سایبران
موسسه اطلاع رسانی امور سایبری
شهریور ۱۴۰۴
Cyberban WorldNews Agency

طوفان الاقصی سایبری

گزارشی تحلیلی از عملیات‌های سایبری پس از عملیات طوفان‌الاقصی

- با مقدمه‌ای از دکتر محمد رستم‌پور
- بررسی انواع حملات‌سایبری پس از طوفان‌الاقصی
- نقش سایبر در رزم (واکاوی عملیات‌های سایبری پس از وقایع میدانی)
- حملات‌سایبری به زیرساخت‌های حیاتی و صنعتی
- کشورهای احتمالی فعال در نبردسایبری
- شناسایی گروه‌های هکری فعال در عملیات‌های سایبری

فهرست مطالب

صاحب امتیاز: خبرگزاری سایبربان (اولین موسسه اطلاع رسانی امور سایبری در ایران)

سردبیر: مهندس کیانوش ادیب

گرافیک: سینا تقی‌زاده

هیئت تحریریه و تحقیقات: مهندس کیانوش ادیب ، مهندس سید احمد موسوی

دکتر محمد رستم پور، کامیار عزیزی

سخن سردبیر:
مهندس کیانوش ادیب

امروزه حملات سایبری به یکی از مهم‌ترین ارکان جنگ‌های ترکیبی تبدیل شده‌اند و حتی به‌صورت مستقل نیز از توان تخریب و اثرگذاری عملیاتی بالایی برخوردارند. این نوع جنگ‌ها با ابعاد مختلف اطلاعاتی، شناختی و نظامی درهم تنیده شده و سطح قابل توجهی از بازدارندگی در برابر دشمنان ایجاد می‌کنند.

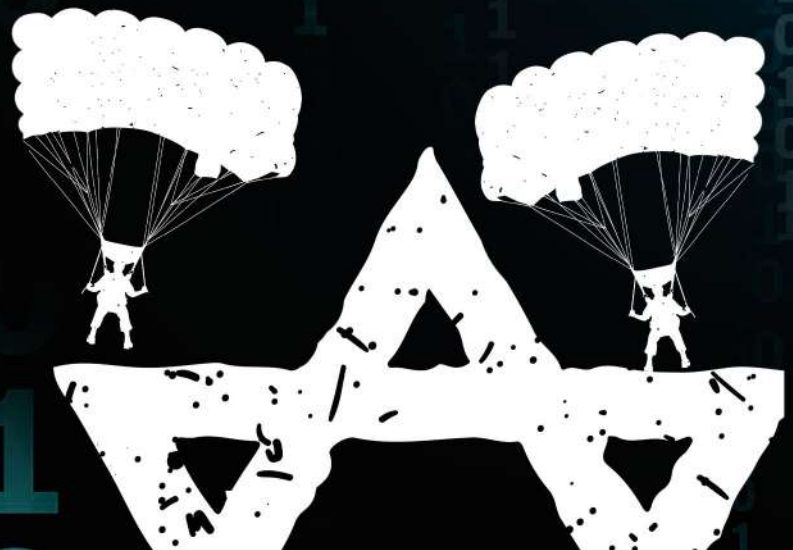
در سال‌های اخیر پس از جنگ روسیه و اوکراین که نمونه ای بارز از نبردهای ترکیبی با آغاز حملات سایبری بود، نبردهای سایبری پس از عملیات «طوفان الاقصی» و درگیری های محورمقاومت علیه رژیم‌صهیونیستی را در حقیقت باید صحنه ای بی‌بدیل از نقش آفرینی سایبر در عملیات های نظامی دانست. به گونه ای که اگر حضور مؤثر بازوی سایبری در کنار سایر اهرم ها در این نبردها نبود، قدرت مانورهای دشمن به مراتب بیشتر و خطرناکتر از شرایط کنونی بود.

بررسی‌های سایبربان از حملات‌سایبری در ۱۰۰ روز نخستین نبرد طوفان‌الاقصی، ضعف‌های آشکار رژیم‌صهیونیستی را که همواره مدعی برخورداری از پیشرفته‌ترین سیستم‌های دفاع سایبری و بالاترین سطح آمادگی امنیت‌سایبری در جهان بوده، آشکار ساخته است.

این ویژه‌نامه، حملات‌سایبری صورت گرفته توسط گروه‌های مختلف را شناسایی و راستی آزمایی کرده و نشان می‌دهد که ادعاهای امنیتی این رژیم تا چه اندازه با واقعیت فاصله دارد.

امید است گروه‌های‌سایبری محورمقاومت با تحلیل جامع از دستاوردها و چالش های این ۱۰۰ روز، چشم انداز دقیق‌تری برای راهبردهای آینده خود در عرصه سایبری ترسیم کنند.

این اطلاع‌نگاشت‌ها در راستای آگاهی بخشی و بررسی عمیق، حملات نه تنها توان بازدارندگی را افزایش می دهد، بلکه مسیر مقابله با دشمن را در جنگ های ترکیبی آینده هموارتر خواهد کرد.



کارشناس سایبری:
دکتر محمد رستم پور

اطللس آفند و پدافند سایبری رژیم صهیونیستی پس از عملیات طوفان‌الاقصی

به موازات پیشرفت فناوری در حوزه‌های متنوع سایبری، تهدیدات و خطرات به‌کارگیری آن نیز رو به تزاید و فزونی می‌رود. به‌ویژه آنکه در جهان قطبی‌شده امروز، کشورهای مختلف می‌کوشند ضعف بعضاً غیرارادی خود در عرصه هایی همچون زمین و فضای جغرافیایی را با سرمایه گذاری و تمرکز دانشی در دیگر حوزه‌ها جبران کنند و منافع ملّی خود را بیشینه سازند. با این نگاه باید دانست تمامی کشورها به ویژه آنانی که بازیگران مهم و کلیدی محیط ژئوپلتیک به شمار می‌روند، همگی از عرصه سایبر متأثر می‌شوند و بر آن اثر می‌گذارند. این مهم را باید به ورود جهان به دوره‌ای که به دلیل تکثیر اینترنت از حیث فرهنگی و سیاسی، جهان متمایزی است؛ اضافه کرد. پیشرفت های فناورانه در زمینه هوش مصنوعی، اتوماسیون، یادگیری ماشینی در کنار بالا رفتن دسترسی به بیگ دیتا، مرحله جدیدی از منازعه سیاسی میان قدرت‌های جهانی و رقبای منطقه‌ای برپا کرده است.

اگر تا دیروز، حمله به ستادهای انتخاباتی، تلاش برای نفوذ طولانی روی چهره‌های سیاسی و برپایی انقلاب‌های رنگی برای تغییر روندهای سیاسی به عنوان «مداخله سیاسی» تعریف می‌شد، امروز حملات سایبری در طیفی گسترده از هک وب‌سایت‌های برگزاری انتخابات گرفته تا دستکاری افکار عمومی انواعی از مداخله یا اثرگذاری سیاسی به شمار می‌آیند.این حملات در دسته‌بندی‌های گوناگون از آشکار تا پنهان، از فیزیکی تا دیجیتال، از معمولی تا نامتقارن تقسیم‌بندی می‌شوند.

به رغم اینکه ابزارهای جدید فناورانه، این اثرگذاری را آسان‌تر، سریع‌تر و در برخی برهه‌های کوتاه‌مدت، محسوس‌تر ساخته؛ به دلیل پیچیدگی فرایند، ارزیابی دقیقی در مورد آن وجود ندارد، به ویژه در برخی عملیات های نفوذ که دقیق نیستند و نتایج و عواقب ناخواسته و مبهمی به دنبال دارند. از ابتدای برپایی طوفان‌الاقصی یعنی از ۷ اکتبر ۲۰۲۳، به موازات ویران‌کننده‌ترین و خسارت‌بارترین تهاجم همه‌جانبه به رژیم صهیونیستی، عملیات‌های سایبری کوچک و بزرگ، در سطوح خرد، متوسط و کلان و با اهداف گوناگون به دست و ذهن گروه های سایبری پرشماری از کشورها و جغرافیاهای مختلف اجرا شد. احصاء، توصیف، بررسی و ارزیابی این عملیات‌ها در دوره‌های زمانی مختلف و به ویژه چینش آنها در یک تقویم زمانی واجد نکات و نتایج بسیار ارزشمندی است که می‌تواند اطلس تفصیلی **سایبر مقاومت** را تشکیل دهد.

ضرورت

بدین منظور، تمرکز بر ۱۰۰ روز نخست جنگ اهمیتی مضاعف دارد؛ چرا که:

- اولاً هیچ جنگ سایبری با این مدت زمانی طولانی تاکنون رخ نداده است. جنگ‌های سایبری رخ داده تاکنون، همچون جنگ‌های روانی و اطلاعاتی عمدتاً عملیات سایبری یا تنش سایبری بوده‌اند. حتی سازوکارها، زیرساخت‌ها و سیاست‌ها و قواعد و معماری سایبری کشورها براساس وقایع محدود بوده است.

برای نمونه معماری و استراتژی‌های بنیادین و حتی نوع پرداخت عملیاتی تیم‌های پدافندی متنوع و پراکنده در بخش‌های گوناگون ایالات متحده، کاملاً برآمده از تهدیدات و حتی حملاتی است که آمریکا به ویژه از دهه ۸۰ یعنی در چهل سال اخیر داشته است.

در نتیجه این تجربه طولانی از **جنگ سایبری**، یقیناً میدان سایبر به عنوان یکی از وجوه جنگ ترکیبی را تغییر خواهد داد. دو نگاه اساسی در مورد کارایی سایبر در یک هماوردی و رقابت نظامی وجود دارد. گروهی بر آنند که سایبر یک بستر است که سایر عملیات‌های معمول در غلبه بر رقیب مانند زد و خورد نظامی، تحریم اقتصادی یا کشمکش‌های سیاسی بر آن استوار می‌شود و گروهی به سایبر، نگاه کاتالیزوری یا نیابتی دارند که آفند یا پدافند سایبری را زمینه و مقدمه رخ اصلی جنگ می‌شناسند یا آن را جایگزین اشکال سختِ معمول آن می‌نشانند.

سایبر چه در نگاه زمینه‌ای یا دیدگاه متنی، تاکنون در نبردی که به تدریج به دو سالگی‌اش نزدیک می‌شویم، روی میز قرار نداشت تا آن را در تبدیل و تغییر نوع جنگ، نقطه عطف بشناسیم یا خیر...

-ثانیاً به جز زمان، استفاده گسترده از راهبردها و روش‌ها و وزن‌کشی دارایی‌ها و امکان‌ها تاکنون رخ نداده و از این نظر، جنگ غزه را باید جدی‌ترین آزمون سایبری در تمامی انواع تکنیک‌ها و ابزارها فهم کرد.

بسیاری از پدیده‌ها به دلیل فراوانی استفاده و رواج مستمری که در اسناد و تحلیل‌ها دارند، بی‌نیاز از تعریف و توضیح نشان می‌دهند.

این اتفاق، یعنی نبود تعریف دقیق و روشن که ابعاد و زوایای یک پدیده را آشکار کند، در محیط‌های اطلاعاتی چندان اثرگذار نیست. تعدد و فوریت عملیاتی در محیط اطلاعاتی ایجاب می‌کند تا فهم بینابینی و تصور ذهنی از یک پدیده مبنای تصمیم‌گیری و اجرا قرار گیرد.

در نتیجه می‌توان عملیات‌های آفندی و پدافندی پرشماری دید که بدون توجه به تبیین‌های مفهومی، یک هدف عینی را دنبال می‌کنند و عاملان و مجریان، صرف دستیابی به آن را براساس ارزیابی بیرونی، نشانه موفقیت اعلام می‌کنند.

اما در بررسی و ارزیابی به ویژه داوری مالی، کنش‌های نظامی و پروژه‌های سیاسی، تعاریف، مبانی و معیارها باید آشکار، دقیق، صریح و قابل اندازه‌گیری باشند.

صحنه جنگ غزه میدانی برای چنین بررسی و ارزیابی پرهزینه‌ای فراهم کرد تا جدا از ارتقای فناوری‌ها، تکنیک‌ها و ابزارها نیز محک بخورد.

بر این اساس می‌توان گفت بررسی تفصیلی حملات و انواع آنها و تمرکز بر چرایی و چگونگی رخداد آنها می‌تواند هم در ارزیابی **توان سایبری** جبهه مقاومت و هم در شناخت بهتر دارایی‌ها، پیشرفت‌ها و امکان‌های رقیب نیز به کار آید.

در ۱۵ سال اخیر، رقابت های سایبری آمریکا و روسیه و به صورت کلی غرب و شرق در میدان آزمون اوکراین محک می‌خورند.

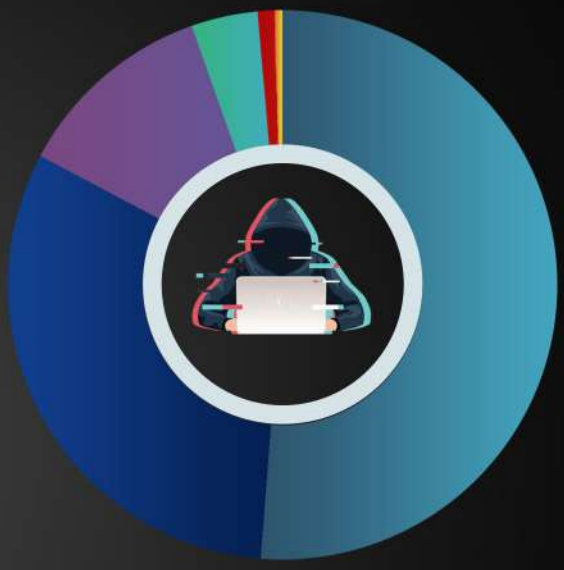
در نگاه بلندمدت، روسیه پیش از راه‌اندازی ترول‌ها و ربات های سیاسی در سراسر اروپا در عملیات‌های پرشماری از جمله انتشار اخبار فیک، راه‌اندازی کمپین‌های اطلاعات گمراه‌کننده، حملات سایبری زیرساختی به شبکه‌های انرژی، مؤسسات مالی یا نهادهای سیاسی و انتخاباتی، عملیات‌های خود را ابتدا در اوکراین تست می‌کند و پس از بازخوردگیری، کوشش می‌کند نسخه اصلاح شده آن را در گستره‌ای وسیع‌تر مانند اروپای شرقی و حتی آمریکا به کار گیرد.

نکته بسیار اساسی درباره عملیات‌های نفوذ و به ویژه عملیات‌های هک و افشاگری، این است که این عملیات‌ها همه بخشی از یک استراتژی سیاسی کلان هستند که به کمک سازمان‌های رسانه‌ای و مافیا، رسانه های اجتماعی، گروه‌های جامعه مدنی و نیروها و احزاب سیاسی به نتیجه می‌رسند و مطلوبیت و اثرگذاری خود را به خوبی نشان می‌دهند.

بررسی انواع حملات سایبری

بررسی انواع حملات سایبری

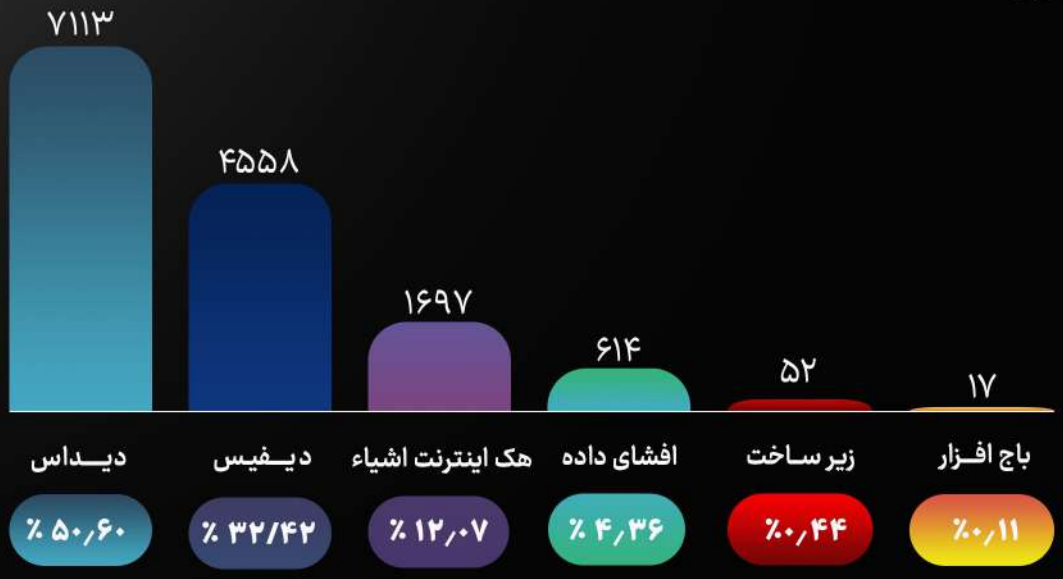
از شروع عملیات طوفان‌الاقصی در ۱۷اکتبر ۲۰۲۳ به مدت ۱۰۰روز، حملات‌سایبری میان حامیان‌غزه و رژیم‌صهیونیستی مورد بررسی و داده‌کاوی قرار گرفت که نمودارهای زیر آمار کلی انواع حملات در جنگ را به تفکیک نشان می‌دهد.
حملات‌سایبری صورت گرفته در این نبرد به ترتیب کیفیت شامل: حملات‌سایبری به زیرساخت‌های صنعتی، حملات افشای داده، حملات هک اینترنت اشیاء، حملات دیفیس(تخریب‌سایت)، حملات باج افزار و حملات دیداس(اختلال‌منع‌سرویس‌توزیع‌شده) نشان داده شده است.



- زیرساخت صنعتی – SCADA ATTACK
- افشای داده – DATA LEAKS
- هک اینترنت اشیاء – EXPLOSION OF IOT DEVICES
- دیفیس – DEFACE
- باج افزار – RANSOMWARE
- دیداس – DISTRIBUTED DENIAL OF SERVICE

بررسی آماری

طبق داده‌کاوی‌ها و بررسی‌های صورت گرفته در این ویژه نامه آمارکلی حملات‌سایبری بیش از ۱۴۰۰۰ مورد گردآوری شده است.



اختلال منع سرویس توزیع شده

- ۷۱۱۳ حمله‌سایبری به صورت دیداس
- بیشترین اهداف این حملات: بنگاه های اقتصادی دولتی و خصوصی

حامیان غزه
رژیم صهیونیستی و حامیان

دیفیس

- ۴۵۵۸ حمله‌سایبری به صورت دیفیس و مخدوش کردن سرورهای نگهدارنده اطلاعات
- بیشترین اهداف این حملات: سایت های دولتی

هک اینترنت اشیاء (IOT)

- ۱۶۹۷حمله سایبری به شبکه اینترنت اشیاء
- بیشترین اهداف این حملات: دوربین های مدار بسته

افشای داده

- ۶۱۴ حمله‌سایبری به صورت افشای داده و دسترسی غیر مجاز به اطلاعات
- بیشترین اهداف این حملات: پایگاه داده اطلاعات هویتی

زیرساخت

- ۵۲ حمله‌سایبری به بخش های مهم صنعتی و اختلال در زنجیره تأمین انرژی
- بیشترین اهداف این حملات:
  - شبکه تولید و توزیع برق مراکز صنعتی و شهری
  - مراکز توزیع و تصفیه آب و فاضلاب شهری و کشاورزی

باج افزار

- ۱۷ حمله باج افزاری
- بیشترین اهداف این حملات: اطلاعات بنگاه های اقتصادی و مراکز ارائه خدمات دولتی

بررسی و داده‌کاوی‌های صورت گرفته بیانگر این است که بیشترین حملات‌سایبری، حملات منع‌سرویس‌توزیع‌شده بوده که از نظر سطح پیچیدگی و آسیب‌زایی در پایین‌ترین سطح قرار دارد، در صورتی که حملات زیرساختی با کمترین تعداد در بالاترین سطح اثرگذاری قرار دارند.

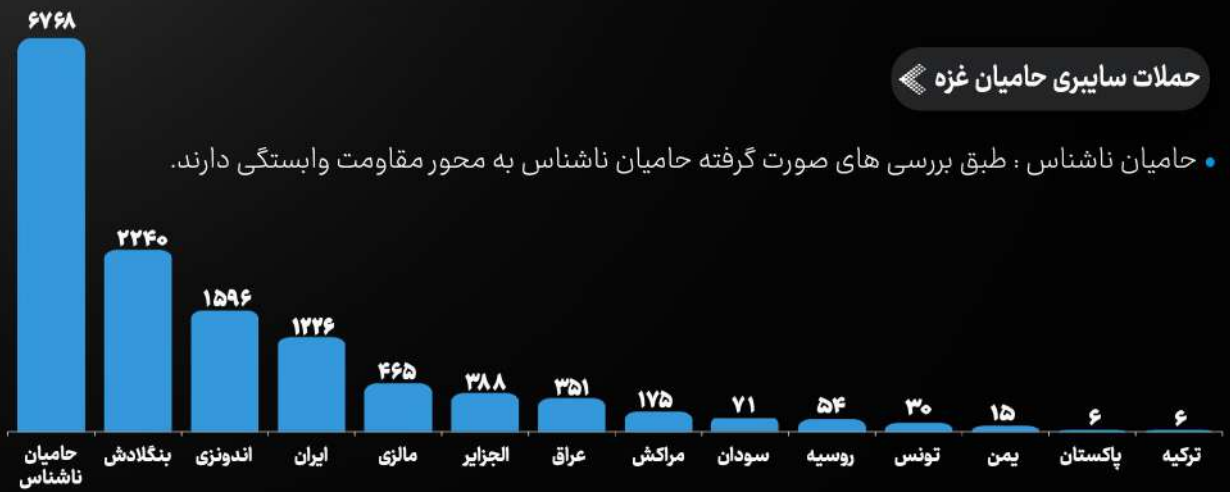
کشورهای فعال
درنبرد سایبری

کشورهای فعال در جنگ سایبری پس از طوفان الاقصی

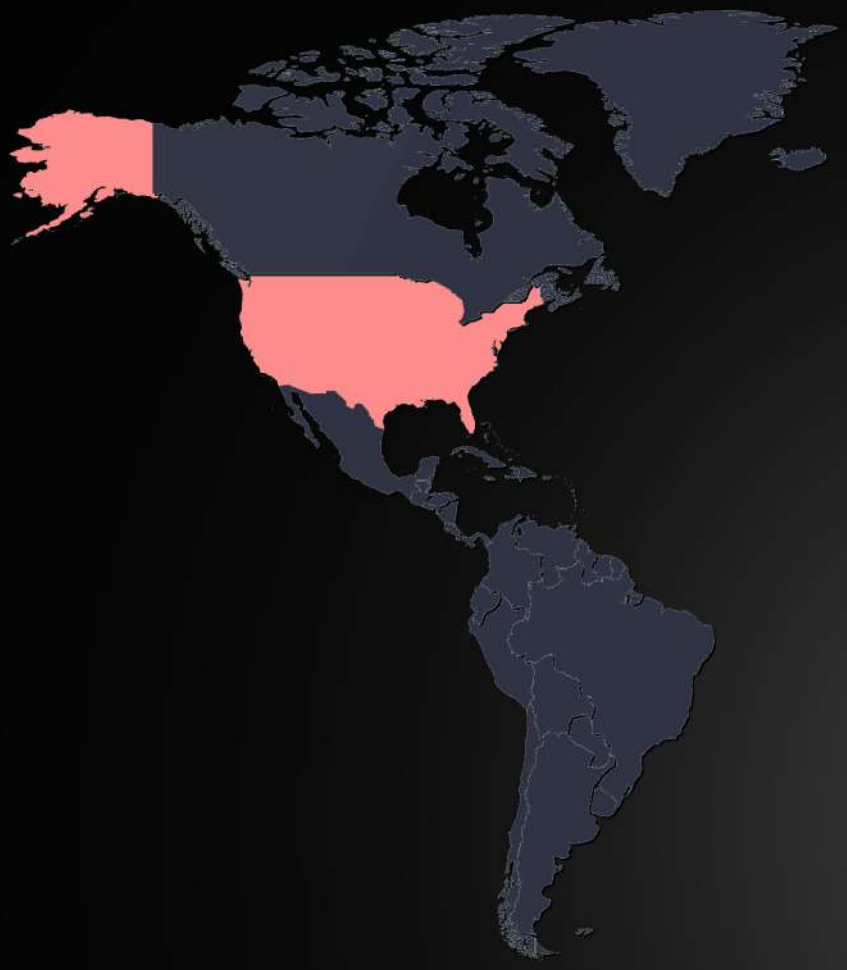
نبردهای سایبری پس از طوفان الاقصی در واقع میان دو محور حامیان غزه و رژیم صهیونیستی و حامیان به وقوع پیوست. در این نبردها اغلب مهاجمین به صورت گروه‌های ناشناس حاضر شده و گروه‌های اندکی نیز با پرچم وارد میدان شدند.

حملات سایبری حامیان غزه

- حامیان ناشناس : طبق بررسی های صورت گرفته حامیان ناشناس به محور مقاومت وابستگی دارند.



- تعداد حملات‌سایبری حامیان غزه : ۱۳۳۹۱



رژیم صهیونیستی و حامیان

- حامیان ناشناس : طبق بررسی های صورت گرفته حامیان ناشناس به کشور های ایالات متحده آمریکا ، انگلستان ، آلمان و استرالیا وابستگی دارند.

- تعداد حملات سایبری رژیم صهیونیستی و حامیان :۶۴۵


گروه های هکری

گروه های هکری فعال در نبرد سایبری طوفان الاقصی

گروه های هکری حامی غزه

در این بخش به منظور آشنایی بیشتر با گروه‌های هکری فعال در نبرد طوفان الاقصی، نام و نشان‌واره گروه‌های حامی غزه ارائه شده است. لازم به ذکر است در این نبردها، برخی گروه‌های هکری اقدام مستقلی انجام ندادند، بلکه در حملات گروه‌های بزرگتر مشارکت داشتند.

گروه های هکری حامی غزه


حملات سایبری
حامیان غزه

حملات سایبری حامیان غزه در نبرد طوفان الاقصی

پس از عملیات طوفان‌الاقصی، گروه‌های‌سایبری به میدان آمدند و رژیم‌صهیونیستی و حامیانش را هدف حملات قرار دادند. در داده‌کاوی های صورت گرفته میزان حملات ، تعداد گروه‌های مشارکت کننده و پرچم‌احتمالی آنها را مشاهده می‌نمایید.

گروه های سایبری حامیان‌ناشناس غزه

- ACEH ABOUT HACKED WORLD
- ALTOUFAN TEAM
- ANON BLACK FLAG
- Anonymous Collective
- Anonymus x
- Arab Anonymous Team
- Ayyildiz Tim
- AHU Official
- Anonymous arabia]
- Anonymous Palestine
- Black basta
- Black Magic
- Black Security Team
- Black Shadow
- Blacksec
- BOOM SECURITY
- C.O.A Agency
- Cyber Army of Palestine
- CYBER ERROR SYSTEM
- Cyber toufan
- Cyber Av3ngers
- D3ltaboys
- Devilattacks
- EAGLE CYBER CREW
- Electronic Tigers Unit
- Fallaga Team
- Force Electronic Quds
- Forces of light
- For Humanity
- GARUDA SECURITY
- GB ANON 17
- Ghost of Palestine
- GhostSec
- Gaza Children's Group
- Hacktivist Of Garuda
- Handala
- Homeland Justice
- HostKillCrew
- IDF Leaks
- IETHESIA
- Iman19X
- IRoX Team
- IXP666SECTEAM
- Jateng Cyber Team
- Jewish Peace Advocate
- KEP TEAM
- Kerala Cyber Xtractors
- Key2Pay
- karma
- khalifah cyber crew
- kuningan exploiter
- Lisium
- LOLSEC ANON
- LockBit
- MuddyWater
- Malek Team
- Neo Cyber
- PADANG SYSTEM ERROR
- Rubit
- SkyNet
- Soldiers Of Solomon
- SS-Cyber-team
- Sharp Boys
- SparrowCorp
- team 1722
- team 1956
- team 313
- Team Azrael Angel Of Death
- Team Herox
- TengkorakCyberCrew Official
- the CyberWatchers
- The Returnees
- TYG Team
- weedsec
- X7ROOT SELLER
- yoos e cybery
- Zer-Day Lab
- 177 Member Team

حامیان‌ناشناس گروه‌های هکری هستند که بدون پرچم در این جنگ‌سایبری حضور داشتند و بیشترین تعداد گروه‌ها را تشکیل می‌دهند. اکثر این گروه‌ها به محورمقاومت وابستگی داشتند.

گروه‌های سایبری با پرچم احتمالی مراکش

نام گروه‌های فعال

- Moroccan Defenders Group
- Moroccan Ghosts
- Morrocan Black Cyber Army
- Team R66
- Team One Piece

گروه‌های سایبری با پرچم احتمالی مالزی

نام گروه‌های فعال

- 4 EXPLOITATION Channel
- CsCrew
- DragonForce Malaysia
- Ghost Clan Malaysia
- khalifah cyber crew
- Malasysia Cyber Defacer
- STUCX TEAM
- SynixCyberCrimeMY

گروه‌های سایبری با پرچم احتمالی اندونزی

نام گروه‌های فعال

- TENG4HBL4CKHAT
- GANOSEC TEAM
- Lulz Security Agency
- GARNESIA TEAM
- 5UL4WES1 TENG4H BL4CKHAT
- AnonGhostIndonesia
- ISLAMIC CYBER TEAM
- ISLAMIC CYBER TEAM INDONESIA
- VulzSec Official
- DARK OLYMPUZT CREW
- Dark Storm
- Esteem Restoration Eagle
- Hacktivist Indonesia
- HIZBULLAH CYB3R TEAM INDONESIA
- INFINITE INSIGHT.ID
- Ketapang Grey Hat Team
- StarsX Team
- JAWA BARAT EROR NETWORK

گروه‌های سایبری با پرچم احتمالی بنگلادش

نام گروه‌های فعال

- Mysterious Team Bangladesh
- The Anonymous BD
- SYLHET GANG SG
- THE CAMP 22

گروه‌های سایبری با پرچم احتمالی الجزایر

نام گروه‌های فعال

- Anonymous Algeria
- BEN MHIDI 54
- Muslim Cyber Army (CMA)
- Nothwhome Of Security
- اسماعیل مان 54

گروه‌های سایبری با پرچم احتمالی پاکستان

نام گروه‌های فعال

- Team Insane PK

گروه‌های سایبری با پرچم احتمالی روسیه

نام گروه‌های فعال

- Usersec
- KILLNET

گروه‌های سایبری با پرچم احتمالی عراق

نام گروه‌های فعال

- team1915

گروه‌های سایبری با پرچم احتمالی ترکیه

نام گروه‌های فعال

- Aslan Neferler Tim
- Ayyildiz Tim

گروه‌های سایبری با پرچم احتمالی یمن

نام گروه‌های فعال

- ابنا الصعده یمن
- YourAnonTl3x

گروه های‌سایبری با پرچم احتمالی سودان

نام گروه‌های فعال

- Anonymous sudan

گروه‌های سایبری با پرچم احتمالی ایران

نام گروه‌های فعال

- Hagh1oyann
- Moses Staff
- Yare comnam
- Cyber Fattah Team
- Solomon's ring

گروه‌های سایبری با پرچم احتمالی تونس

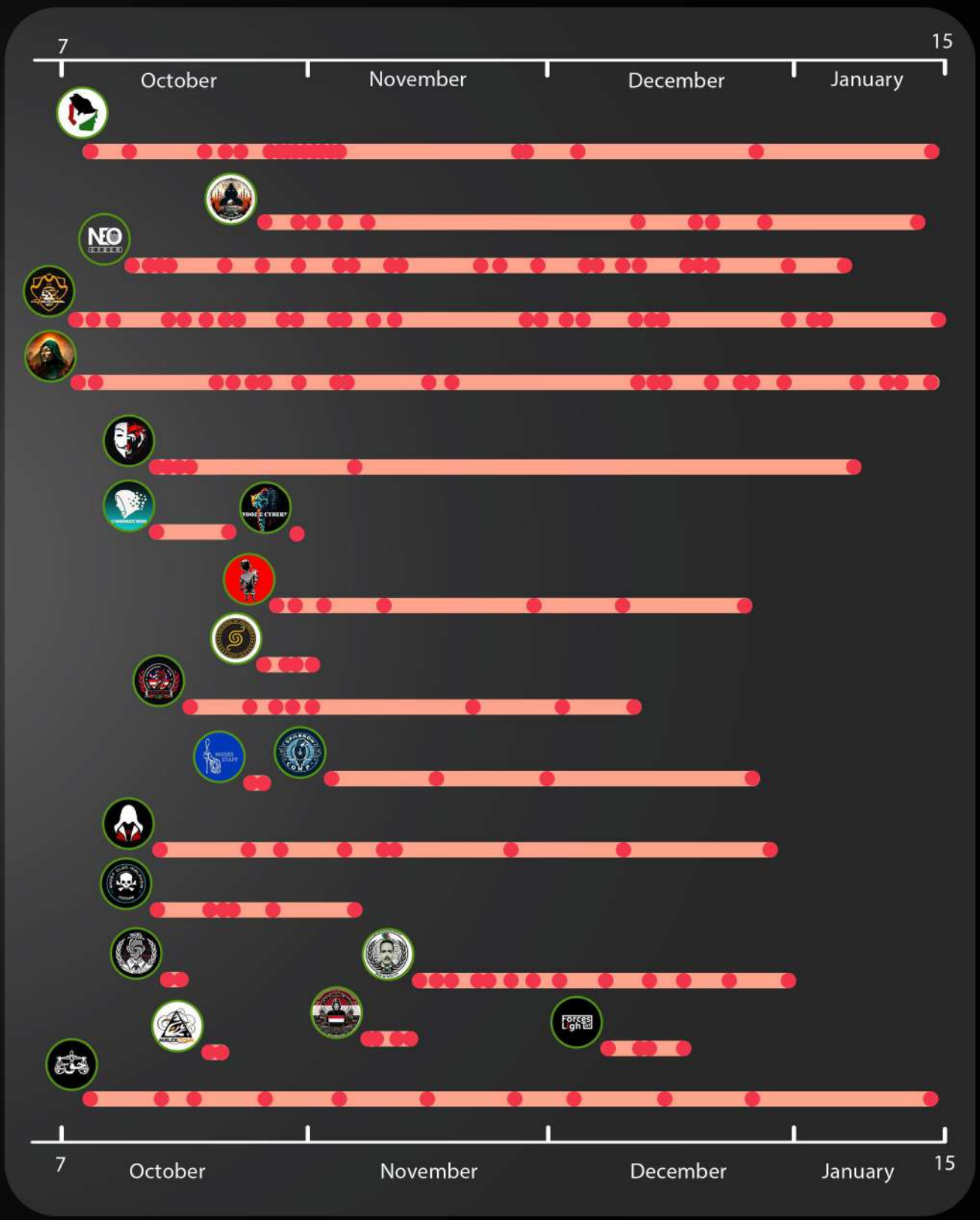
نام گروه‌های فعال

- organization clay hacker tunisia

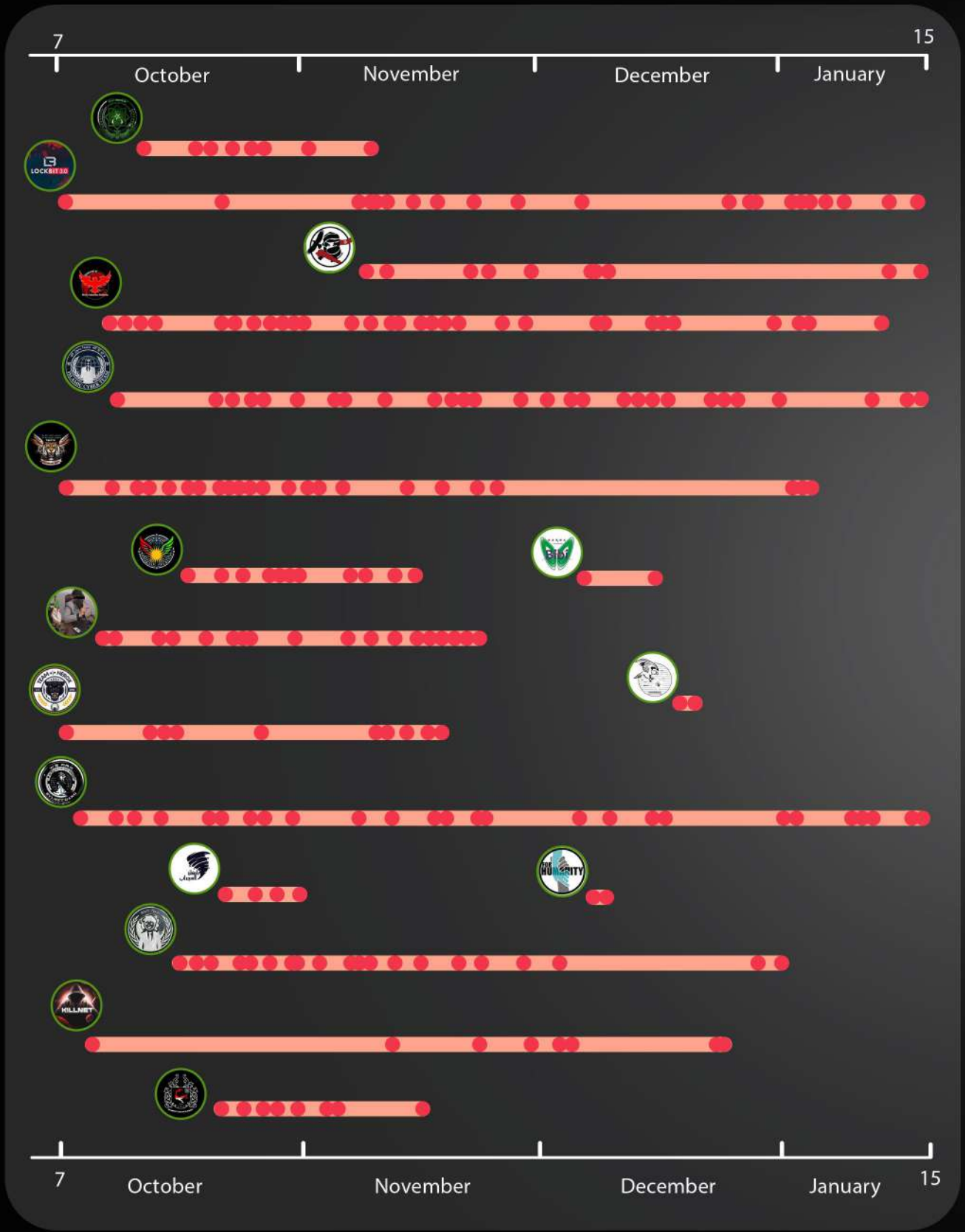
تراکم حملات حامیان غزه

تراکم حملات موثرترین گروه های هکری حامی غزه

نمودار پیش رو تراکمی از انواع حملات‌سایبری گروه های موثر در ۱۰۰روز ابتدایی نبرد طوفان‌الاقصی را نشان می دهد، نقاط قرمز بیانگر بازهٔ زمانی حملات است.



تراکم حملات گروه های موثر حامی غزه



حملات سایبری
رژیم صهیونیستی

حملات سایبری رژیم صهیونیستی و حامیان

در طول این نبرد علاوه بر رژیم صهیونیستی، برخی کشورهای دیگر نیز حضور داشتند که در این بخش به گروه‌های سایبری وابسته به آنها اشاره می‌شود.

آمار کلی حملات رژیم صهیونیستی

نام گروه‌های سایبری رژیم‌صهیونیستی

- WERedEvil
- Termux
- ICD – Israel Cyber Defense
- Silencers of Evil

نام گروه‌های سایبری با پرچم‌احتمالی آمریکا

- Predatory sparrow (گنجشک درنده)

نام گروه‌های سایبری با پرچم‌احتمالی هند

- DARK CYBER WARRIOR
- Team Ucc
- kerala cyber thunuders
- BlackDragonSec
- Indian Cyber Force
- Indian Cyber Sanatani

نام گروه‌های سایبری با پرچم‌احتمالی اوکراین

- glory sec

نام گروه‌های سایبری ضد ایران

- ARVIN
- Opiran

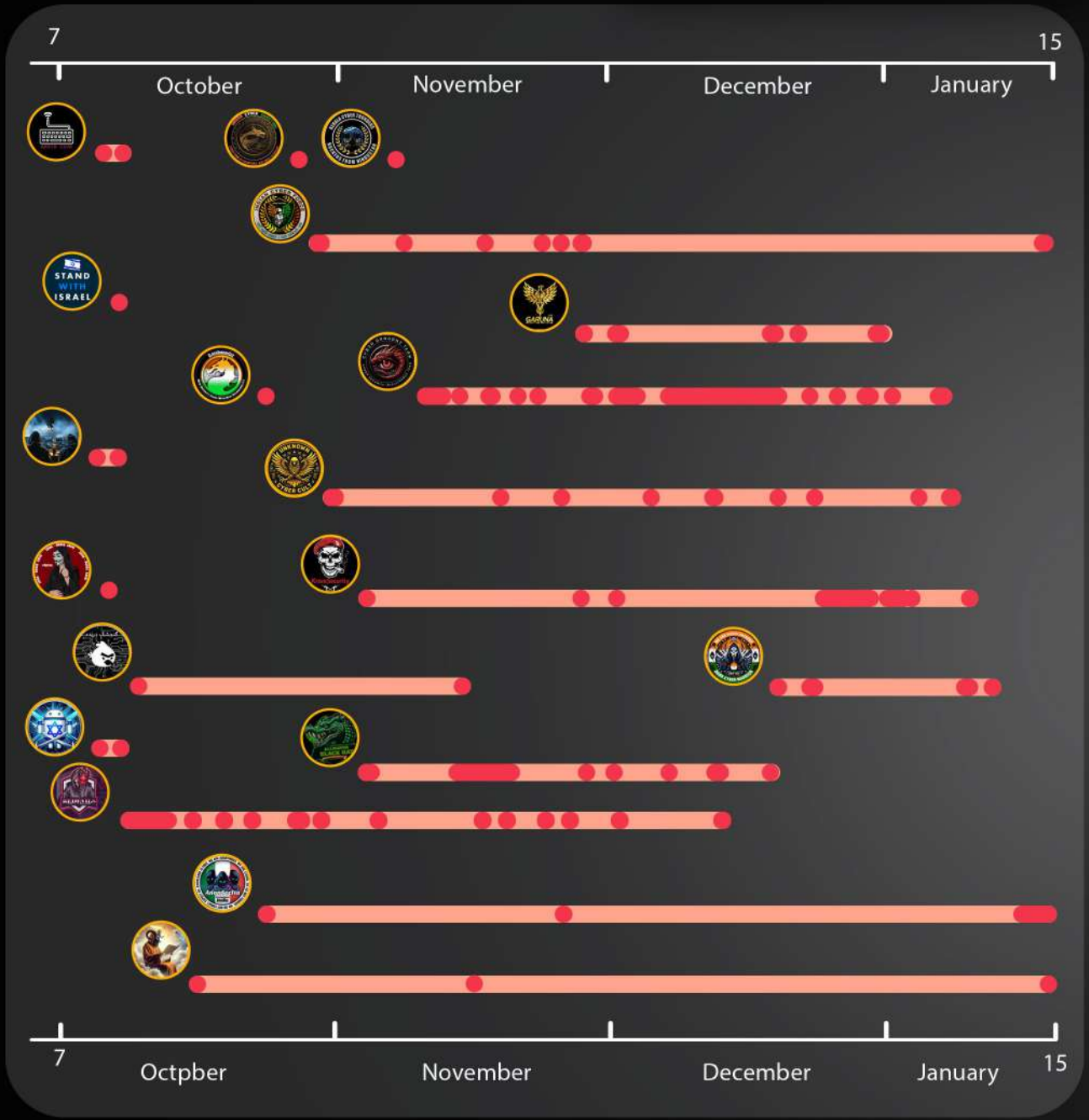
نام گروه‌های سایبری با پرچم‌احتمالی ایتالیا

- Anonymous Italia

نام گروه‌های سایبری حامیان ناشناس رژیم‌صهیونیستی

- ALIGATOR BLACK HAT
- Garuna ops
- KromSec
- Cyb3r DragOnz Team

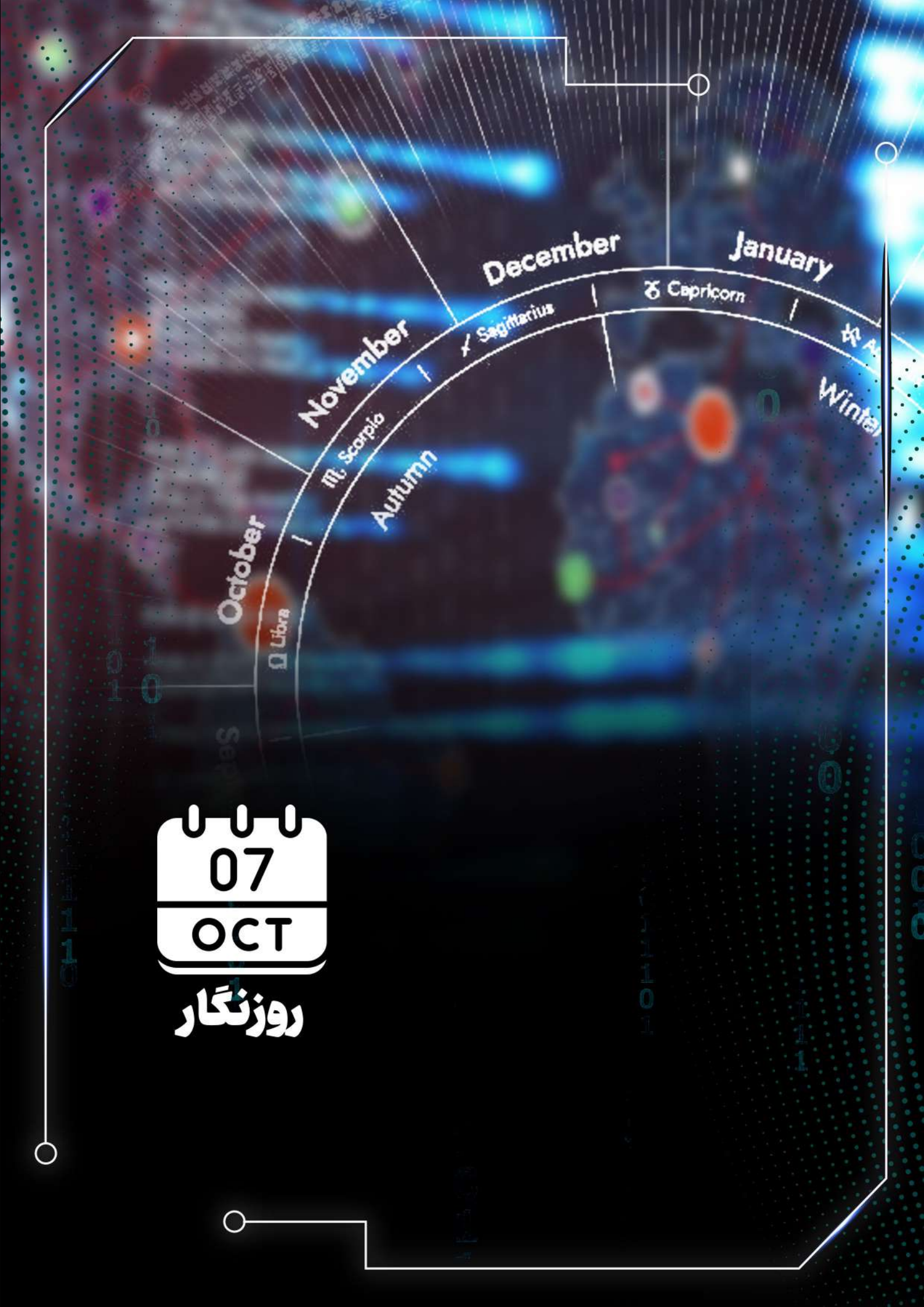
تراکم حملات گروه های حامی رژیم صهیونیستی



از تاریخ ۷ اکتبر۲۰۲۳ الی ۲۰ ژانویه ۲۰۲۴ بازهٔ زمانی حملات گروه‌های حامی رژیم‌صهیونیستی در نمودار بالا نشان داده شده است.

طبق آمار فوق گروه‌های هکری رداویلز،گنجشک درنده و ترموکس مهم‌ترین حملات را علیه حامیان غزه انجام دادند.

گروه‌های هکری آنانیموس ایتالیا و ترموکس نیز بیشترین بازهٔ زمانی حملات را در نبرد ۱۰۰ روزه را داشته و گروه هکری گنجشک‌درنده بیشترین آسیب را به حامیان غزه داشته اند.



07
OCT

روزنگار

روزنگار تراکم حملات سایبری

در این بخش به بررسی تراکم حملات‌سایبری در بازه زمانی ۷ اکتبر۲۰۲۳ الی ۱۵نوامبر ۲۰۲۴ می پردازیم. برخی از وقایع و حوادث به ویژه حملات وحشیانه رژیم‌صهیونیستی در ۱۰۰ روز ابتدایی نبرد طوفان الاقصی موجب تشدید و اوج گیری حملات سایبری در این بازه زمانی شد که در ادامه در نمودار صفحه‌ی ۲۰ به آن اشاره شده است.

حملات سایبری از ۷ اکتبر ۲۰۲۳ الی ۱۵ نوامبر ۲۰۲۴

در گزارش زیر روزهایی که تراکم بیشتری از حملات‌سایبری را داشتند با کادر زرد مشخص شده است.

OCTOBER	باج افزار	دیفیس	زیرساخت	افشای داده	هک IOT	دیداس
7	-	۱ حمله سایبری	-	۱ حمله سایبری	۱ حمله سایبری	۵۳ حمله سایبری
8	-	۱۲ حمله سایبری	۱ حمله سایبری	۸ حمله سایبری	-	۱۲۹ حمله سایبری
9	-	۲۰ حمله‌سایبری	۲ حمله سایبری	۸ حمله سایبری	۱ حمله سایبری	۱۰۸ حمله‌سایبری
10	-	۱۰۵ حمله سایبری	۲ حمله سایبری	۷ حمله سایبری	-	۱۱۳ حمله سایبری
11	-	۲۱ حمله سایبری	-	۵ حمله سایبری	۲ حمله سایبری	۵۸۸ حمله سایبری
12	-	۳۲ حمله سایبری	-	۶ حمله سایبری	-	۸۸ حمله‌سایبری
13	۱ حمله سایبری	۲۷ حمله سایبری	۲ حمله سایبری	۹ حمله سایبری	۱حمله‌سایبری	۴۹ حمله سایبری
14	۱ حمله سایبری	۷۲ حمله سایبری	۳ حمله سایبری	۱۱ حمله سایبری	۳ حمله سایبری	۱۲۶ حمله‌سایبری
15	۱ حمله سایبری	۷۲ حمله سایبری	۳ حمله سایبری	۱۸ حمله سایبری	۱ حمله سایبری	۸۳ حمله‌سایبری
16	-	۴ حمله سایبری	۱ حمله سایبری	۱۲ حمله سایبری	۱۶ حمله سایبری	۱۴۸ حمله سایبری

تعداد کل حملات:
۷: ۵۶ حمله
۸: ۱۵۰ حمله
۹: ۱۳۸ حمله
۱۰: ۲۲۷ حمله
۱۱: ۶۱۶ حمله
۱۲: ۱۲۰ حمله
۱۳: ۸۹ حمله
۱۴: ۲۱۶ حمله
۱۵: ۷۷ حمله
۱۶: ۱۵۵ حمله

OCTOBER	باج افزار	دیفیس	زیرساخت	افشای داده	هک IOT	دیداس
17 تعداد کل حملات: ۱۹۲ حمله	-	۵۳ حمله سایبری	۳ حمله سایبری	۴ حمله سایبری	-	۱۳۲ حمله سایبری
18 تعداد کل حملات: ۳۸۴ حمله	-	۱ حمله سایبری	۱ حمله سایبری	۹ حمله سایبری	۳ حمله سایبری	۳۱۳ حمله سایبری
19 تعداد کل حملات: ۴۴۶ حمله	۱ حمله سایبری	۴۷ حمله سایبری	۱ حمله سایبری	۲۱ حمله سایبری	۳ حمله سایبری	۳۹۳ حمله سایبری
20 تعداد کل حملات: ۱۷۰ حمله	-	۴۷ حمله سایبری	۲ حمله سایبری	۳ حمله سایبری	-	۱۱۸ حمله سایبری
21 تعداد کل حملات: ۲۶۵ حمله	-	۱۵۲ حمله سایبری	۱ حمله سایبری	۹ حمله سایبری	-	۱۰۳ حمله سایبری
22 تعداد کل حملات: ۱۹۷ حمله	-	۱۲۱ حمله سایبری	-	۱۰ حمله سایبری	۵ حمله سایبری	۶۱ حمله سایبری
23 تعداد کل حملات: ۱۷۳ حمله	-	۷۲ حمله سایبری	۲ حمله سایبری	۱۳ حمله سایبری	۱ حمله سایبری	۸۵ حمله سایبری
24 تعداد کل حملات: ۲۵۲ حمله	-	۸۵ حمله سایبری	-	۹ حمله سایبری	۱ حمله سایبری	۱۵۷ حمله سایبری
25 تعداد کل حملات: ۳۱۶ حمله	-	۷۸ حمله سایبری	۲ حمله سایبری	۵ حمله سایبری	۳ حمله سایبری	۲۲۹ حمله سایبری
26 تعداد کل حملات: ۱۰۷ حمله	-	۴۵ حمله سایبری	-	۷ حمله سایبری	-	۵۵ حمله سایبری
27 تعداد کل حملات: ۲۶۰ حمله	-	۹ حمله سایبری	۱ حمله سایبری	۷ حمله سایبری	۱۰۵ حمله سایبری	۱۳۸ حمله سایبری
28 تعداد کل حملات: ۹۷ حمله	-	۳۵ حمله سایبری	-	۱۴ حمله سایبری	-	۴۵ حمله سایبری
29 تعداد کل حملات: ۱۸۹ حمله	۱۶ حمله سایبری	-	-	۸ حمله سایبری	-	۱۶۵ حمله سایبری
30 تعداد کل حملات: ۲۲۲ حمله	-	۱۳ حمله سایبری	۱ حمله سایبری	۳ حمله سایبری	-	۲۰۵ حمله سایبری
31 تعداد کل حملات: ۱۱۸ حمله	۶۵ حمله سایبری	-	-	۱۲ حمله سایبری	-	۴۱ حمله سایبری

NOVEMBER	باج افزار	دیفیس	زیرساخت	نشت داده	هک IOT	دیداس
1 NOVEMBER تعداد کل حملات: ۱۸۴ حمله	-	۱۴۸ حمله سایبری	۱ حمله سایبری	۶ حمله سایبری	-	۲۹ حمله سایبری
2 NOVEMBER تعداد کل حملات: ۱۹۰ حمله	۱۰۳ حمله سایبری	-	-	۸ حمله سایبری	-	۷۹ حمله سایبری
3 NOVEMBER تعداد کل حملات: ۵۳ حمله	-	-	-	۶ حمله سایبری	-	۴۷ حمله سایبری
4 NOVEMBER تعداد کل حملات: ۴۱ حمله	-	-	-	۵ حمله سایبری	-	۳۶ حمله سایبری
5 NOVEMBER تعداد کل حملات: ۸۳ حمله	-	۱ حمله سایبری	-	-	۲ حمله سایبری	۸۰ حمله سایبری
6 NOVEMBER تعداد کل حملات: ۱۳۵ حمله	-	۱ حمله سایبری	۳ حمله سایبری	۲ حمله سایبری	۱ حمله سایبری	۱۲۸ حمله سایبری
7 NOVEMBER تعداد کل حملات: ۳۶ حمله	-	-	-	-	۱ حمله سایبری	۳۵ حمله سایبری
8 NOVEMBER تعداد کل حملات: ۲۴ حمله	-	-	-	۴ حمله سایبری	-	۲۰ حمله سایبری
9 NOVEMBER تعداد کل حملات: ۵۹ حمله	-	-	-	۳ حمله سایبری	-	۵۷ حمله سایبری
10 NOVEMBER تعداد کل حملات: ۲۴ حمله	-	-	۲ حمله سایبری	۳ حمله سایبری	-	۱۹ حمله سایبری
11 NOVEMBER تعداد کل حملات: ۲۴ حمله	-	-	-	۴ حمله سایبری	۱ حمله سایبری	۱۹ حمله سایبری
12 NOVEMBER تعداد کل حملات: ۱۵ حمله	۱ حمله سایبری	-	-	۳ حمله سایبری	۱ حمله سایبری	۱۱ حمله سایبری
13 NOVEMBER تعداد کل حملات: ۱۹ حمله	-	-	-	۲ حمله سایبری	-	۱۷ حمله سایبری
14 NOVEMBER تعداد کل حملات: ۲۸ حمله	-	-	-	۱ حمله سایبری	-	۶ حمله سایبری
15 NOVEMBER تعداد کل حملات: ۶۳ حمله	-	-	-	۳ حمله سایبری	۱ حمله سایبری	۵۹ حمله سایبری

NOVEMBER	باج افزار	دیفیس	زیرساخت	نشت داده	هک IOT	دیداس
NOVEMBER 16 تعداد کل حملات: ۷ حمله	-	-	-	۱ حمله سایبری	-	۶ حمله سایبری
NOVEMBER 17 تعداد کل حملات: ۸ حمله	-	-	۱ حمله سایبری	۱ حمله سایبری	-	۶ حمله سایبری
NOVEMBER 18 تعداد کل حملات: ۶۸ حمله	-	۲ حمله سایبری	۱ حمله سایبری	۱۵ حمله سایبری	۱ حمله سایبری	۵۴ حمله سایبری
NOVEMBER 19 تعداد کل حملات: ۹۰ حمله	-	-	-	۳ حمله سایبری	۱ حمله سایبری	۸۶ حمله سایبری
NOVEMBER 20 تعداد کل حملات: ۲۰۷ حمله	-	-	-	۳ حمله سایبری	۲ حمله سایبری	۲۰۲ حمله سایبری
NOVEMBER 21 تعداد کل حملات: ۶۹ حمله	-	-	-	۱۳ حمله سایبری	۷ حمله سایبری	۴۹ حمله سایبری
NOVEMBER 22 تعداد کل حملات: ۶۵ حمله	-	-	-	۵ حمله سایبری	-	۶۰ حمله سایبری
NOVEMBER 23 تعداد کل حملات: ۵۵ حمله	-	-	-	۱ حمله سایبری	-	۵۴ حمله سایبری
NOVEMBER 24 تعداد کل حملات: ۱۴ حمله	-	-	-	۱ حمله سایبری	-	۱۳ حمله سایبری
NOVEMBER 25 تعداد کل حملات: ۱۰ حمله	-	-	۱ حمله سایبری	۲ حمله سایبری	-	۷ حمله سایبری
NOVEMBER 26 تعداد کل حملات: ۱۴ حمله	-	-	-	۳ حمله سایبری	۱ حمله سایبری	۱۰ حمله سایبری
NOVEMBER 27 تعداد کل حملات: ۱۶ حمله	-	-	-	-	-	۱۶ حمله سایبری
NOVEMBER 28 تعداد کل حملات: ۵۰ حمله	-	-	-	-	-	۵۰ حمله سایبری
NOVEMBER 29 تعداد کل حملات: ۶۲ حمله	-	-	۱ حمله سایبری	۲ حمله سایبری	-	۵۹ حمله سایبری
NOVEMBER 30 تعداد کل حملات: ۵۲۵ حمله	-	۱ حمله سایبری	-	-	۴۹۲ حمله سایبری	۳۲ حمله سایبری

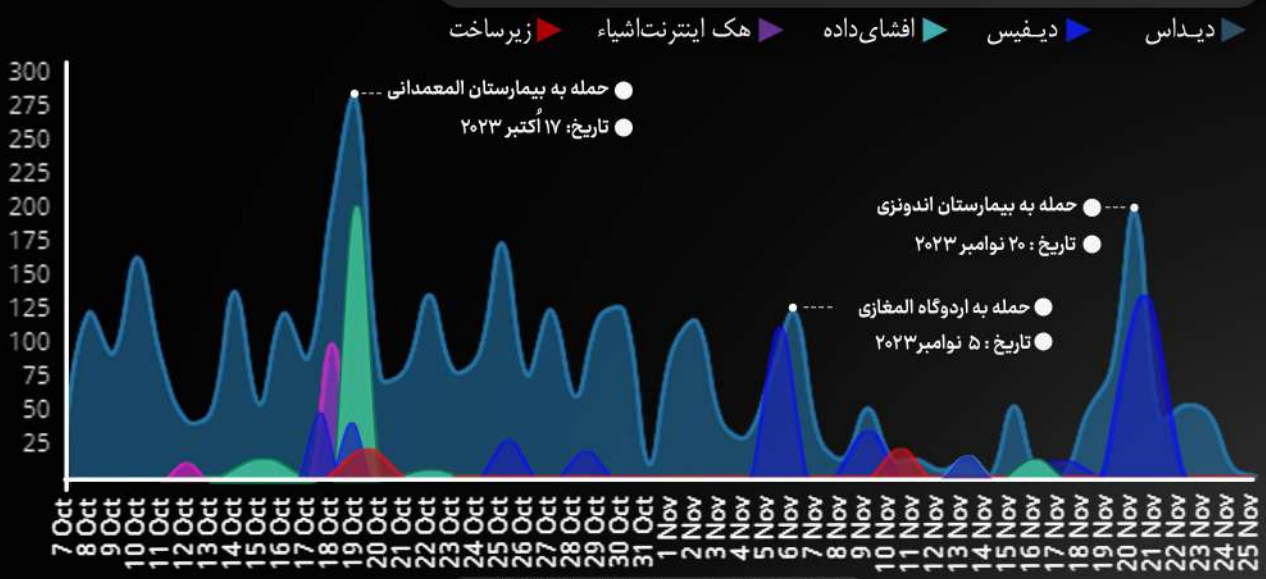
DECEMBER	باج افزار	دیفیس	صنعتی	نشت داده	هک IOT	دیداس
1 تعداد کل حملات: ۲۸ حمله	-	۳ حمله سایبری	-	۳ حمله سایبری	-	۲۲ حمله‌سایبری
2 تعداد کل حملات: ۳۸۵ حمله	-	-	۱ حمله سایبری	۵ حمله سایبری	-	۳۷۹ حمله سایبری
3 تعداد کل حملات: ۸۲ حمله	-	۷ حمله سایبری	-	۳ حمله سایبری	-	۷۲ حمله سایبری
4 تعداد کل حملات: ۱۱۲حمله	-	-	-	۱ حمله سایبری	-	۱۱۱ حمله سایبری
5 تعداد کل حملات: ۳۳ حمله	-	-	-	۲حمله‌سایبری	-	۳۱ حمله سایبری
6 تعداد کل حملات: ۲۳ حمله	-	-	-	۴حمله‌سایبری	-	۱۹ حمله سایبری
7 تعداد کل حملات: ۸۳ حمله	-	-	۱ حمله سایبری	-	-	۸۲ حمله سایبری
8 تعداد کل حملات: ۱۸ حمله	-	-	-	۱حمله‌سایبری	-	۱۷ حمله سایبری
9 تعداد کل حملات: ۱۰۳حمله	-	-	-	-	۶۸ حمله سایبری	۳۵ حمله سایبری
10 تعداد کل حملات: ۶۳ حمله	۱ حمله سایبری	۱ حمله سایبری	-	۳حمله‌سایبری	-	۵۹ حمله سایبری
11 تعداد کل حملات: ۱۳۵حمله	-	۱ حمله سایبری	-	۲ حمله سایبری	-	۱۳۲ حمله سایبری
12 تعداد کل حملات: ۲۳حمله	-	۱ حمله سایبری	-	-	-	۲۱ حمله سایبری
13 تعداد کل حملات: ۱۴۶حمله	-	۳ حمله سایبری	-	۱ حمله سایبری	-	۱۴۲ حمله سایبری
14 تعداد کل حملات: ۴۲حمله	-	۳ حمله سایبری	-	-	-	۳۹ حمله سایبری
15 تعداد کل حملات: ۱۲۸حمله	-	۲۷ حمله سایبری	-	-	-	۱۰۱ حمله سایبری
16 تعداد کل حملات: ۱۸حمله	-	-	-	۳ حمله سایبری	-	۱۵ حمله سایبری

DECEMBER	باج افزار	دیفیس	صنعتی	نشت داده	هک IOT	دیداس
17	-	-	-	۷ حمله سایبری	-	۲۱۶ حمله سایبری
18	-	۱۴ حمله سایبری	-	۲ حمله سایبری	-	۴۵ حمله سایبری
19	-	۲ حمله سایبری	-	۱ حمله سایبری	-	۱۰۷ حمله سایبری
20	۱ حمله سایبری	-	-	۶ حمله سایبری	-	۱۳۸ حمله سایبری
21	-	-	-	۱ حمله سایبری	-	۱۲۹ حمله سایبری
22	-	-	-	۱ حمله سایبری	-	۵۵ حمله سایبری
23	-	-	-	۳ حمله سایبری	-	۲۲ حمله سایبری
24	-	۷۶ حمله سایبری	-	-	۱ حمله سایبری	۳۴ حمله سایبری
25	-	۲۷ حمله سایبری	-	۲ حمله سایبری	-	۵۰ حمله سایبری
26	-	-	۱ حمله سایبری	-	-	۶۰ حمله سایبری
27	-	۲ حمله سایبری	-	-	۵۵ حمله سایبری	۴۱ حمله سایبری
28	-	۲ حمله سایبری	-	۱۵ حمله سایبری	-	۱۸ حمله سایبری
29	-	۱۵ حمله سایبری	-	۱ حمله سایبری	-	۵۷ حمله سایبری
30	-	۱ حمله سایبری	-	۴۰ حمله سایبری	۱۶۷ حمله سایبری	۵۸ حمله سایبری
31	-	۱ حمله سایبری	-	۴ حمله سایبری	-	۵۳ حمله سایبری

JANUARY		باج افزار	دیفیس	زیرساخت	نشت داده	هک IOT	دیداس
1	تعداد کل حملات: ۵۶ حمله	-	۱حمله‌سایبری	-	۱حمله‌سایبری	-	۵۴حمله‌سایبری
2	تعداد کل حملات: ۱۱۵حمله	-	-	-	۱حمله‌سایبری	-	۱۱۴حمله‌سایبری
3	تعداد کل حملات: ۳۵ حمله	-	۱حمله‌سایبری	-	-	-	۳۴حمله‌سایبری
4	تعداد کل حملات: ۳۱ حمله	۱حمله‌سایبری	-	-	۲حمله‌سایبری	-	۲۹حمله‌سایبری
5	تعداد کل حملات: ۳۲حمله	-	-	-	۱حمله‌سایبری	-	۳۱حمله‌سایبری
6	تعداد کل حملات: ۸۲ حمله	-	-	-	۷حمله‌سایبری	-	۷۵حمله‌سایبری
7	تعداد کل حملات: ۲۴ حمله	-	-	-	۲حمله‌سایبری	-	۲۲حمله‌سایبری
8	تعداد کل حملات: ۲۸ حمله	-	-	-	-	-	۲۸حمله‌سایبری
9	تعداد کل حملات: ۱۰۷حمله	-	-	-	۳حمله‌سایبری	-	۱۰۴حمله‌سایبری
10	تعداد کل حملات: ۳۹حمله	-	-	-	-	-	۳۹حمله‌سایبری
11	تعداد کل حملات: ۵۹۸حمله	-	۱حمله‌سایبری	-	۳حمله‌سایبری	۱حمله‌سایبری	۵۹۳حمله‌سایبری
12	تعداد کل حملات: ۸۱۲حمله	-	-	-	۶حمله‌سایبری	۷۳۱حمله‌سایبری	۷۵حمله‌سایبری
13	تعداد کل حملات: ۷۲حمله	-	۱حمله‌سایبری	-	۳حمله‌سایبری	-	۶۸حمله‌سایبری
14	تعداد کل حملات: ۱۲۰حمله	-	-	-	۸حمله‌سایبری		۱۱۲حمله‌سایبری
15	تعداد کل حملات: ۶ حمله	۱حمله‌سایبری	-	-	۲حمله‌سایبری	-	۴حمله‌سایبری

روزنگار حملات سایبری در نبرد ۱۰۰ روز ابتدایی طوفان الاقصی

نمودار حوادث میدانی و اوج گیری حملات سایبری در ۱۰۰ روز ابتدایی نبرد



نمودار حملات سایبری۵۰ روز اول طوفان الاقصی

نمودار حملات سایبری۵۰ روز دوم طوفان الاقصی

بررسی حوادث میدانی و اوج گیری حملات سایبری

- **۱۲ اکتبر الی ۲۱ اکتبر:** تشدید حملات‌سایبری در پی حمله وحشیانه رژیم‌صهیونیستی به بیمارستان شفاء و بیمارستان المعمدانی
- **۵ نوامبر الی ۱۱ نوامبر:** تشدید حملات‌سایبری در پی حمله رژیم‌صهیونیستی به اردوگاه المغازی
- **۱۶ نوامبر الی ۲۲ نوامبر:** افزایش حملات‌سایبری در پی حمله رژیم‌صهیونیستی به بیمارستان اندونزی و مدرسه الخوره
- **۲۸ نوامبر الی ۷ دسامبر:**

آتش‌بس موقت میان غزه و صهیونیست‌ها، تنش ایران و آمریکا در تنگهٔ‌هرمز، حمله یمن به کشتی آمریکایی و حمله رژیم‌صهیونیستی به خان یونس موجب تشدید حملات‌سایبری شد.

- **۱۷ دسامبر الی ۳۰ دسامبر:** در پی حمله گروه هکری گنجشک‌درنده به سیستم سوخت‌رسانی ایران و اختلال در پمپ‌بنزین‌ها و ترور سردار شهید سیدرضی‌موسوی در سوریه حملات‌سایبری افزایش یافت.
- **۹ ژانویه الی ۱۴ ژانویه :**

عملیات تروریستی داعش با هدایت موساد در سالگرد شهادت شهیدسلیمانی موجب افزایش حملات‌سایبری شد.

حملات زیرساخت

بررسی حملات زیرساخت

به حملاتی که زیرساخت‌های حیاتی از قبیل مراکز توزیع و تصفیه آب و فاضلاب، نیروگاه‌های تولید و توزیع‌برق، پالایشگاه و پتروشیمی، کارخانه‌های صنعتی و سامانه‌های هوشمند مدیریت شهری را از طریق سیستم‌های کنترل اتوماسیون صنعتی (اسکادا - دیسپچینگ و ...) را مورد هدف قرار می دهند، حملات زیرساختی و صنعتی می‌گویند.

کشورهای فعال

بررسی آماری حملات زیرساخت

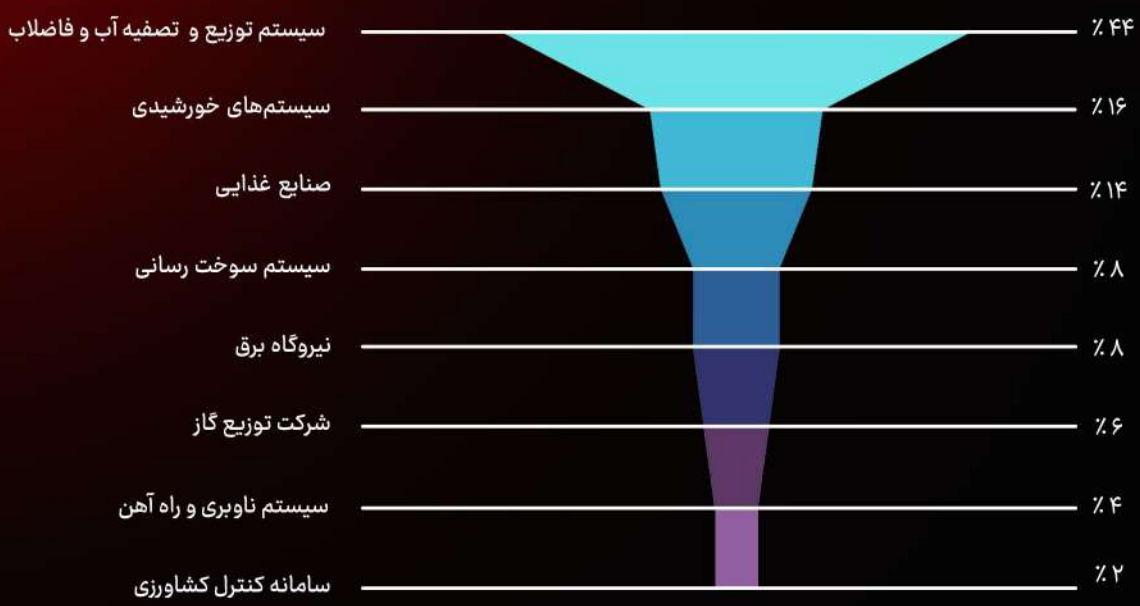
تعداد حملات زیرساخت گروه های هکری حامی غزه

تعداد حملات زیرساخت گروه های حامی رژیم صهیونیستی

- عامل بیشترین حملات زیرساخت : سایبر آونجرز
- مهم ترین هدف: رژیم صهیونیستی و آمریکا
- مهم ترین زیرساخت مورد هدف: سیستم های توزیع و تصفیه آب

بررسی آماری حملات زیرساخت

تفکیک جزئی:

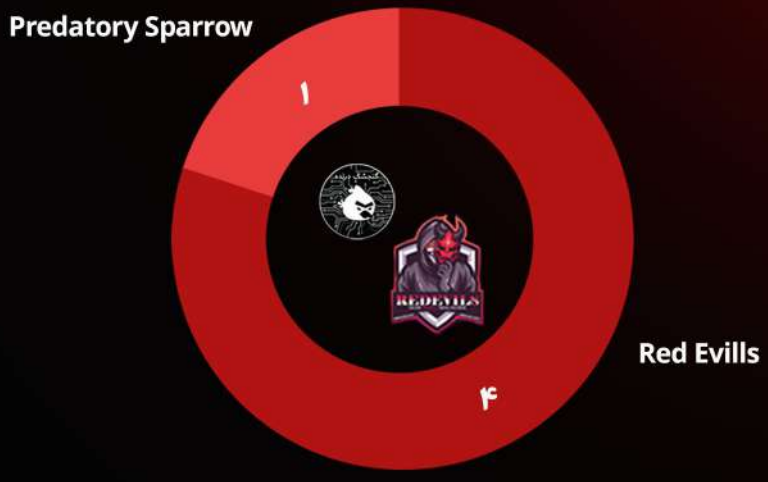


بررسی آمار تعداد حملات زیرساخت حامیان غزه

نمودار کلی حملات سایبری به زیرساخت های صنعتی رژیم صهیونیستی:

آمار حملات زیرساخت رژیم صهیونیستی و حامیان

نمودار کلی حملات سایبری به زیرساخت های صنعتی حامیان غزه:



گروه های فعال در حملات زیرساخت

- در این بخش به گروه‌های عامل حملات زیرساخت و مهم ترین اهداف آنها پرداخته شده است.

گروه‌های هکری حامی غزه

سایبر اُونجرز

تعداد کل حملات: **۱۹ حمله سایبری**

آغاز فعالیت در جنگ: **۶ اکتبر**

کشور احتمالی: **محور مقاومت**

مهم ترین حمله سایبری

حمله به سیستم های ۱۰ ایستگاه توزیع و تصفیه آب

اختلال در نیروگاه های تولید و توزیع برق

حمله به پالایشگاه و پتروشیمی

حق جویان

تعداد کل حملات: **۴ حمله سایبری**

آغاز فعالیت در جنگ: **۱۵ اکتبر**

کشور احتمالی: **ایران**

مهم ترین حمله سایبری

نفوذ به ۱ پمپ بنزین و ۴ کارگاه صنعتی

گوست سِک

تعداد کل حملات: **۳ حمله سایبری**

آغاز فعالیت در جنگ: **۱۴ اکتبر**

کشور احتمالی: **حامی غزه**

مهم ترین حمله سایبری

حمله به چند سیستم تصفیه آب کشاورزی

فورسس آف لایت

تعداد کل حملات: **۳ حمله سایبری**

آغاز فعالیت در جنگ: **۱۲ دسامبر**

کشور احتمالی: **محور مقاومت**

مهم ترین حمله سایبری

اختلال در ۳ پمپ بنزین

ابناء الصعده

تعداد کل حملات: **۲ حمله سایبری**

آغاز فعالیت در جنگ: **۱۰ نوامبر**

کشور احتمالی: **یمن**

مهم ترین حمله سایبری

کارخانه تولید آلومینیوم وابسته به صنایع نظامی

تیگ تیم

تعداد کل حملات: **۲ حمله سایبری**

آغاز فعالیت در جنگ: **۹ اکتبر**

کشور احتمالی: **حامی غزه**

مهم ترین حمله سایبری

نفوذ و تخریب سامانه مدیریت کشاورزی

کِپ تیم

تعداد کل حملات: **۲ حمله سایبری**

آغاز فعالیت در جنگ: **۹ اکتبر**

کشور احتمالی: **حامی غزه**

مهم ترین حمله سایبری

نفوذ به سیستم تصفیه آب کشاورزی

سلجرز آف سلیمان

تعداد کل حملات: **۲ حمله سایبری**

آغاز فعالیت در جنگ: **۸ اکتبر**

کشور احتمالی: **محور مقاومت**

مهم ترین حمله سایبری

نفوذ به بزرگترین کارخانه آرد و نیروگاه اشالیم رژیم صهیونیستی

غزه چیلدرن گروپ

تعداد کل حملات: **۲ حمله سایبری**

آغاز فعالیت در جنگ: **۱۸ اکتبر**

کشور احتمالی: **محور مقاومت**

مهم ترین حمله سایبری: **شرکت علوم زیستی IMBH**

سایبر واچرز

تعداد کل حملات: **۲ حمله سایبری**

آغاز فعالیت در جنگ: **۹ اکتبر**

کشور احتمالی: **حامی غزه**

مهم ترین حمله سایبری: **سامانه های کنترل کشاورزی**

دراگون فورس مالیزیا

تعداد کل حملات: **۱ حمله سایبری**

آغاز فعالیت در جنگ: **۱۵ اکتبر**

کشور احتمالی: **مالزی**

مهم ترین حمله سایبری: **اختلال در ۱ پمپ بنزین**

اسپارو کورپ

تعداد کل حملات: **۱ حمله سایبری**

آغاز فعالیت در جنگ: **۱۸ دسامبر**

کشور احتمالی: **حامی غزه**

مهم ترین حمله سایبری: **سیستم های مودباس**

الکترونیک تایگر یونیت

تعداد کل حملات: **۱ حمله سایبری**

آغاز فعالیت در جنگ: **۹ اکتبر**

کشور احتمالی: **محور مقاومت**

مهم ترین حمله سایبری: **سیستم های ناوبری و سیستم های کنترل نظارتی**

فورس الکترونیک قدس

تعداد کل حملات: **۱ حمله سایبری**

آغاز فعالیت در جنگ: **۱۵ اکتبر**

کشور احتمالی: **محور مقاومت**

مهم ترین حمله سایبری: **نفوذ به سیستم مدیریت شهری**

استاکس تیم

تعداد کل حملات: **۱ حمله سایبری**

آغاز فعالیت در جنگ: **۱۵ اکتبر**

کشور احتمالی: **مالزی**

مهم ترین حمله سایبری: **سیستم مدیریت کشاورزی**

آنانیموس سودان

تعداد کل حملات: **۱ حمله سایبری**

آغاز فعالیت در جنگ: **۷ اکتبر**

کشور احتمالی: **سودان**

مهم ترین حمله سایبری: **اختلال در ۵ سیستم کنترل صنعتی**

گروه های هکری رژیم صهیونیستی و حامیان

رد اویلز

تعداد کل حملات: **۴ حمله سایبری**

آغاز فعالیت در جنگ: **۹ اکتبر**

کشور احتمالی: **رژیم صهیونیستی**

مهم ترین حمله سایبری: **سیستم تاسیسات و ارتباطی لبنان**

پریدیتوری اسپارو

تعداد کل حملات: **۱ حمله سایبری**

آغاز فعالیت در جنگ: **۱۰ اکتبر**

کشور احتمالی: **آمریکا**

مهم ترین حمله سایبری: **سیستم سراسری توزیع سوخت ایران**


افشای داده

بررسی حملات افشای داده

در این بخش به بررسی حملات افشای‌داده می پردازیم که این نوع حملات توسط گروه‌های هکری با هدف دستیابی به انواع اطلاعات شامل داده‌های شخصی، دولتی، نظامی و ... انجام می‌گردد.
در ادامه به بررسی و داده‌کاوی ابعاد مختلف حملات افشای‌داده و گروه‌های هکری فعال در این نوع حمله‌سایبری پرداخته شده است.

کشورهای مورد هدف

بررسی آماری افشا داده

تعداد حملات افشای داده گروه های هکری حامی غزه
۵۷۷

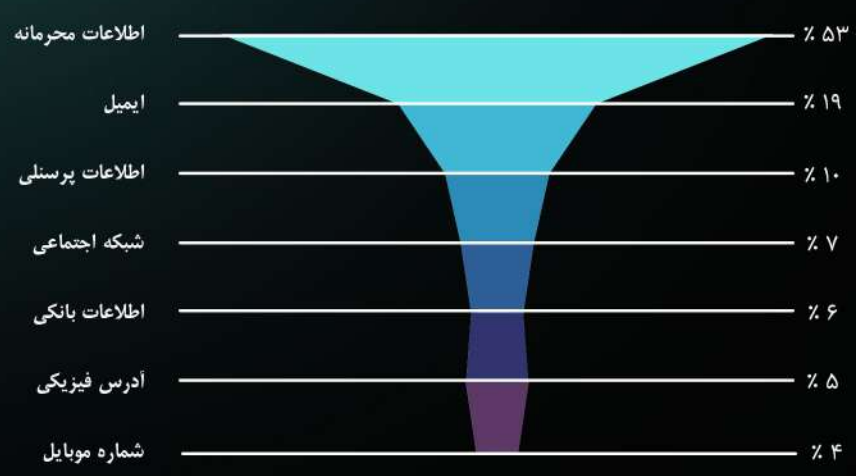
تعداد حملات افشای داده گروه های حامی رژیم صهیونیستی
۳۷

- عامل بیشترین حمله افشا داده : Ben Mhidi54
- آسیب پذیر ترین کشور: هند
- مهم ترین سازمان مورد هدف: وزارت جنگ (دفاع) رژیم صهیونیستی

بررسی آماری افشا داده

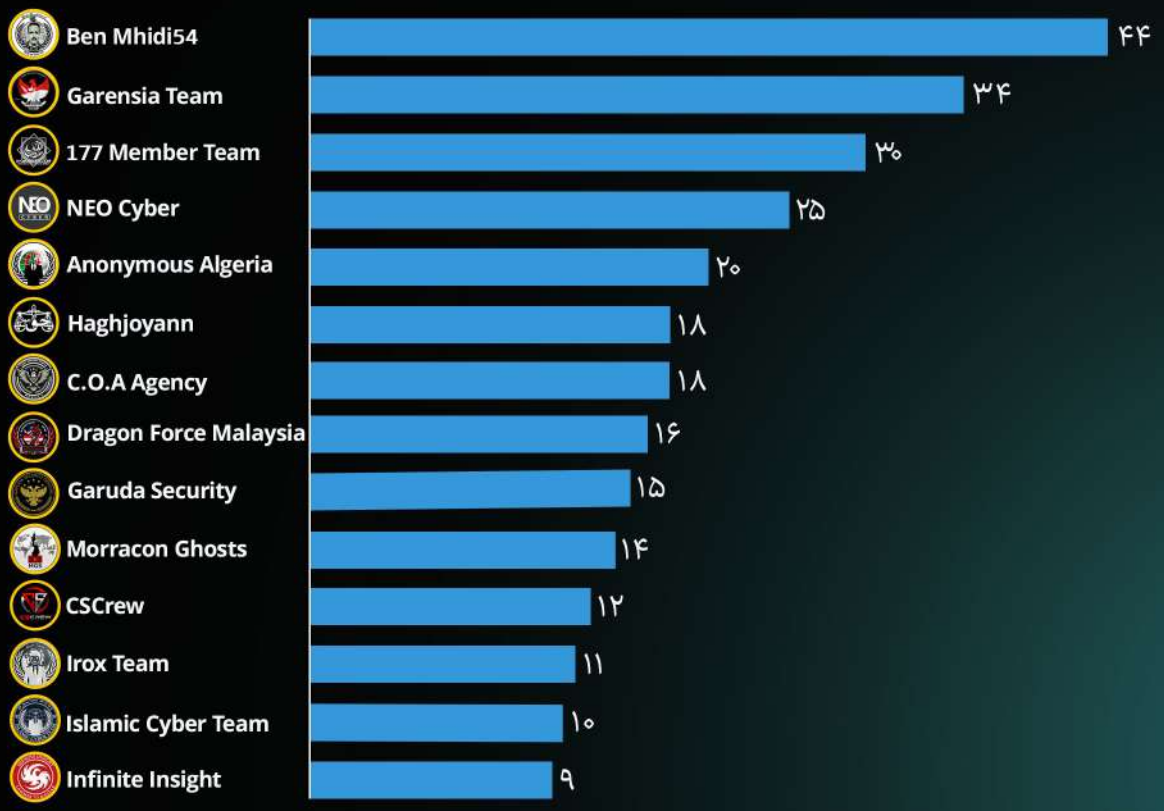
تفکیک کلی:

تفکیک جزئی:



آمار حملات افشای داده حامیان غزه

نمودارکلی حملات افشای‌داده به پایگاه‌های داده رژیم‌صهیونیستی و حامیان :



با توجه به تراکم بالای حملات افشای‌داده اسامی گروه‌هایی که کمتر از ۹ حمله‌سایبری داشته اند،به همراه تعداد حملات ذکر شده است:

گروه های عامل ۱ حمله افشای داده

Team one piece
Khalifah Cyber Crew
Cyber Cheetahs
4EXPLOITATION Channel
Black Basta
Ayyldiz Team
Kay2Pay
The Returnees
Israel Angel of Death
Jateng Cyber Team
Hacktivist Of Garuda
GB Anon17
Force Electronic Qods
Boom Security
Hacktivist Of indonesia
Cyber Flood
ACEH

گروه های عامل ۲ حمله افشای داده

Black shadow
Homeland Justice
Morrocon Deface Group
Sharp Boys
SS Cyber Team
Eagle Cyber Crew
Anonymous X
Team Insane PK
Islamic Cyber Indonatia
Gano Sec
Nothwhome Of Security
Electronic Tigers Unit
Muslim Cyber Army

گروه های عامل ۳ حمله افشای داده

Anonymous Palestine
SynixCyberCrimeMY
Ghost Of Plastine
Iranian Hacker
AHU Official
d۳ltaboys

گروه های عامل ۴ حمله افشای داده

Ghost Sec
5UL4WES1 TENG4H
Ixp666sec Team

گروه های عامل ۶ حمله افشای داده

The Anonymous BD
Morrocon Black Cyber

گروه های عامل ۷ حمله افشای داده

Anonymous Sudan
Ghost Clan Malaysia

گروه های عامل ۸ حمله افشای داده

Padang System Error
Anon Black Flag
Ixp۶۶۶sec Team
Ketapang Gray hat Team

آمار حملات افشای داده رژیم صهیونیستی و حامیان

نمودارکلی حملات افشاداده به پایگاه‌های داده غزه و حامیان غزه:


دیفیس

بررسی حملات دیفیس

به حملاتی که مهاجمین صفحات‌شخصی‌سازی شده تحت وب خود را پس از نفوذ به سرورهای اصلی سایت آپلود می‌نمایند، حملات دیفیس یا تخریب سایت می گویند.

کشورهای فعال

بررسی آماری دیفیس

تعداد حملات افشای داده گروه های هکری حامی غزه

۴۴۶۱

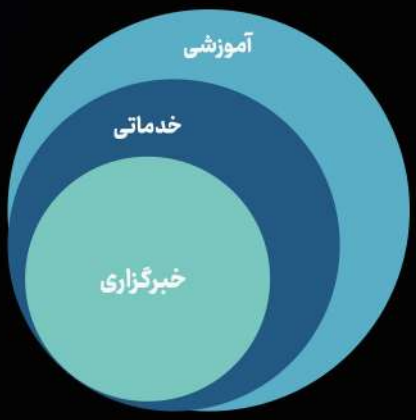
تعداد حملات افشای داده گروه های حامی رژیم صهیونیستی

۶۰

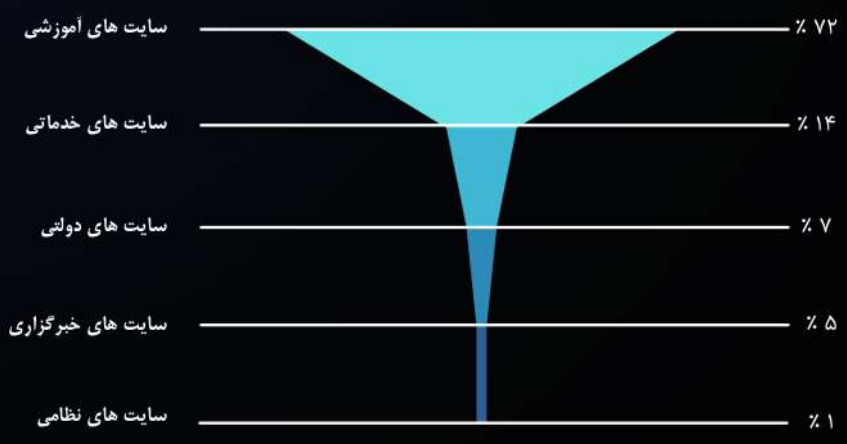
- عامل بیشترین حمله دیفیس : (CYBER ERROR SYSTEM)
- آسیب پذیر ترین کشور: هند
- مهم ترین سایت مورد هدف: بانک های رژیم صهیونیستی

بررسی آماری حملات دیفیس

تفکیک کلی:



تفکیک جزئی:



گروه های شاخص حامی غزه

سایبر ارور سیستم

تعداد کل حملات: **۱۶۵۴ حمله سایبری**

آغاز فعالیت در جنگ: **۱۲ اکتبر**

کشور احتمالی: **محور مقاومت**

مهم ترین حمله سایبری: **نفوذ به بزرگترین کارخانه آرد و نیروگاه اشالیم رژیم صهیونیستی**

حق جویان

تعداد کل حملات: **۵۴۵ حمله سایبری**

آغاز فعالیت در جنگ: **۱۵ اکتبر**

کشور احتمالی: **ایران**

مهم ترین حمله سایبری: **نفوذ به ۱ پمپ بنزین و ۴ کارگاه صنعتی**

استیم رستریشن ایگل

تعداد کل حملات: **۴۸۸ حمله سایبری**

آغاز فعالیت در جنگ: **۱۳ اکتبر**

کشور احتمالی: **اندونزی**

مهم ترین حمله سایبری: **نفوذ به ۱ پمپ بنزین و ۴ کارگاه صنعتی**

حملات دیفیس حامیان غزه

گروه های شاخص هکری رژیم صهیونیستی و حامیان

ایندین سایبر فورس

تعداد کل حملات: **۴۶ حمله سایبری**

آغاز فعالیت در جنگ: **۱۳ اکتبر**

کشور احتمالی: **هند**

مهم ترین حمله سایبری: **نفوذ به ۱ پمپ بنزین و ۴ کارگاه صنعتی**

نمودارکلی حملات افشای‌داده به پایگاه‌های داده رژیم‌صهیونیستی و حامیان :


SECURITY BRE
VIRUS DETE
باج افزار

بررسی حملات باج افزار

حمله سایبری باج افزار به روشی گفته می‌شود که در آن نرم‌افزار مخرب از طریق اجرای غیرمجاز روی سیستم قربانی، اقدام به سرقت اطلاعات، آسیب‌رسانی یا کنترل سیستم می‌کند. باج افزارها شامل ویروس‌ها، کرم‌ها، تروجان‌ها، اسپای‌ور است.
هدف اصلی مهاجمان معمولاً سرقت اطلاعات حساس یا اخاذی مالی است.

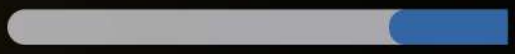
کشورهای مورد هدف

اوکراین | استرالیا | رژیم صهیونیستی | هند | آمریکا | ایران | اندونزی | الجزایر | مصر

بررسی آماری باج افزار:

تعداد حملات باج افزار گروه های هکری حامی غزه

تعداد حملات باج افزار گروه های حامی رژیم صهیونیستی



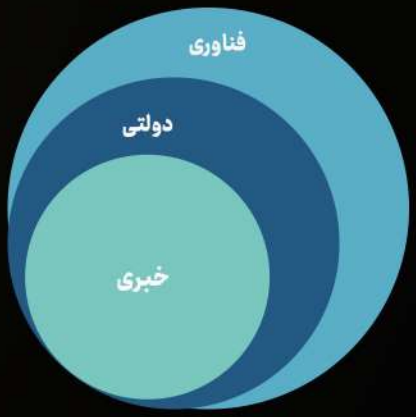
۱۴

- عامل بیشترین باج افزار: (LockBit)
- آسیب پذیر ترین کشور: مصر

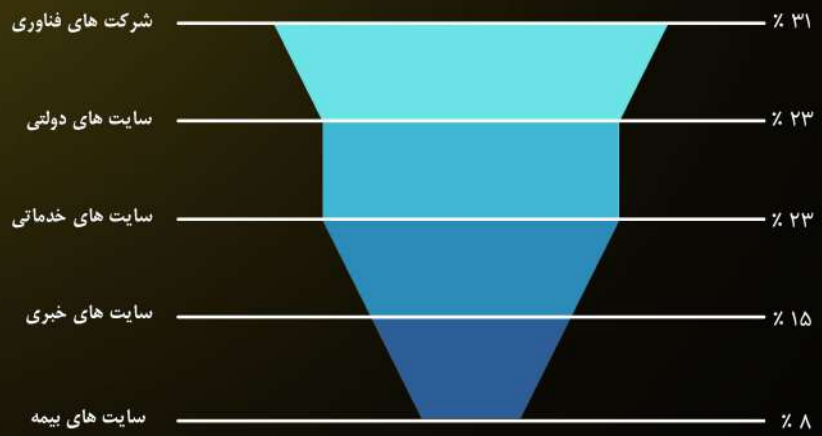
۳

- مهم ترین بخش مورد هدف: سرورهای فورتی نت بانک های مصر

تفکیک کلی:

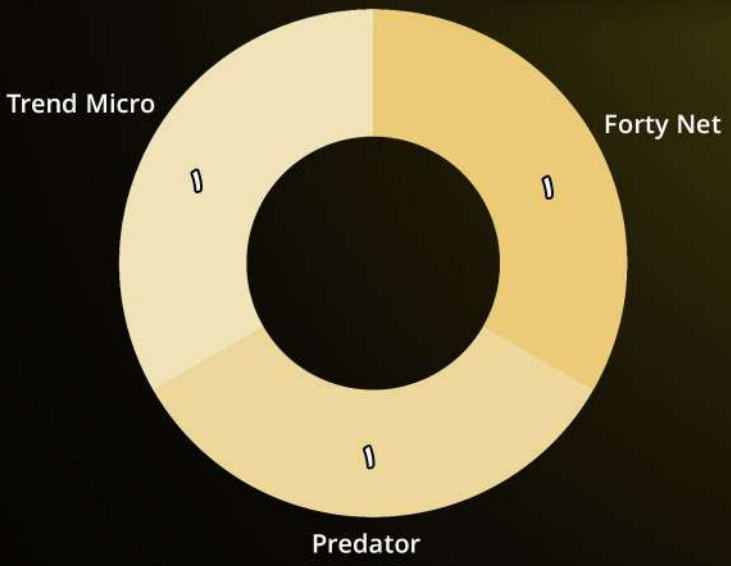


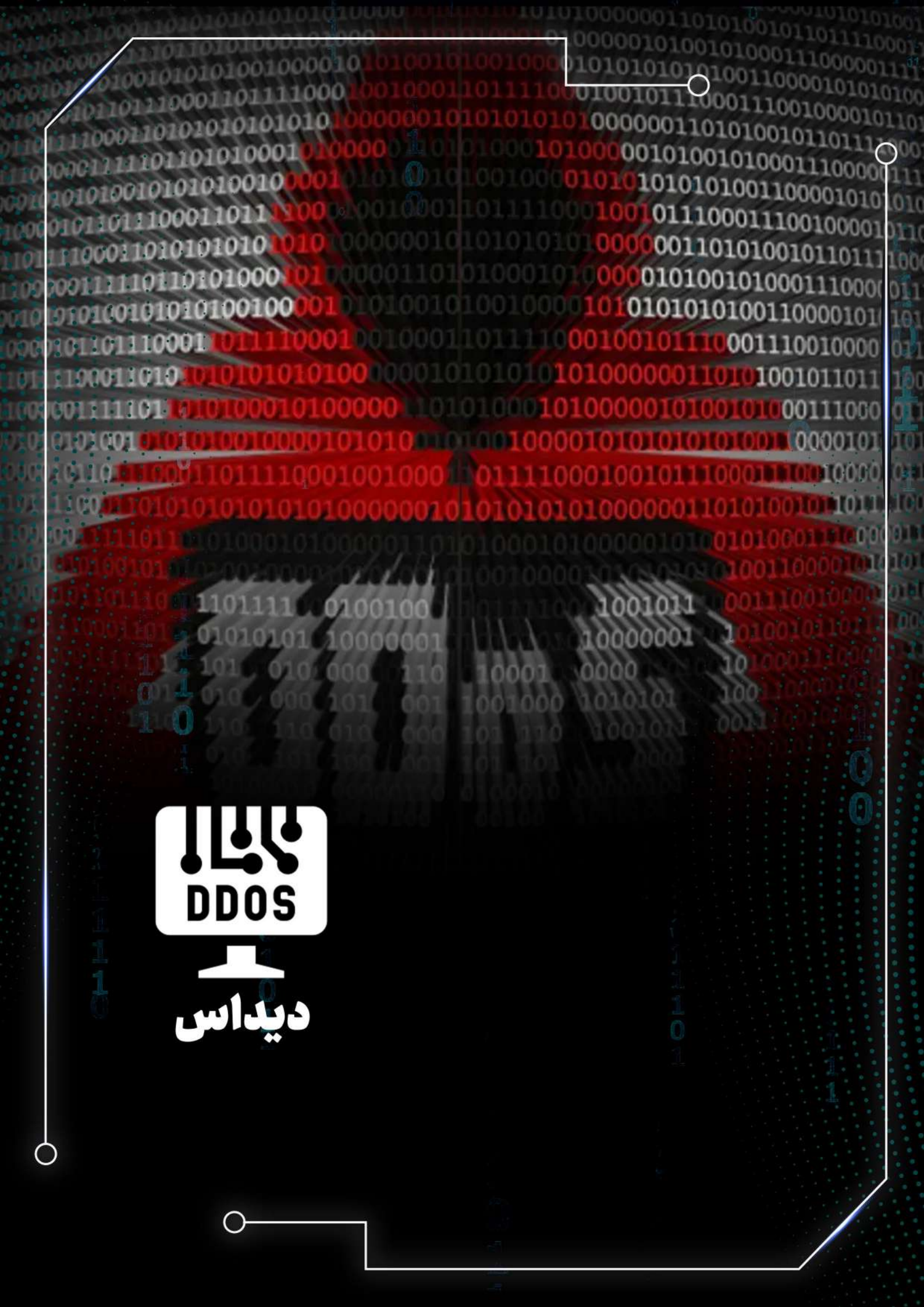
تفکیک جزئی:



بررسی آمار تعداد حملات حامیان غزه :

بررسی آمار تعداد حملات رژیم صهیونیستی و حامیان :




DDOS
دیداس

بررسی حملات منع سرویس توزیع شده (دیداس)

حملات منع‌سرویس‌توزیع‌شده (دیداس) یکی از رایج ترین انواع حملات در این جنگ‌سایبری بوده است در نمودار های پیش رو تراکم حملات دیداس در بین حامیان‌غزه و رژیم‌صهیونیستی مورد بررسی آماری قرار گرفته است.

کشورهای فعال

بررسی آماری دیداس

تعداد حملات دیداس گروه های هکری حامی غزه

۶۵۷۲

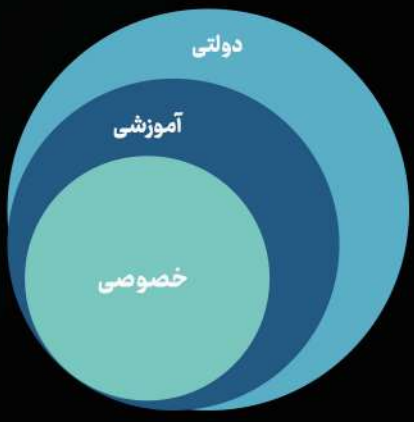
- عامل بیشترین حمله دیداس : (Neo Cyber)
- آسیب پذیر ترین هدف: رژیم صهیونیستی
- مهم ترین سایت مورد هدف: مرکز تحقیقات هسته ای رژیم صهیونیستی

تعداد حملات دیداس گروه های حامی رژیم صهیونیستی

۵۱۳

بررسی آماری دیداس

تفکیک کلی:



تفکیک جزئی:

گروه‌های شاخص رژیم صهیونیستی و حامیان:

سایبر دراگون تیم

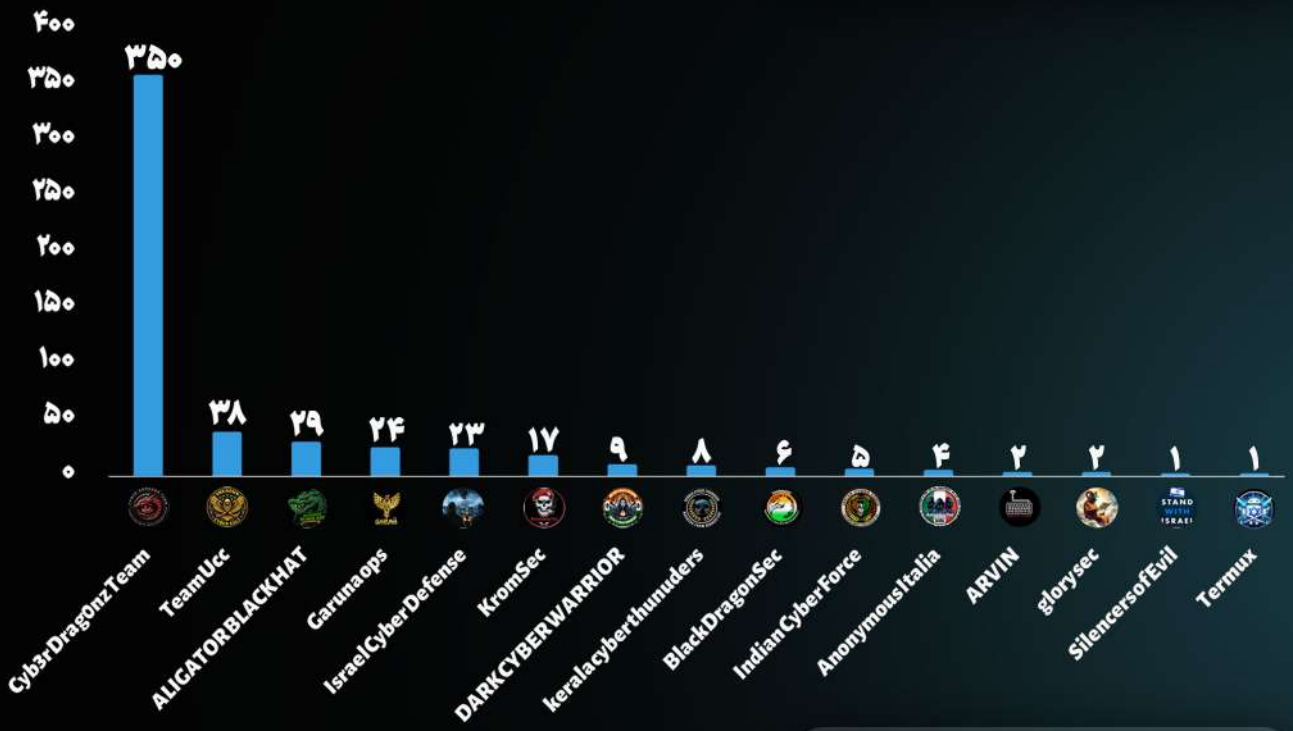
تعداد کل حملات: **۳۵۰ حمله سایبری**

آغاز فعالیت در جنگ: **۲ نوامبر**

کشور احتمالی: **حامی رژیم صهیونیستی**

مهم ترین حمله سایبری **سایت اتاق بازرگانی رژیم صهیونیستی**

حملات دیداس رژیم‌صهیونیستی و حامیان



گروه‌های شاخص حامی غزه:

با توجه به تراکم بالای حملات دیداس اسامی گروه‌هایی که کمتر از ۱۰ حمله‌سایبری داشته اند، به همراه تعداد حملات در صفحات بعد ذکر شده است:

نئوسایبر

تعداد کل حملات: **۹۸۵ حمله سایبری**

آغاز فعالیت در جنگ: **۱۱ اکتبر**

کشور احتمالی: **محور مقاومت**

مهم ترین حمله سایبری **سایت اتاق بازرگانی رژیم صهیونیستی**

آنانیموس سودان

تعداد کل حملات: **۵۵ حمله سایبری**

آغاز فعالیت در جنگ: **۷ اکتبر**

کشور احتمالی: **سودان**

مهم ترین حمله سایبری **سایت جروزالم پست رژیم صهیونیستی**

حق جویان

تعداد کل حملات: **۳۸۷ حمله سایبری**

آغاز فعالیت در جنگ: **۱۵اکتبر**

کشور احتمالی: **ایران**

مهم ترین حمله سایبری **سایت بانک های دولتی رژیم صهیونیستی**

حملات دیداس حامیان غزه

حملات دیداس حامیان غزه

گروه های عامل ۹ حمله دیداس

team 1956

گروه های عامل ۸ حمله دیداس

Nothwhome Of Security
Malasysia Cyber Defacer
LockBit
Handala
Dark Storm
DARK OLYMPUZT CREW
Cyber Flood
ALTOUFAN TEAM

گروه های عامل ۷حمله دیداس

SynixCyberCrimeMY
HostKillCrew
Hacktivist Indonesia
Devilattacks
Cyber toufan
BOOM SECURITY

گروه های عامل ۶حمله دیداس

weedsec
JAWA BARAT EROR NETWORK

گروه های عامل ۵حمله دیداس

Team R66
Homeland Justice
Aslan Neferler Tim

گروه های عامل ۴حمله دیداس

Team Insane PK
Gaza Children's Group
Electronic Tigers Unit
Blacksec

گروه های عامل ۳حمله دیداس

team 1722
khalifah cyber crew
Ghost Clan Malaysia

گروه های عامل ۲حمله دیداس

ابنا الصعده یمن
Nothwhome Of Security
GhostSec

گروه های عامل ۱حمله دیداس

StarsX Team
SkyNet
rubit
Kerala Cyber Xtractors
Jateng Cyber Team
IETHESIA
Hacktivist Of Garuda
Black Security Team
Black Magic
anonymous joe

مقام معظم رهبری:

این بلا را عملکرد خود صهیونیست‌ها بر سرشان آورد، وقتی ظلم و جنایت از حد گذشت، وقتی درنده‌خویی به نهایت رسید، باید منتظر طوفان بود.

۱۸ مهرماه ۱۴۰۲

موسسه اطلاع رسانی امورسایبری
Cyberban WorldNews Agency