تهدیدات سایبری ایران

از قتل‌عام تا جنگ؛

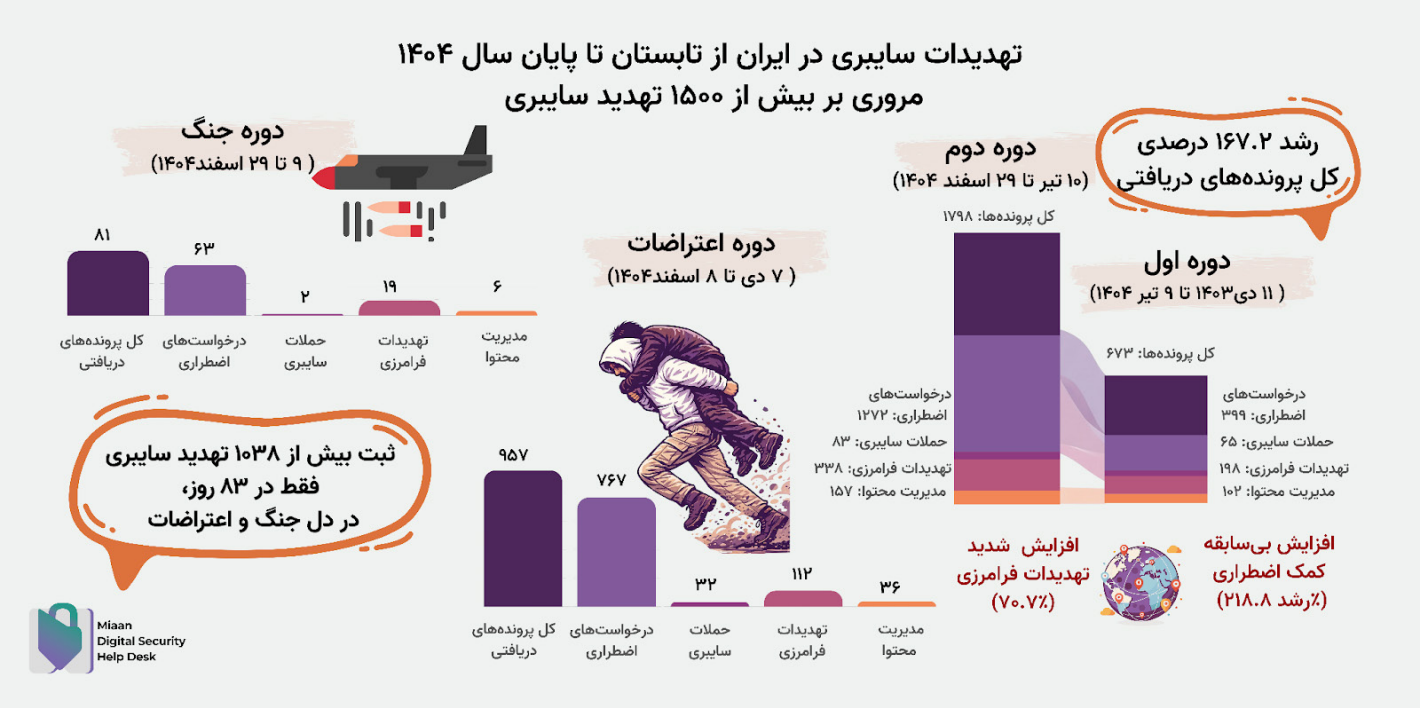
تشدید سرکوب سایبری و فرامرزی همزمان با قطع اینترنت

فروردین ۱۴۰۵

خلاصه اجرایی و روندهای کلان

گزارش سوم از مجموعه گزارش‌های تهدیدات سایبری ایران، با توجه به روند تحولات پس از اعتراض‌های دی‌ماه و تشدید تنش‌ها در پی درگیری‌های نظامی، با تاخیر منتشر شده است. با در نظر گرفتن حساسیت این بازه زمانی و ظهور الگوهای جدید، در این گزارش به‌صورت استثنایی بازه زمانی جمع‌آوری داده‌ها به دوره هشت ماهه، از یازدهم تیر ۱۴۰۴ تا اول فروردین ۱۴۰۵، گسترش یافته است. این گزارش در حالی منتشر می‌شود که حق دسترسی به اینترنت کاربران ایرانی بیش از ۲۵ روز است که در جریان جنگ اسراییل و آمریکا با ایران نقض شد.

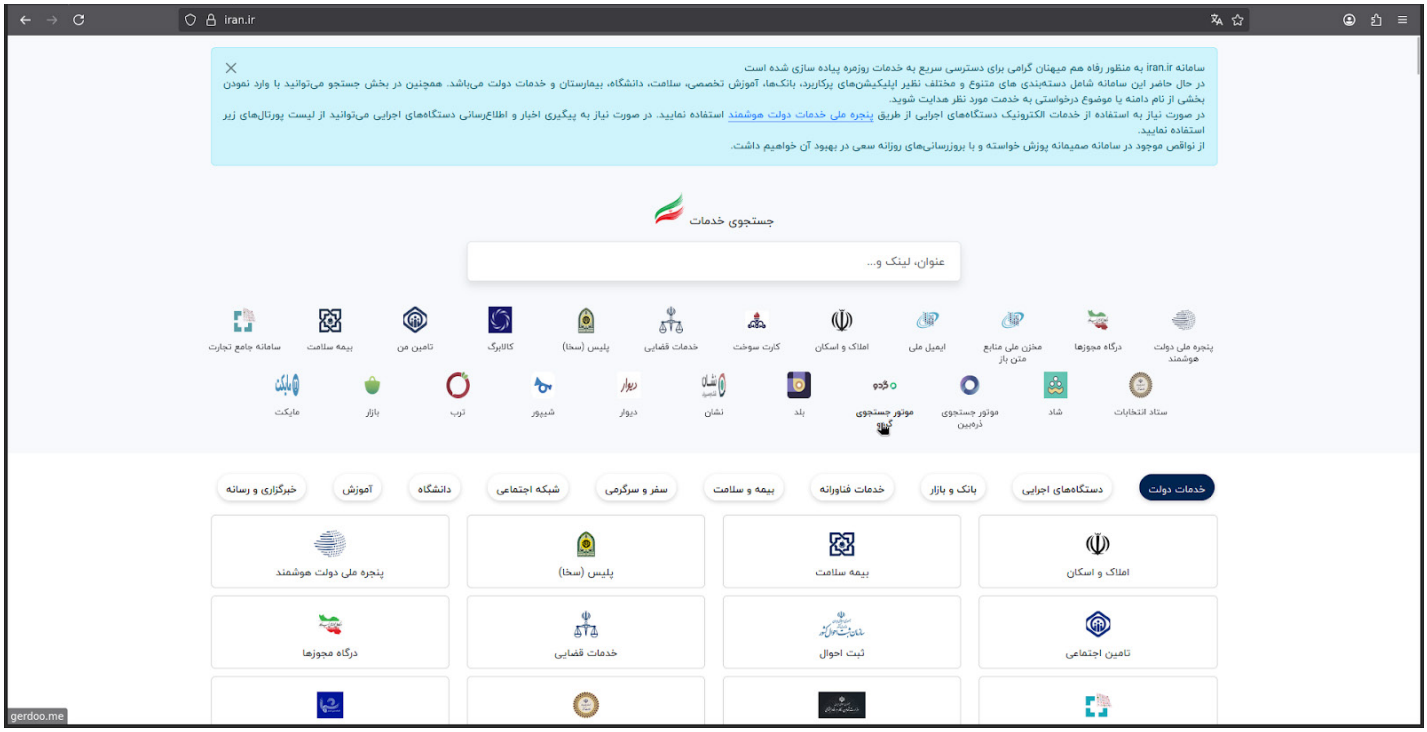
داده‌های بازه‌ی یازدهم تیر تا نهم دی‌ماه ۱۴۰۴ نشان‌دهنده تغییری پارادایمی در الگوهای سرکوب دیجیتال، به‌ویژه در بُعد فرامرزی است. در این دوره، حجم تهدیدات سایبری نسبت به شش‌ماهه پیشین ۱۵ درصد افزایش یافته است. هم‌زمان، درخواست برای دریافت مشاوره‌های امنیت دیجیتال نیز رشد چشمگیر ۶۷ درصدی را تجربه کرده؛ افزایشی که بیانگر بالا رفتن سطح نگرانی کاربران نسبت به وضعیت امنیت سایبری است، حتی در میان کسانی که لزوماً هدف مستقیم حملات قرار نگرفته‌اند. این روند نشان می‌دهد که دامنه نگرانی‌ها نه‌تنها در داخل کشور، بلکه در میان ایرانیان خارج از کشور نیز گسترش یافته است.



یکی از نقاط عطف این دوره، سرکوب گسترده دیجیتال در واکنش به اعتراضات سراسری دی‌ماه ۱۴۰۴ بود. با وجود قطعی کامل اینترنت به مدت ۱۰ روز، دامنه سرکوب دیجیتال در مرزهای ایران محدود نماند و به اشکال مختلفی از فشار و تهدید علیه کاربران و فعالان در خارج از کشور نیز تسری یافت. در همین راستا، موارد نقض حقوق دیجیتال در این ماه نسبت به بازه مشابه در سال گذشته با افزایش چشمگیر ۵۰۰ درصدی مواجه بوده است؛ افزایشی که نشان‌دهنده هم‌افزایی ابزارهای سرکوب داخلی و فرامرزی در این مقطع زمانی است.

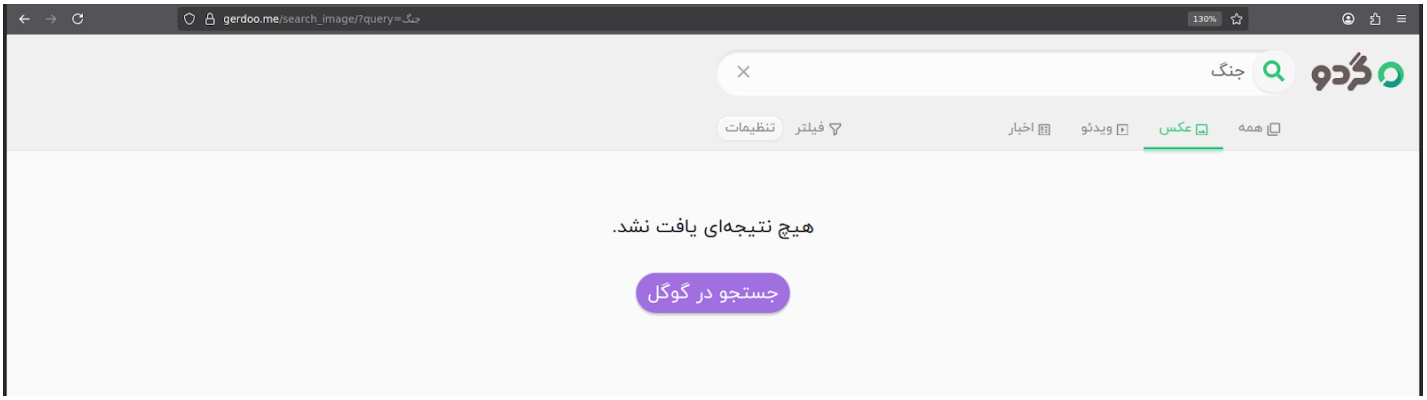
از خاموشی تا فهرست سفید: استراتژی در حال تحول کنترل اینترنت در ایران

تمام این موارد در شرایطی رخ می‌دهد که از اعتراض‌های دی ماه (اواخر دسامبر تا ژانویه) تاکنون، اینترنت در ایران به مدت بیش از ۳۹ روز قطع بوده است. تحقیقات فیلتر واچ نشان می‌دهد که با توجه به سیاست‌های جدید دولت ایران، چشم‌اندازی برای بازگرداندن اتصال اینترنت وجود ندارد. دولت به‌سرعت در حال گسترش خدمات داخلی بر بستر شبکه ملی اطلاعات (NIN) است. وب‌سایت *Iran.ir* به مرکز اصلی این وضعیت تبدیل شده و روز به روز خدمات بیشتری روی آن ارائه می‌شود.

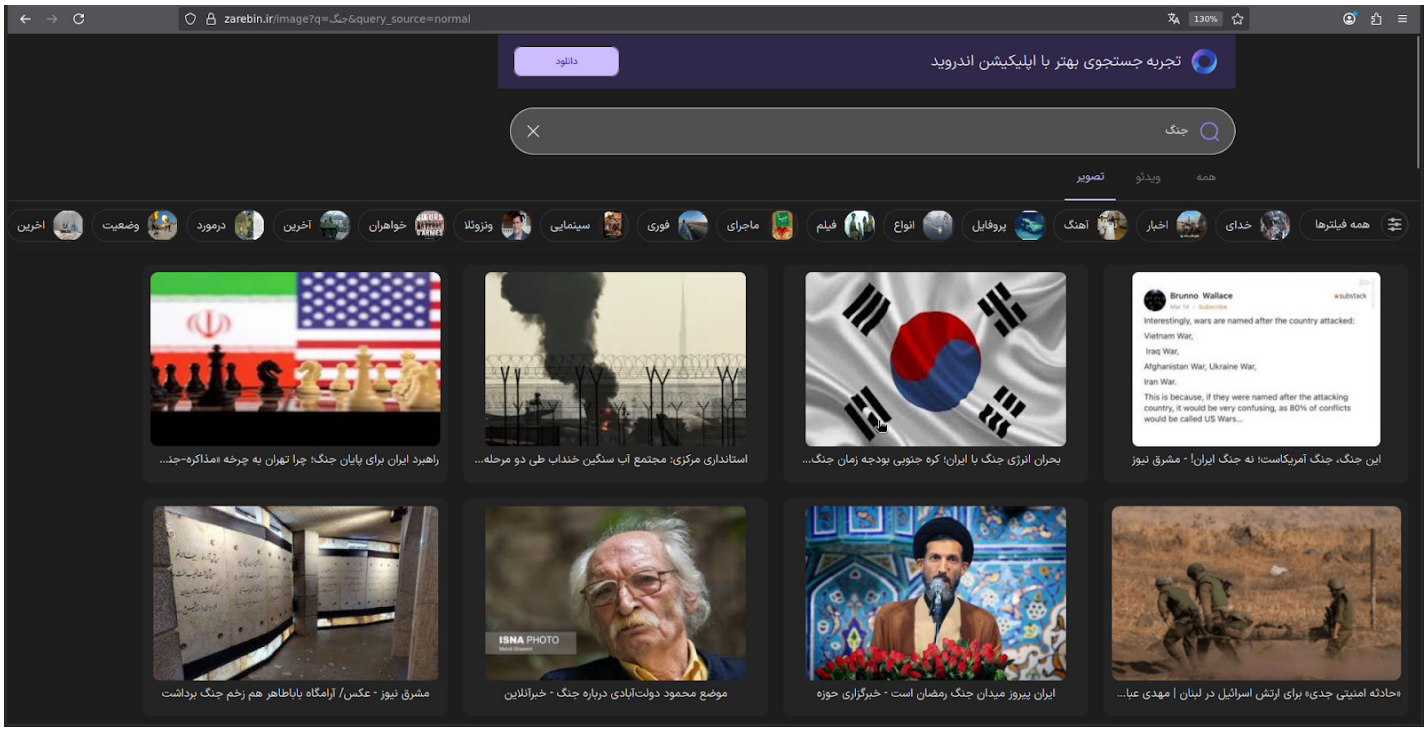


توسعه دسترسی مبتنی بر فهرست سفید همچنان ادامه دارد و این تغییر استراتژیک از سانسور سنتی به مدل فهرست سفید باعث ایجاد اثرات جانبی قابل توجهی شده است: بسیاری از خدمات داخلی یا به‌درستی کار نمی‌کنند و یا اصلاً کار نمی‌کنند. شبکه ملی اطلاعات بسیار کند است و مردم به‌طور فزاینده‌ای به سمت پلتفرم‌های داخلی سوق داده می‌شوند.

سانسور شدید بر موتورهای جستجوی داخلی و تمام پلتفرم‌های محلی اعمال می‌شود. جستجو برای کلمات کلیدی مانند «جنگ» یا «آتش‌بس» در سایت *https://gerdoo.me* هیچ نتیجه‌ای در بخش تصاویر، ویدیو یا اخبار نشان نمی‌دهد، گویا هیچ جنگی نه در ایران و نه در هیچ جای دنیا وجود ندارد.



در موتور جستجوی https://zarebin.ir، جستجوی نام «مجتبی خامنه‌ای» تنها نتایجی را نمایش می‌دهد که بر قدرت و ثروت او خارج از ایران تمرکز دارند. به همین ترتیب، جستجوی کلمه کلیدی «جنگ» محتوایی ارائه می‌کند که روایت پیروزی قاطع ایران در جنگ را نمایش می‌دهد.



هر گیگابایت دسترسی VPN که کاربران را به اینترنت متصل می‌کند—چه از طریق سرورهای فهرست سفید و چه Starlink—با قیمت بین ۱ تا ۳ میلیون تومان (تقریباً ۶ تا ۲۴ دلار آمریکا) فروخته می‌شود؛ هزینه‌ای **۵ تا ۲۰ برابر میانگین جهانی برای هر گیگابایت**، که عملاً دسترسی به اینترنت را به کالایی لوکس تبدیل کرده که بسیاری از مردم توان پرداخت آن را ندارند.

همزمان، قیمت بسته‌های اینترنت ارائه‌شده توسط اپراتورهای تلفن همراه نیز افزایش یافته است، اگرچه این ترافیک **دسترسی به اینترنت جهانی را فراهم نمی‌کند** و تنها می‌تواند برای استفاده از خدمات روی شبکه ملی اطلاعات مورد استفاده قرار گیرد.

مهم‌ترین رویدادها:

- تلاش برای فریب یک روزنامه‌نگار ساکن لندن و کشاندن او به عراق با هدف ربایش
- تلاش برای نفوذ به یک شبکه تلویزیونی حامی رضا پهلوی در لندن
- تلاش برای سرقت حساب‌های آنلاین گروهی از خبرنگاران ایرانی-آمریکایی و ایرانی-بریتانیایی در لندن و نیویورک
- تلاش برای از کار انداختن وب‌سایت یک سازمان حقوق بشری وابسته به یکی از فعالان برجسته حقوق بشر ایرانی در پاریس
- جعل هویت فعالان سرشناس حقوق بشری
- ارسال جاوا اسکریپت مخرب از طریق لینک پخش زنده تلویزیونی
- اختلال در دسترسی به MahsaAlert
- افزایش دامنه تهدیدات فرامرزی به گروه‌های فعال جامعه مدنی عراقی مخالف سیاست‌های منطقه‌ای جمهوری اسلامی
- بازداشت‌های مرتبط با استارلینک نسبتاً زیاد بوده، اما عمدتاً ناشی از رعایت‌نکردن اصول پایه امنیت ارتباطی است، نه شناسایی فنی کاربران از طریق ردیابی‌های فنی.
- کشف یک زنجیره و کمپین نسبتا بزرگ حمله سایبری با استفاده از بدافزارهای اندرویدی

در این بازه زمانی، شاهد شکل‌گیری و تشدید الگوهای پیچیده‌ای از **تهدیدات فرامرزی** بودیم که ماهیتی چند لایه و هماهنگ داشتند. این تهدیدات از حملات DDoS علیه وب‌سایت‌های فعالان برجسته حقوق بشر ایرانی، که نشانه‌هایی از بهره‌گیری از زیرساخت‌های حکومتی ایران در آن‌ها مشاهده می‌شد، آغاز شده و تا انتشار هدفمند بدافزار از طریق پلتفرم‌هایی مانند تلگرام ادامه یافت.

همچنین، استفاده از لینک‌های فیشینگ برای دسترسی غیرمجاز به حساب‌های خبرنگاران سرشناس ایرانی-آمریکایی، نشان‌دهنده تمرکز بر اهداف خارج از مرزهای جغرافیایی ایران بود. در کنار این موارد، بهره‌گیری از ابزارهای هوش مصنوعی برای تولید و انتشار اطلاعات جعلی، و نیز داکسینگ (Doxing) فعالان و ایرانیان مقیم خارج از کشور، ابعاد جدیدی به این تهدیدات افزوده است.

این اقدامات، که با تهدیدات علنی و گسترده مقامات ایرانی در رسانه‌های رسمی از جمله صدا و سیمای حکومتی همراه بوده، نشان‌دهنده شکل‌گیری یک الگوی نظام‌مند از «سرکوب فرامرزی» است؛ پدیده‌ای که به‌واسطه ترکیب ابزارهای سایبری، اطلاعاتی و رسانه‌ای، به سطحی بی‌سابقه از پیچیدگی و گستره دست یافته و آن را از نمونه‌های پیشین متمایز می‌کند.

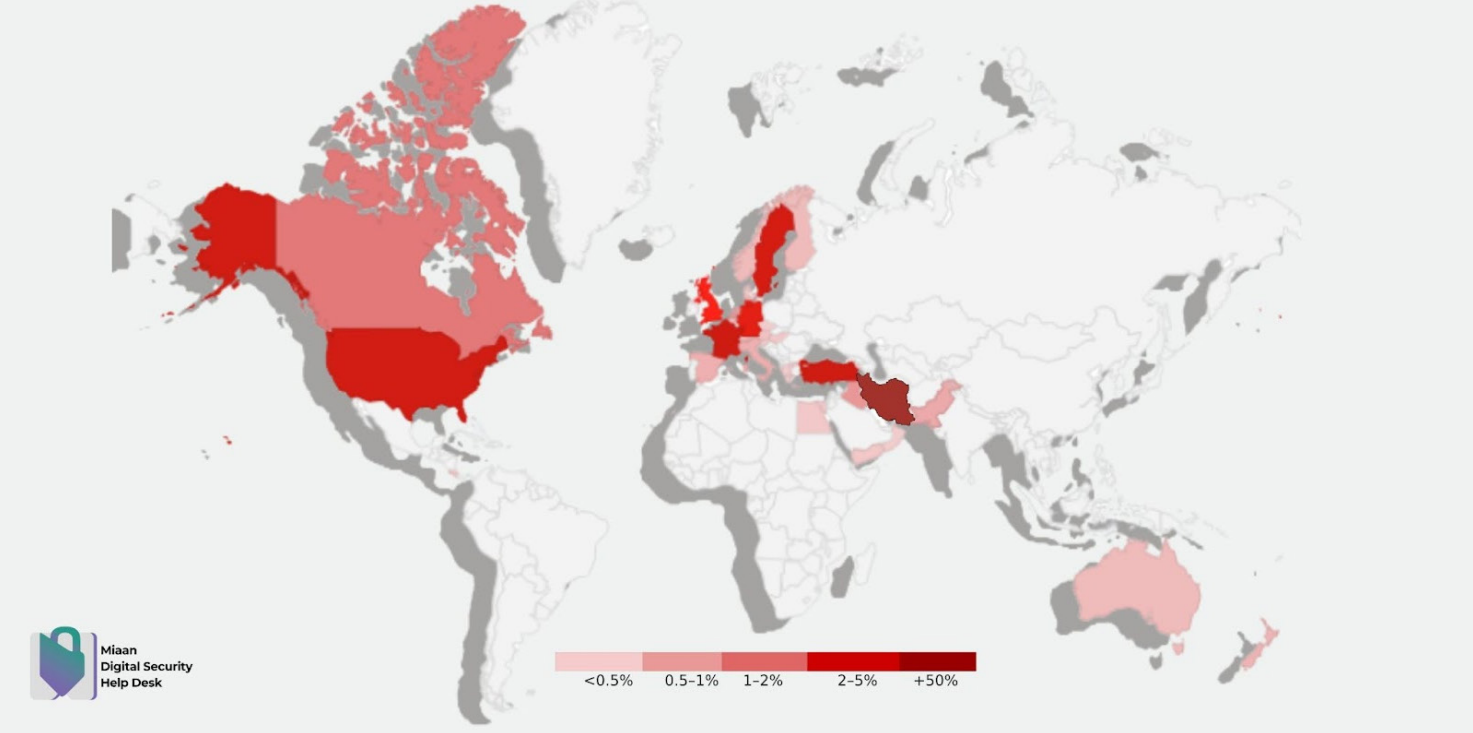
الگوی غالب حملات چنین است:

- جعل هویت پلتفرم‌های معتبر مانند Gmail، WhatsApp، Facebook، Meta و Telegram
- سوءاستفاده از زیرساخت‌های مشروع یا نیمه‌مشروع برای افزایش اعتبار حمله
- استفاده از دامنه‌های تازه‌ثبت‌شده، سرویس‌های ایمیل ابری، لینک‌های کوتاه‌شده، و دامنه‌های پوششی
- تمرکز بر فعالان، روزنامه‌نگاران، کنشگران و افراد دارای نقش عمومی یا ارتباطات حساس
- در برخی موارد، شواهد فنی یا محتوایی وجود دارد که نشان می‌دهد حملات می‌توانند با بازیگران همسو با حکومت ایران یا با استفاده از زیرساخت‌های ایرانی مرتبط باشند

سرکوب فراسرزمینی: آمار و ترندها

جمهوری اسلامی تلاش‌های خود را برای سرکوب دیجیتال از مرزهای ایران فراتر برده است. نزدیک به ۳۰٪ از تمامی پرونده‌های بازه شش ماهه ۱۱ تیر تا ۹ دی ۱۴۰۴ مربوط به فعالان مدنی دیاسپورا و خارج از مرزها بوده است.

- **نقشه توزیع اهداف فرامرزی**: کشورهای هدف به ترتیب شامل بریتانیا، آمریکا، سوئد، ترکیه، آلمان و فرانسه بوده‌اند. ترکیه (با ۳.۳٪ رشد) و بریتانیا (با ۲.۹٪ رشد) بیشترین افزایش سهم حملات را نسبت به نیمه اول داشتند، در حالی که سهم حملات در آمریکا ۲٪ کاهش یافت. با توجه به تمرکز رسانه‌های فارسی‌زبان خارج از ایران در بریتانیا می‌توان نتیجه گرفت که روزنامه نگاران به صورت فردی یا سازمانی همچنان و مانند دوره‌های پیشین در صدر اهداف جمهوری اسلامی قرار دارند. یکی از دلایل افزایش نرخ سرکوب دیاسپورا در ترکیه را نیز می‌تواند به علت افزایش نرخ مهاجرت ایرانیان به این کشور و همچنین فعال‌تر شدن دیاسپورای ایرانی ساکن ترکیه باشد.



- **گسترش دایره سرکوب**: سرکوب سایبری فرامرزی ۲۵به دیاسپورای ایرانی محدود نماند؛ ۲٪ از موارد مربوط به فعالان جامعه مدنی عراقی (مخالف سیاست‌های منطقه‌ای جمهوری اسلامی) و ۱.۶٪ مربوط به روزنامه‌نگاران افغانستانی (مخالف طالبان و جمهوری اسلامی) بود.
- **مورد ویژه**: کشف یک مورد جعل هویت برای فریب یک روزنامه‌نگار و کشاندن او به عراق جهت پیشبرد اهداف سرکوب فرامرزی.

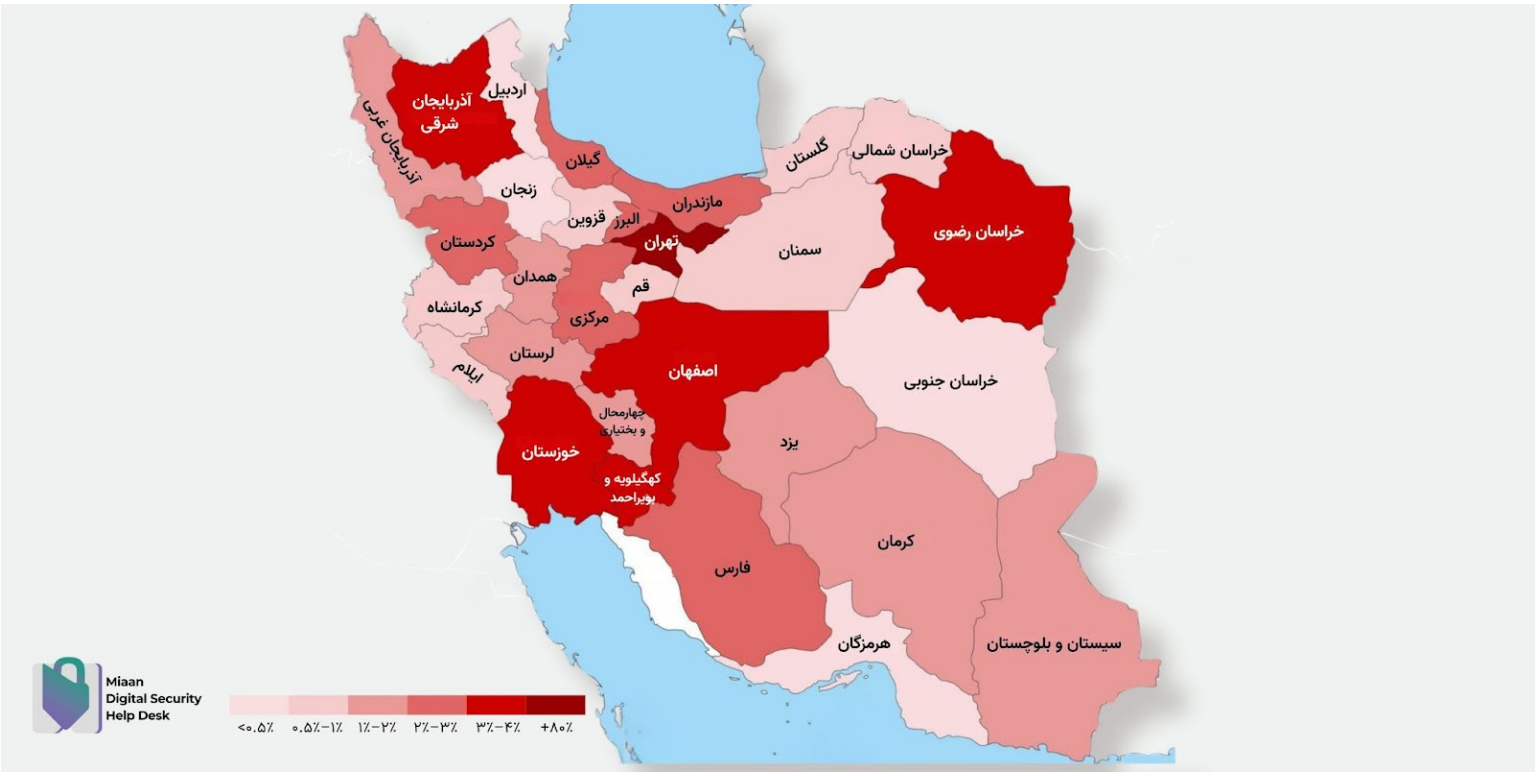
مقایسه تهدیدات فرامرزی در دوران اعتراضات و جنگ

با شروع اعتراضات دی ماه و سرکوب گسترده معترضان در ایران، سرکوب فرامرزی فعالان جامعه مدنی نیز ادامه یافت اما با چند تغییر. از ۷ دی ۱۴۰۴ ما شاهد افزایش ۱۵ درصدی ارجاع پرونده از آلمان بودیم. اگرچه در این دوره نیز انگلستان به عنوان کشور میزبان بیشترین تعداد رسانه‌های فارسی‌زبان در صدر کشورهایی بود که فعالان آن

هدف قرار گرفته بودند.

با شروع جنگ از ۹ اسفند نیز سرکوب فرامرزی متوقف نشد. اگرچه در این دوره تعداد پرونده‌های ارجاع شده از آلمان به بیش از ۲۶ درصد رسید. فعال بودن اپوزیسیون جمهوری اسلامی (جمهوری‌خواه و هواداران سامانه سلطنت) در این کشور از جمله دلایل افزایش نرخ هدف قرار گرفتن دیاسپورای ایرانی در آلمان است. در این دوره یک ساله همچنان فعالان جامعه مدنی در انگلستان نیز با رشدی دو درصدی در صدر اهداف قرار دارند.

تهدیدات داخلی: جغرافیای سرکوب در ایران

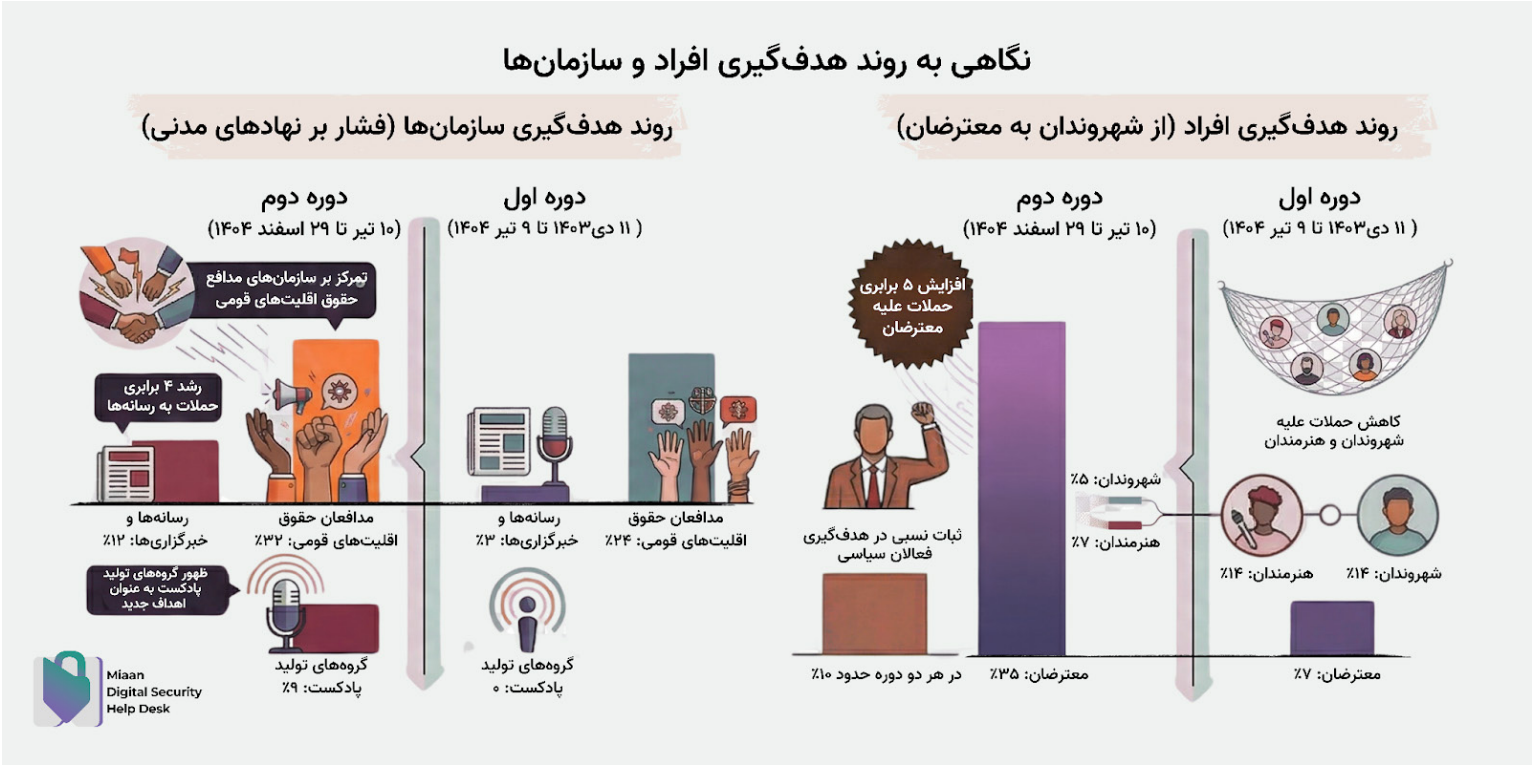


در بازه زمانی یازدهم تیر تا ۹ دی سهم تهدیدات مربوط به داخل ایران ۷۱.۶٪ از کل موارد ارجاعی بوده است (که نسبت به دوره قبل حدود ۸ درصد کاهش داشته و به سهم کشورهای دیگر مانند ترکیه و بریتانیا افزوده شده است).

- **توزیع استانی:** استان تهران با ۴۷٪ همچنان بیشترین سهم را در گزارش‌های تهدیدات سایبری دارد (هرچند ۱۲٪ کاهش نسبت به نیمه اول داشته است). پس از تهران، استان‌های آذربایجان شرقی، خوزستان، اصفهان، کردستان و سیستان و بلوچستان در رده‌های بعدی هستند. استان‌های فارس، مرکزی و خوزستان هر کدام حدود ۳٪ افزایش حملات را تجربه کرده‌اند.
- **پراکندگی در دوران اعتراضات دی و بهمن:** همزمان با آغاز اعتراضات سراسری دی‌ماه در ایران، سایت «میز کمک‌های فوری» تصمیم به تغییر سیاست گرفت و به صورت عمومی اقدام به تبلیغات کرد. این موضوع موجب شد که الگوی مراجعان نیز تغییر کند. اگرچه در دوران اعتراضات نیز بیشترین نرخ ارجاع پرونده مربوط به موارد بازداشت و ضبط دستگاه‌ها بود که با جهش قابل توجه ۷۶۳ مورد در طول تنها ۳۱ روز شد. توزیع جغرافیایی سرکوب بسیار گسترده بود (درخواست‌هایی از ۲۷ استان ثبت شد). تهران

(بیش از ۳۰٪)، اصفهان، خراسان رضوی، کهگیلویه و بویراحمد و البرز بیشترین آمار را داشتند (حدود ۳۰٪ از مراجعان نیز برای امنیت بیشتر نام استان خود را ذکر نکردند).

- **پراکندگی در دوران جنگ اسفند:** پس از حمله آمریکا و اسرائیل به ایران نیز استان تهران در صدر این فهرست قرار داشت. در این دوران اما با رشد دو درصدی تعداد پرونده‌ها از این استان نزدیک به چهل درصد از کل موارد ارجاعی را تشکیل می‌داد. پس از آن استان‌های مرکزی، اصفهان، مازندران، فارس و خوزستان و یزد قرار دارد. (بیش از ۳۲٪ از مراجعان نیز برای امنیت بیشتر نام استان خود را ذکر نکردند).
- **بازداشت خریداران استارلینک:** استفاده از اینترنت ماهواره‌ای استارلینک در جریان جنگ ۱۲ روزه جرم انگاری شد. همین موضوع دستاویزی شد تا در جریان قطعی کامل اینترنت در جریان اعتراضات دی ماه و جنگ اسفند برخورد قضایی-امنیتی با استفاده کنندگان از اینترنت ماهواره‌ای تشدید شود.
- **زمان‌بندی سرکوب سایبری:** در دوره یازدهم تیر ۱۴۰۴ تا اول فروردین ۱۴۰۵ بیش از ۲۰٪ پرونده‌ها در بازه ۱۰ تیر تا ۹ مرداد (بلافاصله پس از پایان جنگ ۱۲ روزه) متمرکز بوده‌اند که نشان‌دهنده آثار امنیتی و جنگ سایبری در این مقطع است.



- **افراد:** در بازه زمانی ۱۱ تیر ۱۴۰۴ تا اول فروردین ۱۴۰۵، با توجه به سه دوره سرکوب پس از جنگ ۱۲ روزه، اعتراضات دی‌ماه و جنگ اسفند، شاهد آن هستیم که بالاترین نرخ درخواست مربوط به امنیت حساب‌های کاربران با ۳۵٪ است. پس از آن، فعالان سیاسی (۱۱٪) قرار گرفته‌اند.
- **سازمان‌ها:** سازمان‌های مرتبط با اقلیت‌های قومی (۳۲٪) و سازمان‌های حقوق بشر (۲۱٪) در صدر اهداف سازمانی قرار داشتند. سهم رسانه‌ها با رشد چشمگیر از ۳٪ به ۱۲٪ رسید. افزایش نرخ سرکوب سازمان‌های حقوق دیجیتال در بازه زمانی ۱۰ تیر ۱۴۰۴ تا اول فروردین ۱۴۰۵، را می‌توان مربوط به دو دوره قطع اینترنت در مواجه با اعتراضات دی‌ماه و جنگ اسفند دانست. نکته قابل‌توجه، ورود گروه‌های تولید پادکست به عنوان هدف جدید است که ۹٪ حملات سازمانی را به خود اختصاص دادند.
- **مشاوره‌های امنیت دیجیتال:** در بازه زمانی یازدهم تیر ۱۴۰۴ تا اول فروردین ۱۴۰۵ دلیل عمده جهش ۶۷ درصدی درخواست‌های مشاوره، در بازه زمانی مشکلات دسترسی و امنیت حساب‌ها (به‌ویژه در

اینستاگرام و واتس‌اپ) بوده است. بسیاری از افراد به دلیل فعالیت‌های مشکوک یا تعلیق حساب‌شان (Suspend) نگران هک شدن توسط نهادهای امنیتی بودند. همچنین مسدودسازی کدهای تایید (OTP) توسط وزارت ارتباطات برای نصب سیگنال، تلگرام و کلاب‌هاوس مشکلات گسترده‌ای ایجاد کرد. در پی انتشار اخبار هک روزنامه‌نگاران (مانند ایران اینترنشنال)، موجی از درخواست‌ها برای «چکاپ امنیت دستگاه» نیز به ثبت رسید.

دسته‌بندی حملات

فیشینگ و مهندسی اجتماعی

این دسته، پرشمارترین بخش پرونده‌ها را در بازه زمانی یازدهم تیرماه تا نهم دی ماه ۱۴۰۴ تشکیل می‌دهد. فیشینگ با اختصاص حدود **۳۹٪** بیشترین سهم حملات را به خود اختصاص داده است.

- **تعداد موارد ثبت شده**: ۵۴ مورد (رشد ۴۵٪ نسبت به نیمه اول سال).
- **تکنیک غالب:** ارسال لینک‌های مخرب تحت عناوینی مانند «نظرسنجی جشنواره هنری» یا «اخطار نقض کپی‌رایت متا» در دایرکت اینستاگرام.
- **نرخ موفقیت:** ۳۸٪ از قربانیان روی لینک‌ها کلیک کرده‌اند.

۱. جعل هویت پلتفرم‌ها و برندهای معتبر: در چندین مورد، مهاجمان خود را به جای تیم‌های پشتیبانی یا حقوقی پلتفرم‌های شناخته‌شده جا زده‌اند. مهم‌ترین تم‌ها عبارت بوده‌اند از:

- هشدار حذف یا تعلیق صفحه/حساب کاربری
- ادعای نقض حق نشر یا مالکیت فکری
- درخواست «بازبینی» یا «اعتراض»
- اعلان جعلی درباره settlement یا پرداخت
- پیشنهاد شغلی جعلی از طرف WhatsApp/Meta
- پیام جعلی Gmail Confidential Mode

اهمیت این الگو در این است که مهاجم از اعتماد قبلی قربانی به برند استفاده می‌کند و بدون نیاز به پیچیدگی فنی بالا، احتمال کلیک یا پاسخ را بالا می‌برد.

۲. فیشینگ مبتنی بر تلگرام: چند پرونده روی تلگرام متمرکز بودند. روش‌های مشاهده‌شده شامل:

- پیام جعلی منتسب به تیم پشتیبانی تلگرام
- معرفی رباتی مانند @AuthenticatorBot
- تماس تلفنی از شماره‌های بین‌المللی برای تشدید فشار
- ادامه‌ی حمله در چند روز متوالی
- ساخت کانال‌های جعلی برای مشروع جلوه دادن روایت مهاجم

در یک مورد، حمله از مرحله تلاش عبور کرده و به تصرف حساب و انتقال مالکیت آن به مهاجمان رسیده است. در موردی دیگر، وجود دستگاه ناشناس روی حساب شناسایی شده است. این موارد نشان می‌دهد که تلگرام فقط بردار فریب اولیه نبوده، بلکه در برخی پرونده‌ها به بردار تصرف کامل حساب تبدیل شده است.

۳. فیشینگ رابطه‌محور و چندمرحله‌ای؛ بخشی از حملات هیچ لینک یا فایل مخربی در مرحله اول نداشتند. مهاجم صرفاً با یک پیش‌متن باورپذیر وارد گفتگو می‌شد، مانند:

- پرس‌وجو درباره یک فرد حقوقی یا یک پروژه تجاری
- دعوت به مصاحبه دانشگاهی یا همکاری علمی
- فرصت شغلی متناسب با پیشینه قربانی
- دعوت به جلسه درباره وضعیت حقوق بشر ایران

این مدل حمله به‌ویژه مهم است، چون نشان می‌دهد مهاجم لزوماً به دنبال کلیک فوری نیست، بلکه ابتدا می‌خواهد اعتماد، تعامل و پاسخ ایجاد کند و سپس در مرحله بعدی لینک، فایل، جلسه جعلی یا درخواست اطلاعات حساس را وارد کند.

۴. سوءاستفاده از زیرساخت‌های مشروع در فیشینگ: در چندین پرونده، مهاجمان از زیرساخت‌هایی استفاده کرده‌اند که از نظر فنی به‌ظاهر معتبر بوده‌اند:

- عبور موفق SPF / DKIM / DMARC
- ارسال از طریق Gmail یا Yahoo
- استفاده از Amazon SES
- استفاده از سرویس‌های کوتاه‌کننده لینک
- استفاده از دامنه‌های مشروع یا دامنه‌هایی که ظاهر سازمانی داشته‌اند

اهمیت این الگو در این است که تشخیص حمله را برای کاربر و حتی برای برخی سامانه‌های فیلترینگ دشوارتر می‌کند. در این موارد، مسئله فقط «دامنه جعلی» نیست، بلکه سوءاستفاده از زنجیره اعتماد دیجیتال است.

بدافزار

بدافزار اندرویدی

دریافت گزارش درباره فایل PDF.apk که به‌صورت مشکوک از طریق تلگرام منتشر می‌شد، در ابتدا به‌عنوان یک نمونه منفرد شناسایی شد. این فایل که ظاهری مشابه یک سند PDF داشت، نقطه شروع کشف یک زنجیره و کمپین نسبتا بزرگ حمله سایبری بود. تحلیل‌های تکمیلی نشان می‌دهد این نمونه بخشی از یک خوشه بدافزاری گسترده‌تر است و نه یک مورد تنها و منزوی. علاوه بر نمونه اولیه، چندین نمونه دیگر نیز شناسایی شدند و شواهد حاکی از آن است که احتمالا نمونه‌های بیشتری نیز وجود دارند که هنوز در کشف نشدند.

نمونه‌های شناسایی‌شده عبارت‌اند از:

- PDF.apk
- Vision-3187.apk
- PDF-977.apk
- PDF-572.apk
- Unknown-8663.apk
- PhotoAi1.0 (1).apk
- هوش مصنوعی.apk

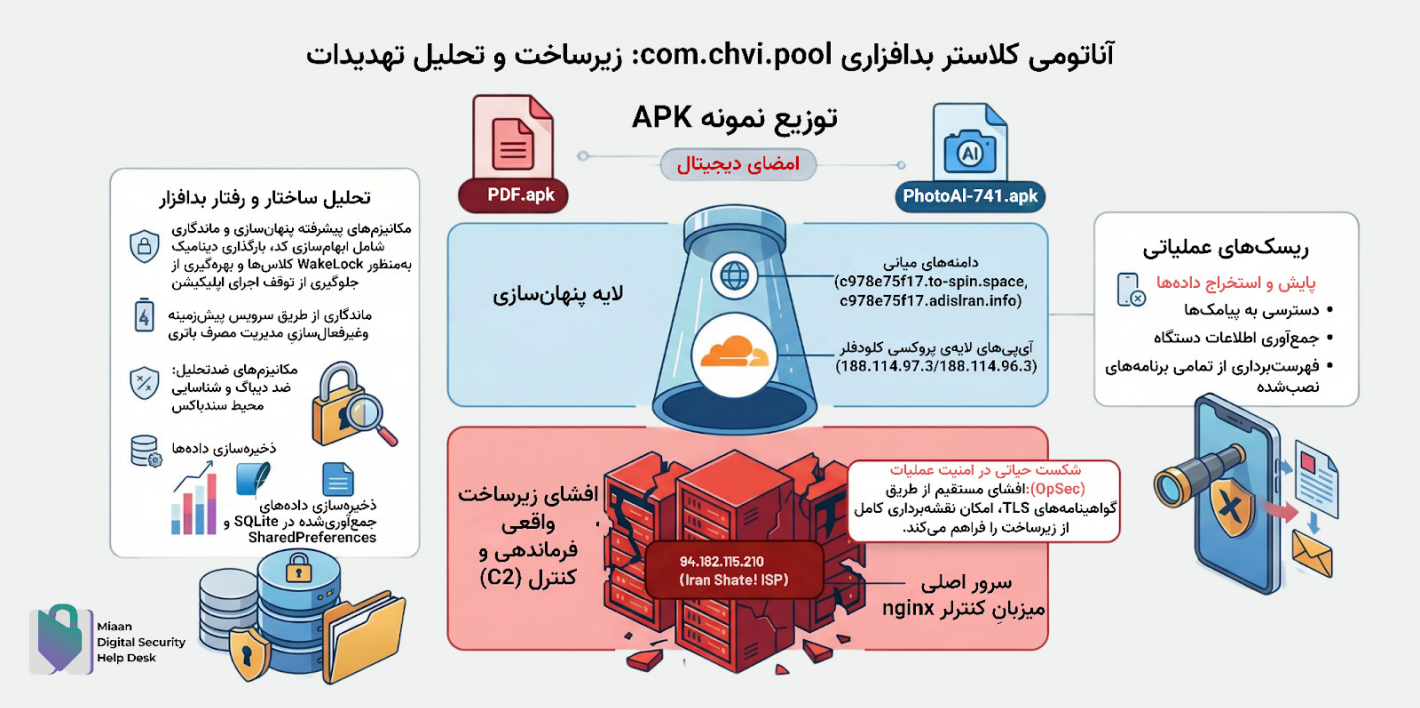
- PhotoAi-741.apk

تمامی این نمونه‌ها دارای نام بسته یکسان com.chvi.pool هستند و با سطح اطمینان بالا به یک خانواده بدافزاری واحد و یک کمپین عملیاتی مشترک که به احتمال زیاد توسط یک فرد یا گروه خاص اجرا می‌شود، تعلق دارند.

خوشه بدافزاری و همبستگی نمونه‌ها

تحلیل ساختاری و رفتاری این نمونه‌ها نشان می‌دهد که همگی بخشی از یک زیرساخت یکپارچه بدافزاری اندرویدی هستند که توسط یک عامل یا اپراتور مشترک مدیریت می‌شود. ویژگی‌های مشترک شامل:

- نام بسته یکسان (com.chvi.pool)
- رفتارهای مشابه در زمان اجرا runtime
- استفاده از الگوهای مشترک در ارتباط با سرور
- استفاده از دامنه‌ها و زیرساخت مشترک



این زیرساخت با استفاده از تکنیک‌های Domain Rotation و بهره‌گیری از کلودفلر به‌عنوان reverse proxy تلاش می‌کند تا زیرساخت واقعی فرماندهی و کنترل (C2) را مخفی نگه دارد. با این حال، تحلیل‌های تکمیلی نشان داد که در یکی از نمونه‌ها، IP واقعی backend افشا شده و امکان شناسایی زیرساخت اصلی فراهم شده است.

ویژگی‌های فنی و رفتاری

تحلیل استاتیک و داینامیک نمونه‌ها نشان می‌دهد که این بدافزارها دارای مجموعه‌ای از قابلیت‌های پیشرفته برای پنهان‌سازی، پایداری و جمع‌آوری اطلاعات هستند:

- رمزگذاری کد
- جلوگیری از تحلیل ایستا توسط ابزارهای متعارف
- بارگذاری داینامیک کلاس‌ها و استفاده از Reflection
- استفاده از Foreground Service برای ماندگاری
- ایجاد WakeLock برای جلوگیری از توقف برنامه
- بررسی معافیت از Battery Optimization
- استفاده از APIهای رمزنگاری
- شناسایی Debugger و محیط تحلیل
- جمع‌آوری اطلاعات محیط دستگاه
- فهرست‌برداری از اپلیکیشن‌های نصب‌شده
- ذخیره‌سازی داده در SharedPreferences و SQLite

در نمونه PDF.apk رفتار پنهان‌سازی آیکون برنامه نیز مشاهده شده است، به‌طوری که اپلیکیشن پس از اجرا برای کاربر نامرئی می‌شود. این رفتار در سایر نمونه‌ها نیز به‌صورت بالقوه وجود دارد، حتی اگر در محیط Sandbox فعال نشده باشد.

قابلیت نظارتی و ریسک عملیاتی

تحلیل APIها نشان می‌دهد که این بدافزارها به قابلیت‌هایی برای دسترسی به SMS inbox مجهز هستند. هرچند برخی از این رفتارها ممکن است در محیط Sandbox بیش‌برآورد شوند، اما وجود این قابلیت‌ها نشان‌دهنده پتانسیل واقعی برای:

- نظارت بر ارتباطات کاربر
- سرقت داده‌های حساس
- اجرای حملات هدفمند

بر این اساس، این بدافزارها در دسته لودر مخفی اندروید / بدافزارهای با کارکرد نظارتی قرار می‌گیرند. یعنی یک لودر پنهان با قابلیت دریافت payload ثانویه و تمرکز بر نظارت و جمع‌آوری داده.

زیرساخت فرماندهی و کنترل (C2)

تحلیل زیرساخت شبکه نشان می‌دهد که این کمپین از یک معماری چند لایه برای پنهان‌سازی backend استفاده می‌کند.

لایه اول: دامنه‌های C2

دامنه‌های زیر در نمونه‌ها مشاهده شده‌اند:

- c978e75f17.tc-spin.space
- c978e75f17.adislran.info
- c978e75f17m.cs2-go.sbs
- c5acc344.geogo.cfd

این دامنه‌ها در اغلب موارد به IPهای کلودفلر می‌رسند:

- 188.114.96.3
- 188.114.97.3

که نشان‌دهنده استفاده از کلودفلر به‌عنوان proxy layer برای مخفی‌سازی origin server است.

لایه دوم: کشف origin backend

در نمونه Pdf-812.apk و همچنین PhotoAi-741.apk، یکی از دامنه‌ها به IP زیر resolve شده است:

- 94.182.115.210

این IP متعلق به یک ارائه‌دهنده اینترنت داخلی ایران یعنی شرکت شاتل است و با احتمال بسیار بالا به‌عنوان origin backend واقعی C2 عمل می‌کند.

لایه سوم: تحلیل مستقیم سرور backend

بررسی مستقیم این IP نشان داد:

- سیستم‌عامل: Ubuntu
- وب‌سرور: nginx 1.24
- سرویس‌های فعال: HTTPS و پورت‌های غیرمعمول (7000/7001)
- استفاده از TLS 1.3 و گواهی Let's Encrypt
- مهم‌تر از همه: گواهی TLS ارائه‌شده روی این سرور متعلق به دامنه melliec.site است.

ارتباط با melliec.site

تحلیل TLS نشان می‌دهد که:

- سرور backend مستقیماً certificate دامنه melliec.site را ارائه می‌دهد
- این دامنه نیز پشت Cloudflare قرار دارد
- اما origin server همچنان به‌صورت مستقیم قابل دسترسی است

این موضوع نشان‌دهنده یک ضعف در پیاده‌سازی OpSec است، زیرا backend بدون ایزوله‌سازی کامل در معرض دسترسی مستقیم قرار دارد

رفتار reverse proxy

ارسال درخواست مستقیم به backend با Hostهای مختلف (از جمله melliec.site و adislran.info) منجر به پاسخ Bad Gateway 502 شده است. این رفتار نشان می‌دهد که:

- سرور به‌عنوان nginx (reverse proxy) عمل می‌کند
- یک backend داخلی (application layer) وجود دارد
- این backend در زمان تست:
  - یا در دسترس نبوده
  - یا فقط به درخواست‌های خاص پاسخ می‌دهد

جمع‌بندی زیرساخت

بر اساس تمامی شواهد:

- تمامی نمونه‌ها به یک زیرساخت مشترک متصل هستند.
- مهاجم از Domain Rotation و کلودفلر برای پنهان‌سازی استفاده می‌کند.
- backend اصلی در IP 94.182.115.210 متمرکز است.
- دامنه melliec.site به این backend متصل است، اما نقش دقیق آن (operational یا auxiliary) هنوز قطعی نیست.
- وجود certificate روی origin نشان‌دهنده ضعف عملیاتی در مخفی‌سازی زیرساخت است.

اهمیت و پیامدهای امنیتی

این خوشه بدافزاری نشان می‌دهد که تهدیدها از سطح فیشینگ ساده فراتر رفته و به سطح compromise کامل دستگاه رسیده‌اند.

در صورت موفقیت، مهاجم قادر خواهد بود:

- پایداری در دستگاه ایجاد کند
- اطلاعات محیطی و هویتی کاربر را جمع‌آوری کند
- قابلیت‌های نظارتی را فعال کند
- payloadهای ثانویه دریافت و اجرا کند

در نتیجه، این کمپین را باید یک تهدید با ریسک بالا، توان جاسوسی در نظر گرفت که می‌تواند علیه کاربران هدفمند، به‌ویژه در محیط‌های پرریسک، مورد استفاده قرار گیرد.

حملات مبتنی بر مرورگر و وب

اجرای جاوا اسکریپت مخرب از طریق سایت پخش زنده: در یک پرونده، یک وب‌سایت پخش زنده صدا و سیمای جمهوری اسلامی به‌عنوان نقطه ورود استفاده شده و بدون نیاز به تعامل اضافی کاربر، مرورگر به دامنه‌های مخرب متصل شده است. در جریان اعتراضات دی ۱۴۰۴ و پس از قطع کامل اینترنت بین‌الملل و اینترانت، لینک پخش زنده شبکه شش سیما به صورت انبوه به روزنامه نگاران دیاسپورا ارسال شد تا با توجه به قطع کامل تمامی مسیرهای اطلاع رسانی از طریق قطع اینترنت، آن‌ها را به کلیک برروی آن تشویق کند. این حمله برای:

- fingerprinting دستگاه
- ردیابی رفتار
- احتمال سرقت نشست
- آماده‌سازی برای فیشینگ هدفمندتر

طراحی شده بود.

اهمیت این نوع حمله در این است که کاربر حتی لازم نیست فایل نصب کند یا حتماً فرمی را پر کند؛ صرف بازدید از صفحه می‌تواند برای شناسایی، رهگیری و حملات بعدی کافی باشد.

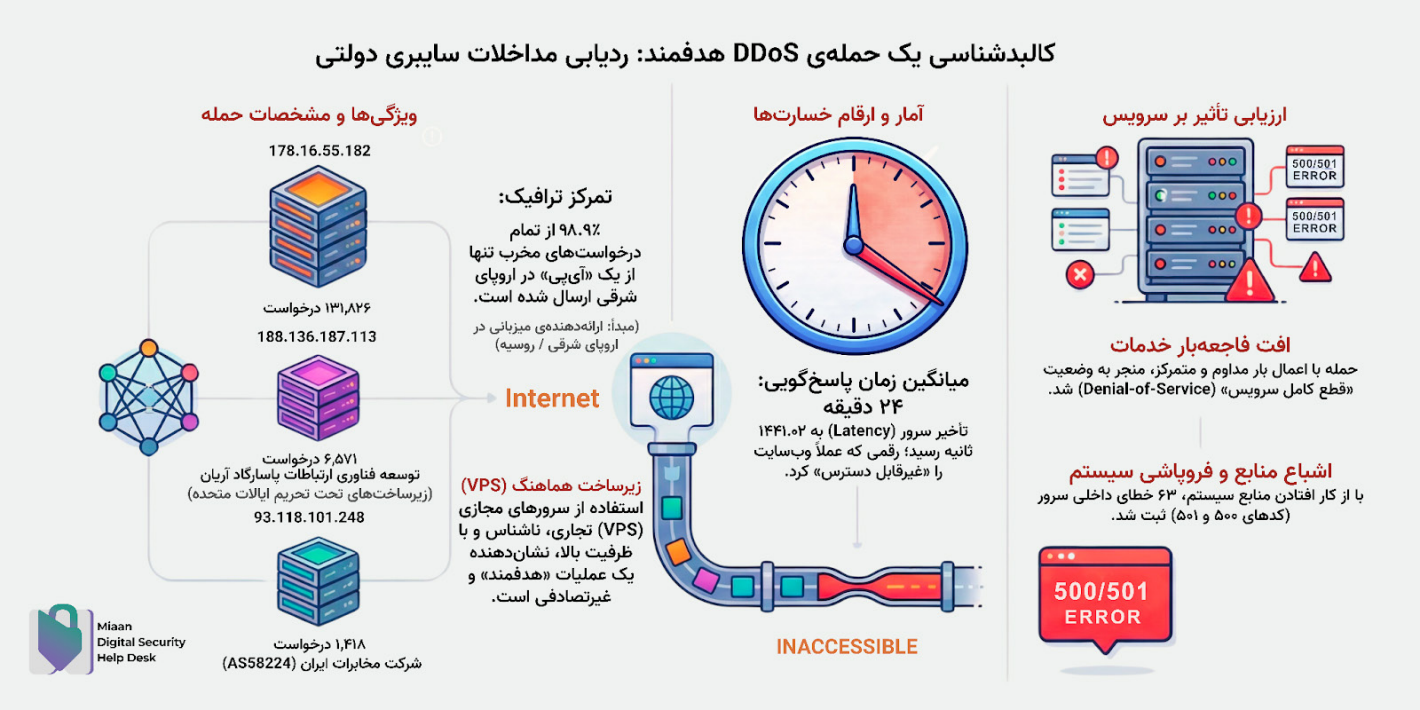
حملات اختلالی و سرکوب زیرساختی

DDoS در لایه کاربرد با نشانه‌های شناسایی و بهره‌برداری

یک پرونده مربوط به حمله شدید به وب‌سایت یک نهاد/چهره سرشناس حقوق بشری بود. این حمله صرفاً flood ساده نبود و در کنار آن مشاهده شد:

- هدف‌گیری مسیرهای سنگین مانند /xmlrpc.php
- اسکن با Nmap
- درخواست‌های غیرعادی برای یافتن ضعف
- الگوهای SQL Injection
- جعل User-Agent مرورگر عادی

بنابراین این حمله را باید ترکیبی از DDoS، شناسایی آسیب‌پذیری و تلاش برای نفوذ دانست. این حمله از آن جهت از اهمیت ویژه‌ای برخوردار است که هدف آن فقط کاهش کیفیت سرویس نبود، بلکه عملاً سانسور دیجیتال، اخلال در دسترسی به اطلاعات یک سازمان حقوق بشری ثبت شده در فرانسه، متعلق به یک فعال سرشناس حقوق بشر ایرانی و خاموش‌کردن این سازمان و بستر اطلاع‌رسانی آن‌ها بود. این حمله بار دوم نیز تکرار شد که نشان از اراده هکرهای حکومتی ایران برای خاموش کردن صدای این نهاد فرانسوی داشت.



تحلیل داده‌های ثبت‌شده نشان می‌دهد که سیستم مورد نظر در معرض یک حمله محروم‌سازی از سرویس توزیع‌شده(DDoS) قرار گرفت که منجر به اختلال شدید در عملکرد سرویس و در نهایت از دسترس خارج شدن آن برای کاربران عادی شد. ویژگی برجسته این حمله، تمرکز بسیار بالای ترافیک روی یک منبع اصلی است؛ به‌طوری که IP با آدرس 178.16.55.182 حدود ۹۸.۹ درصد کل درخواست‌های مخرب را تولید کرده است. این الگو نشان‌دهنده یک حمله متمرکز و هدفمند است، نه یک حمله پراکنده مبتنی بر بات‌نت‌های گسترده. استفاده از زیرساخت VPS پرظرفیت و ناشناس در اروپای شرقی یا روسیه نیز نشان می‌دهد که مهاجم از منابع اجاره‌ای و مقیاس‌پذیر برای اجرای حمله بهره برده است.

در کنار منبع اصلی، دو IP دیگر نیز در حمله مشاهده شده‌اند که اهمیت ویژه‌ای دارند. آدرس 93.118.101.248 به زیرساخت شرکت مخابرات ایران (AS58224) مرتبط است و آدرس 188.136.187.113 به شرکت توسعه فناوری ارتباطات پاسارگاد آریان یا فناپ (AS206065) تعلق دارد که در تاریخ ۱۶ مرداد ۱۴۰۴ توسط ایالات متحده تحریم شده است.

مشارکت این دو منبع، که به زیرساخت‌های دولتی یا نیمه‌دولتی در ایران مرتبط هستند، در حمله به این وب‌سایت یک یافته بحرانی محسوب می‌شود. این موضوع نشان‌دهنده استفاده از زیرساخت‌های حساس در کنار منابع عمومی برای ایجاد اخلال در فعالیت‌های نهادهای حقوق بشری است. این ترکیب از زیرساخت‌های ناشناس و زیرساخت‌هایی با وابستگی حاکمیتی، می‌تواند نشانه‌ای از افزایش سطح پیچیدگی در طراحی و اجرای عملیات نهادهای امنیتی در سرکوب‌های فرامرزی باشد.

از منظر اثرگذاری، داده‌ها نشان‌دهنده یک شکست کامل در عملکرد سرویس هستند. میانگین زمان پاسخ‌گویی سرور به حدود ۱۴۴۱ ثانیه (نزدیک به ۲۴ دقیقه) رسیده که عملاً به معنای غیرقابل استفاده بودن سرویس برای کاربران عادی است. در چنین شرایطی، حتی در صورت در دسترس بودن ظاهری وب‌سایت، تجربه کاربری به‌طور کامل مختل شده و دسترسی عمومی عملاً از بین می‌رود. همچنین ثبت ۶۳ مورد خطای 500 و 501 نشان می‌دهد که سرور در اثر فشار بیش از حد، دچار کمبود شدید منابع شده و توان پردازش درخواست‌ها را از دست داده است.

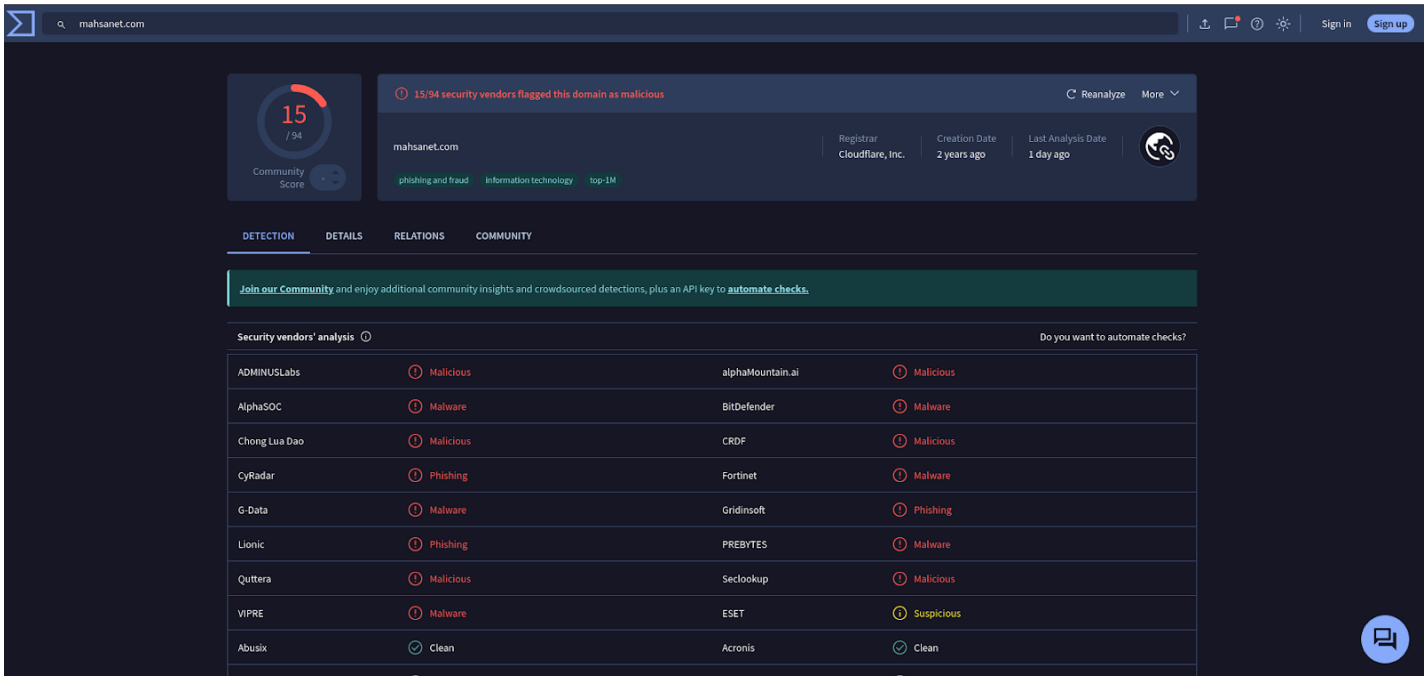
در مجموع، این حمله را می‌توان یک حمله DDoS هدفمند با تأثیر عملیاتی شدید دانست که با استفاده از ترکیبی از زیرساخت‌های اجاره‌ای و زیرساخت‌های مرتبط با نهادهای مخابراتی، توانسته است سرویس را به‌طور کامل از

کار بیندازد. تمرکز بالای ترافیک، الگوی کنترل‌شده حمله و سطح تخریب ایجادشده، همگی نشان‌دهنده یک عملیات برنامه‌ریزی‌شده و مؤثر هستند که فراتر از حملات معمول و پراکنده DDoS ارزیابی می‌شود.

حمله غیرمستقیم و مسموم‌سازی دامنه: اختلال در دسترسی به MahsaAlert

پلتفرم هشدار مردمی MahsaAlert یک سامانه اطلاع‌رسانی و نقشه‌برداری بحران است که توسط ایرانیان خارج از کشور ایجاد شده و اطلاعات مربوط به اعتراضات، دستگیری‌ها و موارد نقض حقوق بشر در ایران را منتشر می‌کند. با شروع تنش میان ایالات متحده، اسرائیل و جمهوری اسلامی ایران، این پلتفرم هشدارهای ویژه در شرایط جنگی صادر می‌کند تا از آسیب‌های جانبی و غیرمستقیم جنگ به غیرنظامیان جلوگیری کند.

پلتفرم MahsaAlert بدون هیچ نفوذ واقعی به سرور یا هک شدن، عملاً از دسترس خارج شد. تحقیقات Raznet نشان می‌دهد که فرد یا گروهی نمونه‌ای واقعی از بدافزار ویندوز (RAT) ساخته و دامنه mahsaalert.com را به‌عنوان سرور فرمان و کنترل (C2) در آن جاسازی کرده‌اند و نمونه بدافزار را در پلتفرم‌هایی مانند VirusTotal آپلود کرده‌اند. هنگامی که موتورهای امنیتی و سندباکس‌ها این بدافزار را اجرا کردند، تلاش برنامه برای اتصال به این دامنه ثبت شد و در نتیجه بسیاری از شرکت‌ها و پایگاه‌های داده تهدید سایبری، دامنه را به‌عنوان زیرساخت بدافزار علامت‌گذاری کردند.



این رویداد نمونه‌ای از حمله غیرمستقیم است: به‌جای نفوذ به سرور، مهاجم با دستکاری سیستم‌های خودکار امنیت سایبری، اعتبار دامنه را خدشه‌دار کرده و باعث شد دسترسی کاربران و شبکه‌ها به آن مسدود شود. هدف گزارش هشدار نسبت به ضعف ساختاری در سیستم‌های اطلاعات تهدید جهانی است: بسیاری از سیستم‌ها دامنه‌ها را تنها بر اساس همبستگی داده‌ها (مثل اتصال بدافزار به دامنه) مخرب می‌دانند، بدون آنکه صحت عملکرد واقعی سرور بررسی شود.

نکته اصلی این گزارش این است که این اتفاق بدون هیچ نفوذ واقعی به سرور رخ داده و تنها از طریق مسموم‌سازی اعتبار دامنه ممکن شده است.

روش‌های رایج مورد استفاده مهاجمان

در کل پرونده‌های غیرتکراری، مهم‌ترین روش‌ها چنین بودند:

- **جعل هویت:** مهاجمان خود را به جای:
  - تیم پشتیبانی تلگرام
  - Meta / Facebook / WhatsApp
  - Gmail
  - مدیر یا همکار سازمان
  - دانشگاه یا پژوهشگر
  - شرکت حقوقی یا استخدامی

  جا زده‌اند.

- **سوءاستفاده از اعتبار فنی:** در بسیاری از ایمیل‌ها:
  - SPF / DKIM / DMARC پاس شده بود
  - دامنه فرستنده یا مسیر ارسال از نظر فنی ظاهراً معتبر بود

- **استفاده از دامنه‌های تازه‌ثبت‌شده یا پوششی:** نمونه‌هایی از دامنه‌های تازه‌ثبت‌شده یا دامنه‌های فیشینگ با ظاهر حرفه‌ای دیده شد که برای:
  - جذب اعتماد
  - تقلید از سرویس واقعی
  - اجرای چندمرحله‌ای حمله

  استفاده شده بودند.

- **استفاده از سرویس‌های مشروع برای پنهان‌سازی مقصد:** از shortenerها، trackerها و سرویس‌های ابری برای مخفی‌کردن مقصد واقعی لینک و افزایش نرخ موفقیت استفاده شده است.

- **حمله چند کاناله:** در بعضی پرونده‌ها، مهاجم فقط به ایمیل یا پیام بسنده نکرده و از:
  - پیام‌رسان
  - تماس تلفنی
  - کانال جعلی
  - ایمیل تهدید

  به‌صورت ترکیبی استفاده کرده است.

- **استفاده از ضد تحلیل و بارگذاری داینامیک:** در بخش بدافزار نیز مشاهده شد که مهاجمان از:
  - رمزگذاری مانیفست
  - dynamic class loading
  - Reflection
  - domain rotation
  - زیرساخت C2 مشترک

برای دشوار کردن تحلیل و پایداری بیشتر عملیات استفاده کرده‌اند.

اهمیت و پیامدهای این حملات

۱. حملات از مرحله فریب عبور کرده‌اند: در چند مورد، نتیجه حمله فقط کلیک یا پیام نبود، بلکه به:

- تصرف حساب
- دسترسی چند روزه
- انتقال مالکیت حساب
- تهدید پس از نفوذ
- یا اختلال گسترده در سرویس

منجر شده است.

۲. اعتماد دیجیتال به‌عنوان سطح حمله هدف قرار گرفته: در این پرونده‌ها، مهاجمان نه‌فقط کاربر، بلکه اعتماد کاربر به برندها، سرویس‌های ایمیلی، لینک‌های کوتاه‌شده و زیرساخت‌های ابری را به سلاح تبدیل کرده‌اند.

۳. حملات، کارکرد سرکوب‌گرانه دارند: به‌خصوص در موارد مربوط به تلگرام، تصرف حساب، تهدید، و DDoS علیه بسترهای اطلاع‌رسانی، اثر حمله صرفاً فنی نیست. این حملات می‌توانند:

- بیان و دسترسی به اطلاعات را محدود کنند
- شبکه‌های ارتباطی را ناامن کنند
- باعث خودسانسوری یا توقف فعالیت شوند
- هزینه روانی و عملیاتی سنگینی بر قربانی تحمیل کنند

۴. ورود به سطح دستگاه، سطح تهدید را بالاتر برده است: اضافه‌شدن خوشه بدافزاری / PDF.apk Vision-3187.apk نشان می‌دهد که بخشی از تهدیدها وارد مرحله‌ای شده‌اند که در آن مهاجم دیگر فقط به دنبال credential یا session نیست، بلکه به دنبال دسترسی پایدار، پنهان و نظارتی در سطح دستگاه است.

نشانه‌های ارتباط با ایران و استفاده از زیرساخت‌های ایرانی

در همه پرونده‌ها نمی‌توان با قطعیت در مورد فرد یا نهاد حمله کننده اظهار نظر کرد. اما در چند مورد، شواهد مهمی وجود دارد که احتمال ارتباط با بازیگران همسو با جمهوری اسلامی یا استفاده از زیرساخت‌های ایرانی را تقویت می‌کند.

۱. حضور مستقیم زیرساخت‌های ایرانی در حمله DDoS: در پرونده حمله به وب‌سایت حقوق بشری، بخشی از ترافیک مهاجم از این زیرساخت‌ها آمده بود:

- AS58224 وابسته به Telecommunication Company of Iran
- AS206065 وابسته به Tose'h Fanavari Ertebabat Pasargad Arian Co. PJS

این مورد از مهم‌ترین شواهد کل مجموعه است، چون نشان می‌دهد در کنار VPSهای خارجی، زیرساخت مخابراتی داخل ایران نیز در حمله دیده شده است.

- مهاجمان از جعل هویت پلتفرم‌ها، چهره‌های دانشگاهی، مدیران سازمانی و نهادهای حقوقی

استفاده کرده‌اند.

- بخش مهمی از حملات با تکیه بر زیرساخت‌های مشروع یا ظاهراً معتبر اجرا شده‌اند.
- در چند مورد، حمله به تصرف واقعی حساب، انتقال مالکیت، و تهدید پس از نفوذ رسیده است.
- یک خوشه بدافزاری اندرویدی و یک پرونده اجرای جاوا اسکریپت مخرب نشان می‌دهد که تهدیدها به فیشینگ محدود نیستند.
- حمله DDoS با مؤلفه‌های شناسایی و تلاش برای نفوذ، نشان‌دهنده سرکوب دیجیتال در سطح زیرساخت است.
- در چند پرونده، به‌ویژه موارد مرتبط با تلگرام، حمله DDoS و بدافزار اندرویدی، نشانه‌های مهمی از ارتباط با ایران یا استفاده از زیرساخت‌های ایرانی مشاهده شده است.

در مجموع، این داده‌ها از وجود یک محیط تهدید چندلایه، تطبیق‌پذیر و در برخی موارد موفق علیه کاربران و نهادهای پرخطر فارسی‌زبان حکایت دارند.

مدیریت محتوا: جنگ روایت‌ها

ادبیات نفرت پراکنانه: در بازه زمانی یازدهم تیر تا دهم دی‌ماه کمپین‌هایی علیه فعالان سیاسی و جامعه مدنی بودیم که در پلتفرم‌های مختلف شروع به کار کرد:

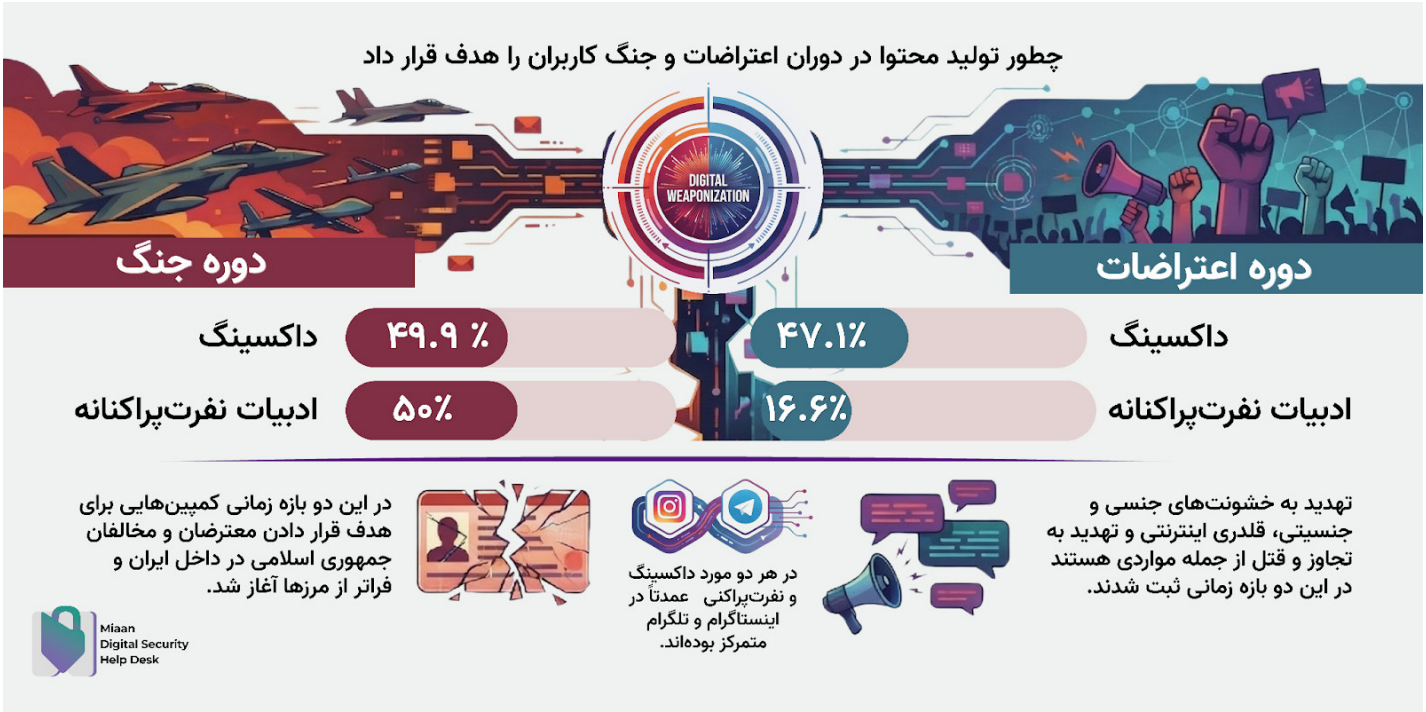
در این کمپین‌ها عموما گروهی از کاربران در شبکه‌های اجتماعی مانند توییتر یک چهره سرشناس را هدف قرار داده او به قتل یا تجاوز تهدید می‌کردند.

جعل هویت: در این روش مهاجمان هویت سازمان‌ها، رسانه‌ها یا شهروند خبرنگاران جعل می‌کردند:

- ساخت اکانت‌های جعلی در اینستاگرام یا کانال‌های جعلی در تلگرام با تغییرات جزئی در نوشتن نام به حروف لاتین

- در این روش با جعل هویت نهادها یا افراد معتبری که با مخاطبان تعامل دارند و از به آن‌ها پیام ارسال می‌کنند، برای شناسایی کاربرانی تلاش شد که با این افراد یا نهادها در ارتباط هستند.

جعل هویت محدود به رسانه‌ها یا شهروند خبرنگاران نبود. چند نهاد خیریه نیز در تلگرام و اینستاگرام با روشی مشابه مورد حمله قرار گرفتند.



در دوران جنگ و اعتراضات به رغم قطعی اینترنت با موج داکسینگ (Doxing) و ادبیات نفرت‌پراکنانه در پتلفرم‌های مختلف مواجه بودیم. با وجود شباهت‌های ظاهری اما این دو موج تفاوت‌های قابل ملاحظه‌ای داشتند:

- **اعتراضات سراسری دی ماه:** شاهد موجی از انتشار اطلاعات معترضان یا مخالفان جمهوری اسلامی در کانال‌های تلگرامی و حساب‌های کاربری اینستاگرامی بودیم که اطلاعاتی مانند شماره تلفن یا آدرس محل سکونت و کار معترضان را منتشر و دنبال کنندگان‌شان را به ایجاد مزاحمت برای آن‌ها دعوت می‌کردند.
- **جنگ اسفند ماه:** پس از حمله آمریکا و اسرائیل به ایران، مقامات نظام فعالان دیاسپورا را به دلیل دعوت به مداخله بشردوستانه در مواجه با سرکوب خونین دی، به مصادره اموال و حتی سلب تابعیت تهدید کردند. پس از آن شاهد ایجاد موجی از افشای اطلاعات این گروه از فعالان در شبکه‌های اجتماعی بودیم.

یکی دیگر از تفاوت‌های داکسینگ در دوران سرکوب و جنگ، کشیده شدن پای رسانه‌های رسمی مانند کانال تلگرامی تابناک به هدف قرار دادن فعالان جامعه مدنی خارج از کشور است. یا لاک شدن اکانت رسمی خبرگزاری مهر به دلیل انتشار آدرس لیلا اوتادی، هنرپیشه، در دبی.

از دیگر تفاوت‌ها نحوی تولید محتوا بود؛ در دوران اعتراضات دی ماه بیشتر شاهد آن بودیم که کانال‌های تلگرامی یا اکانت‌های اینستاگرامی در سطح استانی مخالفان و معترضان را هدف قرار می‌دادند. در جریان جنگ اما یک

محتوای مشابه در سطح ملی در کانال‌ها یا اکانت‌های مختلف منتشر می‌شد.

پس از هشتم اسفندماه شاهد یک تغییر سیاست در پلتفرم ایکس بودیم. در این دوره از زمانی سیاست‌های مربوط به مدیریت محتوا سختگیرانه‌تر اجرا و حساب‌های کاربری گروهی از کاربران مدافع یا مبلغ سیاست‌های جمهوری اسلامی حذف شدند. از جمله:

- حساب‌های کاربری مربوط به رسانه رسمی خبرگزاری مهر در پی انتشار اطلاعات خصوصی
- حساب‌های کاربری تعدادی از مقامات فعلی نظام از جمله چند نماینده مجلس در پی حمایت از سپاه پاسداران
- حساب‌های کاربری برخی از کاربران پر مخاطب که موافقان حمله آمریکا و اسرائیل به ایران را تهدید می‌کردند.
-
- ادبیات نفرت‌پراکنانه در دوبازه زمانی سرکوب اعتراضات دی و جنگ اسفند شامل مواردی مانند «تهدید به خشونت‌های جنسی و جنسیتی»، «قلدری اینترنتی» و «تهدید به تجاوز و قتل» می‌شدند.

در هر دو بازه زمانی شخصیت‌های شناخته شده یا اکانت‌های پر فالوئر هدف کمپین‌های برای اعمال فشار به منظور واکنش نشان دادن و حمایت از سیاست‌های جمهوری اسلامی شدند. در مواردی معترضان و مخالفان جمهوری اسلامی، بخصوص زنان، هدف کمپین‌های تهدید به تجاوز یا قتل قرار می‌گرفتند.

شاخص‌های نقض یا آلودگی

دامنه‌ها

- smtp3707.org
- em557105.smtp3707.org
- onlineviewer.net
- confidential-mail.google.com
- cucps.k12.va.us
- amazonses.com
- awstrack.me
- joining-hosts-room.online
- shorten.ee
- louisebatterseldom.com
- gg.hls2.xyz
- c978e75f17.adislran.info
- c978e75f17.tc-spin.space
- C978e75f17m.cs2-go.sbs
- c5acc344.geogo.cfd

حساب‌های تلگرام و بات‌ها

- @AuthenticatorBot
- @abdallahsarayra06
- @mnzd12300

آدرس‌های اینترنتی

- 84.32.84.32
- 103.2.141.104
- 87.248.110.82
- 76.223.140.188
- 91.195.240.19
- 178.16.55.182
- 93.118.101.248
- 188.136.187.113
- 209.85.220.65
- 209.85.220.41
- 188.114.96.3
- 188.114.97.3
- 94.182.115.210

مکان‌یاب منبع یکسان(URL)

- https://shorten.ee/@help_center_6639

- https://t.ly/lZ6bU
- awstrack.me

هش فایل‌ها

- **PDF.apk**
  MD5: 873e3f275340fa1706b8e32026e6bedc
  SHA1: 71b8262e239869d74cd84eb5632abcfb252dc79d
  SHA256: 7ef0da4c8bd83a5eaaa4a250d027b4ffc168206923d9453f81b02454f58ab020
- **Vision-3187.apk**
  MD5: deae9dae9c418c2db3575c9f91823eb9
  SHA1: 7201a304a4e90ea14af6e6bd4eef6a6965cae613
  SHA256:
33dfa923c2047098170ca5ebdaa25494707dd2e77873be46f07851b60ea982b2
- **Pdf-812.apk**
  MD5: 4044E8EAA4548C72A41705386632FC61
  SHA1: 66D5906CF5EBB54C4CDC5FCA65BBB6D8EC9DD694
  SHA256:
  3D6136E5CC81837B77B12FA73989C23A23F8F68E5CEEF304BA9097FB734B47C4

نام پکیج‌ها

- com.chvi.pool