دهند.

جدول ۱. تشریح ماتریس مایتره

هدف	تاکتیک
جمع‌آوری اطلاعاتی که می‌توانند برای برنامه-ریزی عملیات آینده استفاده کنند	شناسایی
ایجاد منابعی که می‌توانند برای پشتیبانی از عملیات استفاده کنند	توسعه منابع
ورود به شبکه	دسترسی اولیه
اجرای کد مخرب	اجرا
حفظ موقعیت	ماندگاری
به‌دست‌آوردن مجوزهای سطح بالاتر	افزایش دسترسی
اجتناب از شناسایی	اجتناب از دفاع
سرقت نام حساب‌ها و رمزهای عبور	دسترسی به اعتبارنامه
کشف محیط اطراف	کشف
حرکت در محیط	حرکت جانبی
جمع‌آوری داده‌های موردعلاقه به هدف خود	جمع‌آوری
برقراری ارتباط با سیستم‌های به خطر افتاده برای کنترل آن‌ها	فرماندهی و کنترل
سرقت داده‌ها	دسترسی به داده‌ها
دست‌کاری، قطع یا نابودکردن سیستم‌ها و داده‌ها	تأثیر حمله

3. پیشینه تحقیق

اکبری و همکاران [۲]، مهاجمین سایبری قادرند با استفاده از حملات جلوگیری از خدمت توزیع‌شده، تأثیرات بسزایی بر میزبان‌های شبکه رایانه‌ای بگذارند و در مقابل مدافعین با استفاده از انواع روش‌های دفاعی به دفاع بپردازند، در چنین شرایطی تعیین وضعیت شبکه قربانی سخت و پیچیده است. جهت ارزیابی وضعیت صحنه نبرد سایبری، ضروری است مهاجم و مدافع مورد ارزیابی قرار گیرند که تمرکز این پژوهش در ارائه چارچوبی است که وضعیت قربانی را مورد ارزیابی قرار دهد.

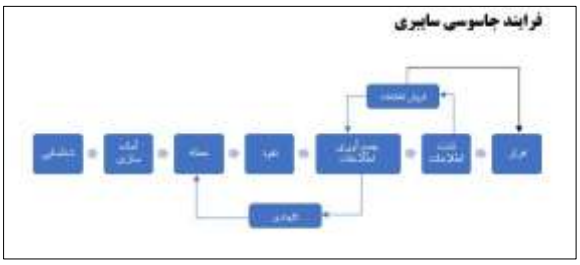
حسن‌نیا و همکاران [۳]، خطای نیروی انسانی در طراحی و پیکربندی شبکه‌ها و سامانه‌ها، بستری برای حمله است و از طرفی شبکه‌های گسترده ازنظر جغرافیایی در معرض حملات بیشتری بوده و نیاز به شناسایی زودهنگام حملات دارند. مرکز عملیات امنیت سایبری که معمولاً در شبکه‌های گسترده استفاده می‌شود، راهکاری برای پایش و شناسایی پیوسته است و در آن، نیروی انسانی نقش اصلی را ایفا می‌کند. در این تحقیق با بررسی موضوع مصورسازی و مقایسه نمونه‌های تجاری مراکز عملیات امنیت، روشی برای کمک به تشخیص بی‌درنگ حملات در شبکه‌های گسترده ارائه‌شده است.

- علی جبار رشیدی و همکاران [۴]، در حال حاضر ابزارهای مختلفی برای ثبت رویدادها و هشدارهای موجود در شبکه‌ها وجود دارد. بااین‌وجود، نیاز به سامانه‌ای که بتوان به کمک آن اطلاعات جمع‌آوری‌شده از تمام این منابع را به‌درستی کنار یکدیگر قرارداد و از ترکیب این اطلاعات تصمیم‌های درست اتخاذ نمود، کاملاً محسوس است. اگر قبل از حمله مهاجمین بتوان آن را پیش‌بینی نمود و اثرات آن را تخمین زد، راهبرد دفاعی مشخص‌تری انتخاب خواهد شد و می‌توان به میزان قابل‌توجهی خسارات را کاهش داد. تجسم حملات سایبری، پیش‌بینی حملات بر اساس یک چارچوب کاری مشخص است. برای این کار می‌توان از روش‌های مختلف ریاضی بهره جست. یکی از این روش‌ها، مدل انتقال باور است.
- کوروش داداش تبار احمدی و همکاران [۵]، هدف اصلی الگوریتم‌های تجسم، ارتقا عملکرد سامانه آگاهی وضعیتی سایبری است که این امر به‌واسطهٔ پر کردن شکاف‌های موجود بین سیستم‌های تشخیص نفوذ و به‌کارگیری مکانیزه‌های دفاعی امنیتی صورت می‌گیرد. در این مقاله طرحی ارائه خواهد شد تا بتوان وضعیت آینده فضای سایبری را تجسم نمود و اقدام پیش‌دستانه‌ای را با بهبود آگاهی وضعیتی به اجرا گذاشت.

کیانوش شوشیان و همکاران [۶]، یکی از تهدیدات مهم سال‌های اخیر در حوزه سامانه‌های رایانه‌ای و فضای سایبر، حملات سایبری مبهم است. مبهم‌سازی در سطح حمله به معنای تغییر حمله، بدون تغییر در رفتار و تغییر در نوع اثرگذاری حمله‌بر قربانی است. در این مقاله با ارائه طبقه‌بندی جدیدی در روش‌های مبهم‌سازی، برای مدل‌سازی حملات سایبری مبهم، روشی مبتنی بر فن افزودن حمله پیشنهادشده است. مهاجم در این روش با افزایش دسته‌بندی غلط در راهبردهای حمله، باعث جداشدن وابستگی میان هشدارها و اقدامات حمله می‌شود؛ بنابراین، با افزایش طول دنباله حمله، مدیران امنیت شبکه به‌راحتی نمی‌توانند حملات سایبری را تشخیص دهند. مدل پیشنهادی بر اساس الگوریتم بیزین ارزیابی شد. جداول و نمودارهای ارزیابی، نشان‌دهنده تدوین مناسب سازوکار ارائه‌شده برای دنباله حملات مبهم بوده به‌طوری که احتمال تشخیص حملات مبهم نسبت به حملات پاک بسیار کمتر است.

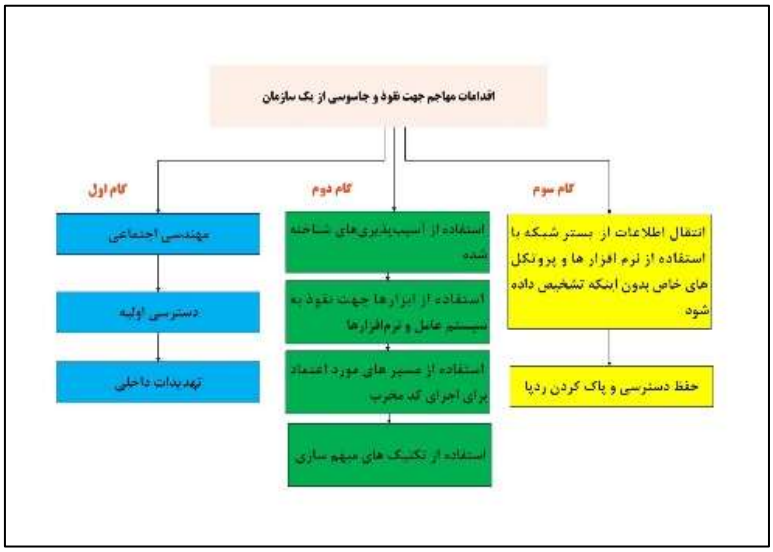
4. روش پیشنهادی

جاسوسی سایبری هجوم خاموش در دنیای دیجیتال است که باهدف سرقت اطلاعات حساس و محرمانه به‌صورت گام‌به‌گام انجام می‌شود. در این فرایند، جاسوسان سایبری بانفوذ به سیستم‌ها و شبکه‌های رایانه‌ای، به دنبال یافتن اطلاعات ارزشمندی هستند که می‌توانند از آن‌ها برای مقاصد مختلفی مانند سوءاستفاده مالی، اخاذی، خرابکاری و غیره استفاده کنند که برای رسیدن به هدف خود از روش‌ها و فرایندهای مختلفی استفاده می‌کنند.



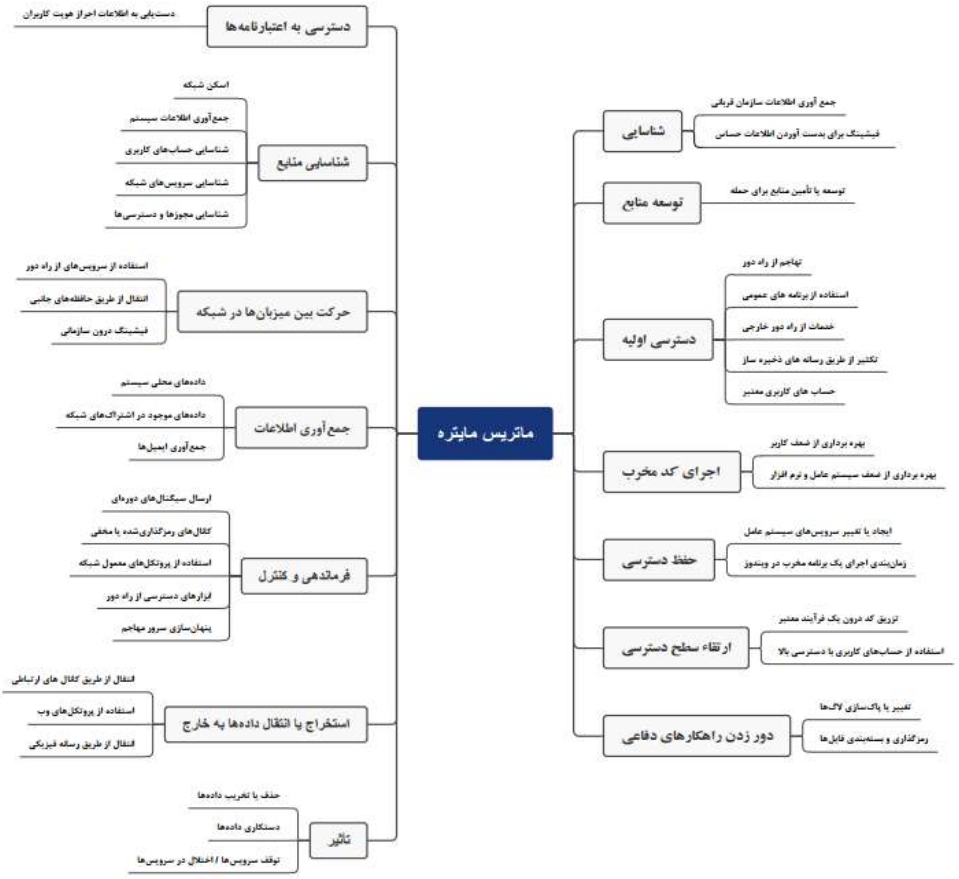
شکل (۲). فرایند جاسوسی سایبری [۷]

باتوجه‌به مدل ارائه‌شده شکل (۲) که نمایی از فرایند جاسوسی سایبری را نشان می‌دهد در این بخش اقدامات اجرایی مهاجمین سایبری را در سه‌گام اصلی برابر شکل (۳) نشان داده می‌شود که در گام اول اقدامات جهت شناسایی مواضع، گام دوم اقدامات جهت نفوذ به سیستم و اجرای کدهای مخرب و در گام سوم هدف مهاجم از نفوذ به سیستم که انتقال اطلاعات است را نشان می‌دهد.



شکل (۳). اقدامات مهاجم برای نفوذ و جاسوسی از یک سازمان

ماتریس مایتره در ۱۴ گام و ۲۳۴ فن به توصیف اقدامات مهاجمین سایبری پرداخته است. در این پژوهش ۳۶ فن از ۱۴ گام حمله از ماتریس مایتره استخراج‌شده و بر اساس آن‌ها یک طرح پیشنهادی بر مبنای اقدامات مهاجم سایبری ارائه می‌شود (شکل ۴).



شکل (۴). فن‌های مورداستفاده مهاجم سایبری جهت اقدام به جاسوسی [۸]

5. ارزیابی روش پیشنهادی

در دنیای دیجیتال و پیشرفته امروزی، حملات جاسوسی سایبری به سازمان‌ها به طور مداوم در حال افزایش است. این نوع حملات، باهدف سرقت اطلاعات حساس و محرمانه، به‌طورجدی امنیت و حریم خصوصی را تهدید می‌کنند؛ بنابراین، ارزیابی و تشخیص صحیح حملات جاسوسی سایبری از اهمیت بسیاری برخوردار است.

تشخیص حملات جاسوسی سایبری چالش‌هایی را در بردارد. مهاجمان این‌گونه حملات از روش‌های پیچیده و متنوعی استفاده می‌کنند تا فعالیت‌های خود را پنهان کنند و به طور ناشناس در شبکه‌ها و سیستم‌های هدف عمل کنند. به همین دلیل، نیازمندیم تا راهکارهایی ارائه دهیم که بهبود آگاهی وضعیتی در تشخیص حملات جاسوسی سایبری را فراهم کنیم. ما قصد داریم با استفاده از احصای قرائن و شواهد مبتنی بر فرایند حملات مایتره ۹ آگاهی وضعیتی در تشخیص حملات جاسوسی سایبری را بهبود بخشیم. با تحلیل و بررسی فرایند حملات جاسوسی سایبری و شناسایی قرائن و شواهد مرتبط با این نوع حملات، می‌توانیم الگوها و الزامات حملات را شناسایی کرده و راهکارهایی ارائه دهیم که در تشخیص حملات جاسوسی سایبری مؤثر باشند. در ادامه با تلفیق فرایند جاسوسی سایبری و گام‌های ۱۴گانه حمله به معرفی اقدامات مهاجم و قرائن و شواهد حمله خواهیم پرداخت.

1.5شناسایی[1]

در این مرحله مهاجم برای شناسایی اقدامات زیر را انجام می‌دهد.

1.1.5جمع‌آوری اطلاعات سازمان قربانی[2]

2.1.5فیشینگ برای به‌دست‌آوردن اطلاعات حساس[3]

قرائن:

- ایمیل‌های مشکوک،
- لینک‌های مشکوک،
- پیوست‌های مشکوک،
- درخواست اطلاعات شخصی،
- احساس فوریت.

شواهد:

- غلط‌های املایی و نگارشی،
- طراحی غیرحرفه‌ای ایمیل‌ها،
- نشانی URL جعلی،
- عدم وجود گواهینامه SSL،
- هشدار مرورگر.

روش‌های تشخیص:

- فیلترهای اسپم،
- نرم‌افزار آنتی‌ویروس،
- ابزارهای تشخیص فیشینگ،
- آموزش و آگاهی کاربران.

2.5توسعه منابع[4]

1.2.5 توانمندی‌های مرحله‌ای[5]

این حمله معمولاً برای نفوذ به سیستم‌های پیچیده و حفظ دسترسی بلندمدت به آن‌ها استفاده می‌شود.

قرائن:

- فعالیت غیرمعمول در شبکه،
- کاهش عملکرد سیستم،
- پیام‌های خطا،
- مشکلات ورود به سیستم.

شواهد:

- اسکن شبکه،
- نرم‌افزارهای مخرب،
- لینک‌های مخرب،
- ایجاد حساب کاربری مخفی.

روش‌های تشخیص:

- بررسی لاگ‌های سیستم،
- ابزارهای اسکن امنیتی سیستم،
- ابزارهای تشخیص نفوذ،
- سیستم‌های نظارت بر شبکه.

3.5 دسترسی اولیه[6]

در این مرحله از حمله مهاجم در تلاش است با بهره‌گیری از آسیب‌پذیری‌ها و ضعف‌های موجود به سیستم یا شبکه قربانی نفوذ کند.

1.3.5 تهاجم از راه دور[7]

2.3.5 استفاده از برنامه‌های عمومی[8]

3.3.5 خدمات از راه دور خارجی[9]

4.3.5 تکثیر از طریق رسانه‌های قابل‌حمل[10]

3.3.5 حساب‌های کاربری معتبر[11]

قرائن:

[1] Reconnaissance
[2] Gather Victim Network Information
[3] Phishing for Information
[4] Resource Development
[5] Stage Capabilities
[6] Initial Access
[7] Drive-by Compromise
[8] Exploit Public-Facing Application
[9] External Remote Services
[10] Replication Through Removable Media
[11] Valid Accounts

- افزایش ترافیک شبکه،
- کاهش عملکرد سیستم،
- پیام‌های خطا،
- حضور رسانه‌های ذخیره‌ساز ناشناس،
- تغییرات در تنظیمات حساب کاربری،
- فعالیت غیرمعمول.

شواهد:

- فایل‌های آلوده،
- پورت‌های باز،
- ثبت فعالیت مشکوک،
- نشت داده.

روش تشخیص:

- ابزارهای اسکن،
- ابزارهای آنتی‌ویروس،
- ابزارهای تشخیص نفوذ،
- سامانه کنترل رسانه ذخیره‌ساز،
- نظارت بر فعالیت کاربران.

4.5 اجرا[1]

در این مرحله از حمله مهاجم در تلاش است تا کدهای مخرب را در سیستم اجرا کند.

1.4.5 بهره‌برداری از ضعف سیستم[2]

2.4.5 بهره‌برداری از ابزار مدیریت سیستم‌عامل[3]

قرائن:

- فعالیت غیرمعمول در سیستم،
- کاهش عملکرد سیستم،
- تغییر در تنظیمات سیستم‌عامل،
- اجرای برنامه‌ها یا اسکریپت‌های مشکوک،
- فعالیت غیرمعمول در سرویس مدیریت سیستم‌عامل.

شواهد:

- رصد فرایندهای سیستم،
- تغییرات در پیکربندی،
- ثبت فعالیت مشکوک در لاگ سیستم،
- ایجاد حساب‌های کاربری جدید،

روش تشخیص:

- نظارت بر فعالیت سیستم،
- ممیزی سیستم،
- استفاده از ابزارهای تشخیص نفوذ،
- آموزش به کارکنان،
- بررسی پروسه‌ها و سرویس‌های مشکوک،
- بررسی گزارش‌های ابزارهای امنیتی.

5.5 ماندگاری:

در این مرحله از حمله مهاجم به دنبال راهی برای ماندگاری در سیستم قربانی پس از نفوذ اولیه است. این کار به مهاجم اجازه می‌دهد تا به طور مداوم به سیستم دسترسی داشته باشد و اقدامات مخرب خود را انجام دهد.

- سرویس انتقال هوشمند پس‌زمینه[4]
- خدمات از راه دور خارجی[5]

قرائن:

- فعالیت غیرمعمول در سرویس انتقال هوشمند پس‌زمینه،
- فعالیت غیرمعمول در شبکه،
- کاهش عملکرد سیستم،
- از دسترس خارج‌شدن سیستم.

شواهد:

- تغییر در رجیستری،
- وجود نرم‌افزار ناشناس در پوشه استارتاپ ویندوز،
- ایجاد سرویس‌های مشکوک در ویندوز.

روش‌های تشخیص:

- نظارت مستمر بر رویدادها،
- بررسی فایل‌های مشکوک،
- پیکربندی معماری ویندوز،
- نصب سامانه‌های شناسایی رفتارهای مخرب،
- رصد و پایش ترافیک شبکه.

6.5 افزایش سطح دسترسی۶

در این مرحله از حمله مهاجم به دنبال راهی برای افزایش سطح دسترسی خود در سیستم یا شبکه است. هدف از این حمله، دستیابی به کنترل بیشتر بر سیستم یا شبکه و انجام اقدامات مخرب مانند سرقت داده، خرابکاری یا نصب بدافزار است.

1.6.5 تزریق فرایند[7]

2.6.5 حساب‌های کاربری معتبر[8]

قرائن:

[1] Execution
[2] Exploitation for Client Execution
[3] Windows Management Instrumentation
[4] Background Intelligent Transfer Service (BITS job)
[5] External Remote Services
[6] Privilege Escalation
[7] Process Injection
[8] Valid Accounts

- فعالیت غیرمعمول در فرایندها،
- افزایش ناگهانی در استفاده از CPU یا RAM،
- کاهش عملکرد سیستم.

شواهد:

- تغییرات در فضای نشانی و حافظه فرایند،
- تغییر کلید APIهایی که توسط برنامه‌ها استفاده می‌شود،
- تغییر کدهای اجرایی فرایند،
- بررسی تغییرات در رجیستری‌های سیستم.

روش‌های تشخیص:

- استفاده از نرم‌افزارهای ضدویروس و ضد مالور،
- آنالیز ترافیک شبکه،
- ثبت وقایع فرایندها و رویدادهای سیستم،
- رصد تغییرات امنیتی در حساب کاربری.

7.5 فرار از دفاع[1]

در این مرحله از حمله مهاجم به دنبال راهی برای دورزدن ابزارها و سازوکارهای دفاعی امنیتی است. هدف از این حمله، پنهان‌کردن فعالیت‌های مخرب و افزایش احتمال موفقیت حمله است.

1.7.5 سرویس انتقال هوشمند پس‌زمینه[2]

2.7.5 رمزنگاری یا رمزگشایی از فایل‌ها[3]

قرائن:

- فعالیت غیرمعمول در شبکه،
- نقص در سیستم‌های امنیتی،
- تغییر در رفتار سیستم.

شواهد:

- تغییرات مشکوک در فایل‌ها،
- تغییر در زمان اجرا فایل،
- تغییرات در خطوط شبکه،
- تغییر در سطح دسترسی.

روش تشخیص:

- تجزیه‌وتحلیل ترافیک شبکه،
- نظارت بر سیستم‌های امنیتی،
- تجزیه‌وتحلیل سیستم‌ها،
- استفاده از ابزارهای تخصصی.

[1] Defense Evasion
[2] BITS Jobs
[3] Deobfuscate/Decode Files or Information

8.5 دسترسی به اعتبارها[4]

در این مرحله از حمله هدف مهاجم به‌دست‌آوردن اطلاعات ورود به سیستم کاربران برای دسترسی به حساب‌های کاربری آن‌ها است.

1.8.5 دستیابی به اطلاعات اعتباری در سیستم‌عامل[5]

قرائن:

- تغییر در حساب کاربری،
- عدم ورود کاربران به‌حساب کاربری.

شواهد:

- فعالیت‌های مشکوک در حساب کاربری،
- تغییرات غیرمنتظره در حساب کاربری،
- دسترسی به اطلاعات حساس با حساب کاربری.

روش‌های تشخیص:

- مانیتورینگ و رصد فعالیت‌های حساب‌های کاربری،
- استفاده از سیستم‌های تشخیص تهدیدات،
- رصد سازوکارهای احراز هویت قوی.

9.5 کشف[6]

در این مرحله از حمله هدف مهاجم جمع‌آوری اطلاعات در مورد یک شبکه یا سیستم رایانه‌ای است

1.9.5 کشف فایل‌ها و دایرکتوری‌ها[7]

2.9.5 اسکنر خدمات شبکه[8]

3.9.5 کشف خدمات شبکه[9]

4.9.5 کشف نرم‌افزارها[10]

5.9.5 کشف اطلاعات سیستم[11]

قرائن:

- ترافیک شبکه غیرمعمول،
- فعالیت غیرمعمول در سیستم‌ها،
- نقص در سیستم‌های امنیتی.

شواهد:

- اسکن پورت،
- جمع‌آوری اطلاعات DNS،
- شنود.

[4] Credential Access
[5] OS Credential Dumping
[6] Discovery
[7] File and Directory Discovery
[8] Network Service Discovery
[9] Software Discovery
[10] System Information Discovery
[11] Lateral Movement

روش‌های تشخیص:

-تجزیه‌وتحلیل ترافیک شبکه،
-نظارت بر سیستم‌ها،
-بررسی لاگ‌ها،
-آموزش کارکنان.

10.5 حرکت جانبی[1]

در این مرحله از حمله مهاجم پس از نفوذ اولیه به یک سیستم یا شبکه، به دنبال جابه‌جایی و نفوذ به سایر سیستم‌ها و دستگاه‌های موجود در آن شبکه است.

1.10.5 حمله فیشینگ درون‌سازمانی
2.10.5 تکثیر از طریق رسانه‌های قابل‌حمل[2]
3.10.5 آلودگی محتوای مشترک[3]

قرائن:

-ورود به سیستم از مکان‌های ناشناس،
-تلاش‌های ناموفق برای ورود به سیستم،
-تغییرات در تنظیمات حساب،
-استفاده از حساب‌های کاربری غیرفعال یا کم‌استفاده.

شواهد:

-وجود ابزارهای دسترسی از راه دور،
-ترافیک شبکه مشکوک،
-مشاهده ترافیک شبکه مشکوک،
-اشتراک‌گذاری‌های ناامن،
-شیوع بدافزار در شبکه.

روش‌های تشخیص:

-مانیتورینگ ترافیک شبکه،
-مانیتورینگ حرکت کاربران،
-استفاده از سیستم‌های تشخیص رفتار مشکوک.

11.5جمع‌آوری[4]

در این مرحله از حمله مهاجم سعی می‌کند اطلاعات حساس را از یک شبکه، سیستم یا سرویس خاص جمع‌آوری کنند.

1.11.5 بایگانی داده‌های جمع‌آوری شده[5]
2.11.5 جمع‌آوری خودکار[6]
3.11.5 جمع‌آوری داده از سیستم محلی[7]

قرائن:

-فعالیت غیرمعمول در سیستم،
-کاهش عملکرد سیستم،
-عدم دسترسی کاربر به سرویس‌های شبکه،
-اختلال در بهره‌برداری از دارایی‌های سازمانی.

شواهد:

-افزایش ترافیک در شبکه،
-ثبت ورودی و خروجی‌های نامعقول،
-تغییرات در دسترسی‌ها.

روش‌های تشخیص:

-بررسی لاگ‌ها،
-بهره‌برداری از سامانه‌های تشخیص نفوذ،
-بهره‌برداری از سامانه ضدبدافزاری تحت شبکه،
-بهره‌برداری از سامانه مدیریت رخداد سایبری.

12.5 فرماندهی و کنترل[8]

در این مرحله از حمله مهاجم سعی می‌کند از ترافیک عادی و موردانتظار تقلید کند تا از شناسایی جلوگیری کند.

1.12.5 کانال‌های پشتیبان[9]
2.12.5 انتقال داده به‌وسیله ابزار ورودی[10]
3.12.5 کانال‌های چندمرحله‌ای[11]
4.12.5 پراکسی[12]
5.12.5 نرم‌افزارهای دسترسی از راه دور[13]

قرائن:

-عدم توانایی در برقراری ارتباط،
-دریافت پیام‌های خطا،
-کاهش کیفیت خدمات شبکه،

شواهد:

-افزایش ترافیک نامتعارف،
-وجود نرم‌افزارهای ناشناخته،
-رفتار ناهنجار سخت‌افزار شبکه،
-نشانی ای پی مشکوک،
-پرس‌وجوهای غیرمعمول،
-زمان پاسخ نامتعادل.

روش‌های تشخیص:

-مانیتورینگ ترافیک،

[1] Internal Spearphishing
[2] Replication Through Removable Media
[3] Taint Shared Content
[4] Collection
[5] Archive Collected Data
[6] Automated Collection
[7] Data from Local System
[8] Command and Control
[9] Fallback Channels
[10] Ingress Tool Transfer
[11] Multi-Stage Channels
[12] Proxy
[13] Remote Access Software

- تحلیل رفتار دستگاه‌ها،
- سیستم‌های تشخیص نفوذ.

13.5 دسترسی به داده‌ها[1]

در این مرحله از حمله مهاجم با استفاده از روش‌های مختلف برای جمع‌آوری و استخراج اطلاعات غیرمجاز از شبکه استفاده می‌کند و آن‌ها را به سیستم‌های خود انتقال می‌دهد.

1.13.5 خروج اطلاعات با استفاده از پروتکل جایگزین[2]

2.13.5 انتقال داده به‌حساب ابری[3]

علائم:

- کندی شدید در شبکه،
- قطع ارتباط کاربران با سامانه‌ها،

شواهد:

- افزایش ترافیک شبکه،
- رصد ای پی‌های غیرمعمول و نامشخص،
- رصد ترافیک ارسال‌شده به آدرس‌های ناشناخته.

روش‌های تشخیص:

- آموزش کارکنان،
- مانیتورینگ و ضبط لاگ‌ها،
- مانیتورینگ فعالیت‌های داخلی،
- تحلیل ترافیک شبکه.

14.5 تأثیر حمله[4]

در این مرحله از حمله، هدف مهاجم تخریب یا قطع سرویس‌ها و منابع سیستم‌ها است. این نوع حمله می‌تواند منجر به آسیب‌رسانی به سیستم‌های اطلاعاتی، ازدست‌رفتن داده‌های حساس، اختلال در عملکرد سازمان و حتی آسیب جدی به سیستم‌های فیزیکی شود.

1.14.5 ازبین‌بردن داده‌ها[5]

قرائن:

- قفل‌شدن فایل‌ها،
- نمایش پیغام تهدیدآمیز،
- کاهش سرعت سیستم،
- حذف فایل‌ها،
- غیرعملیاتی شدن سخت‌افزار سیستم.

شواهد:

- تغییرات در پسوند فایل‌ها،
- تغییرات غیرمعمول در رجیستری،
- غیرعملیاتی شدن سخت‌افزار سیستم.

روش‌های تشخیص:

- نظارت مداوم بر سیستم،
- بررسی رفتار سیستم توسط عامل‌های امنیتی،
- بهره‌برداری از سامانه ضد باج‌گیر،
- رصد سی‌ام‌های تشخیص نفوذ.

جدول ۴-۱: نتایج نظرسنجی از خبرگان

نام حمله	روش تشخیص	درصد
جمع‌آوری اطلاعات سازمان قربانیان	آموزش کاربران	۶۵
فیشینگ برای به‌دست‌آوردن اطلاعات حساس	آموزش و آگاهی‌بخشی	۷۲.۵
توانمندی‌های مرحله‌ای	بررسی لاگ سیستم	۶۵
تهاجم از راه دور	سامانه وب	۴۲.۵
استفاده از برنامه‌های عمومی	مانیتورینگ ورودی‌ها	۳۰
خدمات از راه دور خارجی	مانیتورینگ ترافیک شبکه	۷۲.۵
تکثیر از طریق رسانه‌های قابل‌حمل	سامانه کنترل رسانه ذخیره‌ساز	۵۲.۵
حساب‌های کاربری معتبر	نظارت بر فعالیت‌های کاربران	۳۵
بهره‌برداری از ضعف کلاینت	گزارش‌های نرم‌افزارهای امنیتی	۴۰
بهره‌برداری از ابزار مدیریت سیستم‌عامل	بررسی پروسه‌ها و سرویس‌های مشکوک	۴۲.۵
سرویس انتقال هوشمند پس‌زمینه	بررسی فایل‌های مشکوک	۷۳.۵
خدمات از راه دور خارجی	رصد ترافیک شبکه	۴۲.۵
حساب‌های کاربری معتبر	رصد تغییرات امنیتی سیستم‌عامل	۴۲.۵
پروسس اینجکشن	مانیتورینگ و آنالیز فعالیت‌ها	۵۵
حساب معتبر	رصد فعالیت‌های حساب کاربری	۶۰
بهره‌برداری از سرویس سیستم‌عامل برای انتقال فایل بین دستگاه‌ها	بررسی فایل‌ها و محتوای آن‌ها	۶۰
رفع ابهام یا رمزگشایی فایل‌ها یا اطلاعات	بررسی تغییرات در ساختار فایل‌ها	۵۷
تخلیه اعتبارنامه سیستم‌عامل	آموزش کاربران	۴۸
کشف فایل و دایرکتیو	رصد و بررسی تغییرات دسترسی	۵۲.۵

[1] Exfiltration
[2] Exfiltration Over C2 Channel
[3] Transfer Data to Cloud Account
[4] Impact
[5] Data Encrypted for Impact

نام حمله	روش تشخیص	درصد
اسکنر سرویس شبکه	رصد سامانه تشخیص نفوذ	۵۷.۵
کشف نرم‌افزار	آموزش و آگاهی کاربران	۵۵
کشف اطلاعات سیستم	رصد آموزش و آگاهی کاربران	۵۵
کشف سرویس شبکه	رصد سیستم‌های تشخیص نفوذ	۵۷
فیشینگ داخلی طعمه‌ای	آموزش و آگاهی کاربران	۶۰
تکثیر از طریق رسانه‌های قابل‌حمل	رصد دسترسی به رسانه‌های قابل‌حمل	۴۰
محتوای مشترک آلوده	تحلیل و بررسی ترافیک شبکه	۴۸
جمع‌آوری خودکار	رصد و ثبت فعالیت‌ها	۴۳
بایگانی داده‌های جمع‌آوری‌شده	تحلیل فایل مبنی بر رفتار	۵۲
داده از سیستم محلی	مانیتورینگ فعالیت‌ها و لاگ‌ها	۴۵
کانال‌های بازگشتی	مانیتورینگ و آنالیز ترافیک شبکه	۵۹
انتقال داده به‌وسیله ابزار ورودی	بررسی فعالیت کاربران	۵۷
کانال‌های چندمرحله‌ای	رصد سامانه تشخیص نفوذ	۵۹
پراکسی	رصد سیستم‌های تشخیص نفوذ	۵۹
نرم‌افزار دسترسی از راه دور	راهکار مبتنی بر تحلیل محتوا	۵۵
انتقال داده از طریق پروتکل جایگزین	سامانه تشخیص نفوذ	۶۲
انتقال داده به‌حساب ابری	رصد و آنالیز ترافیک شبکه	۶۵
نابودی داده	رصد سیستم‌های تشخیص و پیشگیری از نفوذ	۵۸

6. نتیجه‌گیری

در این پژوهش، انواع فن‌ها و تاکتیک‌های استفاده‌شده توسط مهاجمین سایبری از ماتریس مایتره استخراج و قرائن و شواهد و انواع روش‌های تشخیص حملات، جمع‌آوری‌شده است و درنهایت از خبرگان حوزه پدافند سایبری به تعداد ۴۰ نفر نظرسنجی به‌عمل‌آمده و بهترین راهکارها تشخص حملات معرفی‌شده است و همچنین نتایج این نظرسنجی با استفاده از فرمول آلفای کرونباخ محاسبه‌شده و نتیجه ۰.۹۸۲ را به‌دست‌آمده است که این نتیجه عملکرد صحیح نتایج را نشان خواهد داد. استفاده از این راهکارها، می‌تواند به تشخیص دقیق‌تر حملات جاسوس سایبری کمک کند و همچنین می‌تواند تاب‌آوری سامانه‌ها را در برابر حملات سایبری بالابرده و زمان تشخیص و واکنش به این حملات را به حداقل برساند.

۷. مراجع

[1] Oxstrand, J., Ohara J., Le Blanc K., and Whaley A., “Development of an Initial Model of Human-Automation Collaboration-Results from a Needs Analysis”. SMR/ICHMI/INL/TR-2013/01, INL/EXT-13-28682. Idaho Falls, ID: Idaho National Laboratory (2013).

[2] Hamid Akbari, Seyed Mustafa Safavi Hammami, and Rizvan Dasani, "Situational awareness of distributed denial-of-service attacks based on prediction (visualization of the near future) of the battle scene based on Dempster-Shafer and Bayesian evidence theory," Electronic and Cyber Defense, vol. 7, no. 1 (series 25), pp. 77-94, 2018,

[3] Mohammad Hossein Hasannia, Mohammad Reza Hosni Ahangar, and Arash Ghafouri, "Presentation of an improved method for detecting incidents caused by cyber attacks," Electronic and Cyber Defense, vol. 7, no. 4, pp. 105-115, 2018,

[4] Ali Jabarrashidi, Majid Jafari, and Kurosh Dadash Tabarahmadi, "Visualization of cyber attacks by damage estimation and combination of attacker capability and opportunity based on belief transfer model," Electronic and Cyber Defense, vol. 6, no. 4, pp. 1-12, 2017,

[5] Korosh Dadash Tabarahmadi, Ali Jabarrashidi, and Morteza Berari, "Providing a new architecture for visualizing the effects of cyber attacks based on the integration of high-level information in cyber command and control," Electronic and Cyber Defense, vol. 2, no. 4 (consecutive 8), pp. 1-14, 2013,

[6] Kianoush Shoshian, Ali Jabbar Rashidi, and Mehdi Dehghani, "Modeling fuzzy cyber attacks based on attack matching with attack addition ،فـن" Electronic and Cyber Defense, vol. 7, no. 4, pp. 91-103, 2018,

[7] Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2022). An analysis of cyber espionage process. In Developments and Advances in Defense and Security: Proceedings of MICRADS 2021 (pp. 3-14). Springer Singapore.

پایگاه‌های اینترنتی:

[8] https://www.trellix.com/en-us/img/newsroom/stories/defending-against-cyber-espionage-campaigns-operation-graphite-4.jpg

[9] https://attack.mitre.org/matrices/enterprise/