

نسخه انگلیسی

دانلود نسخه پی‌دی‌اف .PDF

تهدیدات سایبری

هوش مصنوعی در خدمت سرکوب؛ از فیشینگ هدفمند تا آزار جنسیت‌محور

۱۵ اکتبر ۲۰۲۶ فیلتربان

داده‌ها نشان می‌دهند سرکوب دیجیتال در این بازه نه‌تنها ادامه یافته، بلکه به مجموعه‌ای ترکیبی از محروم‌سازی دسترسی، مهندسی اجتماعی هدفمند، بدافزار، جعل هویت، آزار شبکه‌ای و عملیات اخلال‌گرانه تبدیل شده است.

خلاصه اجرایی و روندهای کلان

گزارش چهارم از مجموعه گزارش‌های تهدیدهای سایبری ایران، داده‌های ثبت‌شده در خط فوریت‌های امنیت دیجیتال میان طی بازه شش‌ماهه ۲ فروردین تا ۳۱ شهریور ۱۴۰۵ را بررسی می‌کند. این دوره در امتداد پیامدهای اعتراضات دی‌ماه ۱۴۰۴، موج بازداشت‌ها و توقیف دستگاه‌ها، اختلال‌های گسترده اینترنت و تشدید فشار بر فعالان داخل و خارج از ایران قرار دارد. داده‌ها نشان می‌دهند سرکوب دیجیتال در این بازه نه‌تنها ادامه یافته، بلکه به مجموعه‌ای ترکیبی از محروم‌سازی دسترسی، مهندسی اجتماعی هدفمند، بدافزار، جعل هویت، آزار شبکه‌ای و عملیات اخلال‌گرانه تبدیل شده است. هم‌زمان، دامنه استفاده از هوش مصنوعی در سرکوب دیجیتال به‌طور قابل‌توجهی گسترش یافته و از تقویت فیشینگ و جعل صدای افراد مورد اعتماد تا تولید محتوای جنسی جعلی، انتقال تهدید، تخریب اعتبار و ایجاد اختلاف در شبکه‌های مدنی امتداد پیدا کرده است.

از خاموشی مطلق تا اتصال تحت کنترل

تحقیقات فیلتربان نشان می‌دهد که در این دوره، جمهوری اسلامی به‌جای بازگرداندن کامل اینترنت، الگویی از اتصال محدود، ناپایدار و هویت‌محور را گسترش داد؛ الگویی که هم‌زمان دسترسی کاربران را طبقاتی‌تر، پرهزینه‌تر و قابل‌کنترل‌تر کرده است. مهم‌ترین تحولات این دوره عبارت‌اند از:

- ادامه قطع یا محدودسازی شدید اینترنت بین‌الملل در آغاز دوره؛

دسترسی‌پذیری

اندازه متن − ۱۰۰% +

مطالب مرتبط

۱ «جعل هویت» همچنان در صدر حمله‌های سایبری

۲ گزارش تهدیدهای سایبری ایران: جنگ خاموش علیه اقلیت‌های قومی و فعالان جامعه مدنی

۳ از قتل‌عام تا جنگ؛ تشدید سرکوب سایبری و فرامرزی همزمان با قطع اینترنت

۴ از جنگ تا شناسایی اولین قربانیان ایرانی جاسوس‌افزار خانواده پگاسوس در ایران

۵ موج صعودی جعل هویت در حمله‌های سایبری

۶ گزارش سالانه پلیس سایبری ایران و فرسایش حقوق شهروندان در دوران پس از جنبش زن، زندگی، آزادی

۷ فیلترینگ «نسل جدید»؛ فیشینگ با قالب‌های حکمرانی‌پذیر

۸ معرفی «دیده‌بان فتا» و «مانیتور قضایی»

- بازگشت ناقص اینترنت پس از ۸۸ روز، با ترافیکی بسیار پایین‌تر از سطح پیش از ۱۸ دی؛
- محدود سازی پهنای باند، افزایش تاخیر و اختلال در پروتکل‌ها و DNS بدون قطع ظاهری شبکه؛
- گسترش اینترنت طبقاتی از طریق سیم‌کارت‌های سفید و «اینترنت پرو»؛
- وابسته‌شدن دسترسی بازرگانان و دانشگاهیان به احراز هویت و تایید نهادی؛
- تشدید کنترل بر دیتاسنترها، سرورها، وی‌پی‌ان‌ها و ابزارهای دورزدن فیلترینگ؛
- افزایش برخورد امنیتی با کاربران و فروشندگان استارلینک؛
- کاهش زمان استفاده کاربران از اینترنت و افزایش هزینه دسترسی آزاد؛
- حرکت به‌سوی اتصال فعالیت‌های آنلاین و شناسه‌های مختلف به هویت واقعی کاربران؛
- تداوم بی‌ثباتی شبکه، قطعی برق مراکز داده و اختلال در GPS و خدمات بانکی.

در مجموع، اینترنت ایران در این دوره از وضعیت «قطع کامل» به شبکه‌ای ظاهراً متصل اما ناپایدار، طبقاتی، پرهزینه و تحت نظارت بیشتر گذار کرده است.

محو مرز میان سرکوب در جامعه و فضای مجازی

داده‌های هلپ‌دسک نشان می‌دهند که مرز میان سرکوب در فضای عمومی و کنترل در بسترهای دیجیتال بیش از گذشته مخدوش شده است. رفتار افراد در جامعه، از نوع پوشش و سبک زندگی تا ارائه خدمات به زنان بدون حجاب اجباری، می‌تواند به مسدود شدن سیم‌کارت، قطع اینترنت یا توقیف حساب منجر شود. در جهت معکوس، محتوای منتشر شده در شبکه‌های اجتماعی نیز برای اعمال فشار قضایی، اقتصادی و اجتماعی در فضای فیزیکی مورد استفاده قرار گرفته است.

موارد ثبت‌شده عبارت‌اند از:

- توقیف حساب‌های اینستاگرامی منتشرکننده سبک‌های زندگی مغایر با الگوهای مورد تایید جمهوری اسلامی؛
- تهدید صاحبان کسب‌وکارهای توقیف‌شده به بازداشت با اتهام «تبلیغ علیه نظام» در صورت اطلاع‌رسانی درباره برخوردها در حساب اینستاگرامی خود.
- قطع اینترنت خانگی برخی از فعالان جامعه مدنی، علاوه بر مسدود کردن سیم‌کارت؛

مسدود سازی گسترده سیم‌کارت کاربران در این بازه زمانی ابعادی بسیار گسترده‌تر از سابق به خود گرفت و نه فقط فعالان جامعه مدنی، روزنامه نگاران، فعالان دانشجویی، که شامل دیگر گروه‌های اجتماعی نیز شد.

- مسدود کردن سیم‌کارت کاربران اینستاگرام به‌دلیل انتشار محتوای مغایر با سبک زندگی مورد تایید جمهوری اسلامی و مشروط‌کردن رفع مسدودی به حذف محتوا؛
- الزام برخی کاربران به انتشار تصویر پرچم جمهوری اسلامی یا محتوای حمایتی از حکومت به‌عنوان شرط بازیابی سیم‌کارت؛
- مسدود کردن سیم‌کارت فعالان حوزه لباس، مد و آرایش و الزام آنان از سوی دادستانی به مراجعه به شورای مد و لباس و ارائه تعهد؛
- مسدود کردن سیم‌کارت زنان بدون حجاب اجباری در اصفهان تا زمان رسیدگی قضایی؛
- مسدود کردن سیم‌کارت روزنامه‌نگاران، فعالان سیاسی و فعالان جامعه مدنی؛
- مسدود کردن سیم‌کارت فعالان کارگری، معلمان، هنرمندان و دست‌اندرکاران رسانه و سینما؛
- مسدود کردن سیم‌کارت صاحبان کسب‌وکارهای اینترنتی به‌دلیل انتشار تصاویر مغایر با ضوابط پوشش جمهوری اسلامی؛
- مسدود کردن سیم‌کارت کاربران به‌دلیل انتشار مطالب انتقادی یا سیاسی در شبکه‌های اجتماعی؛

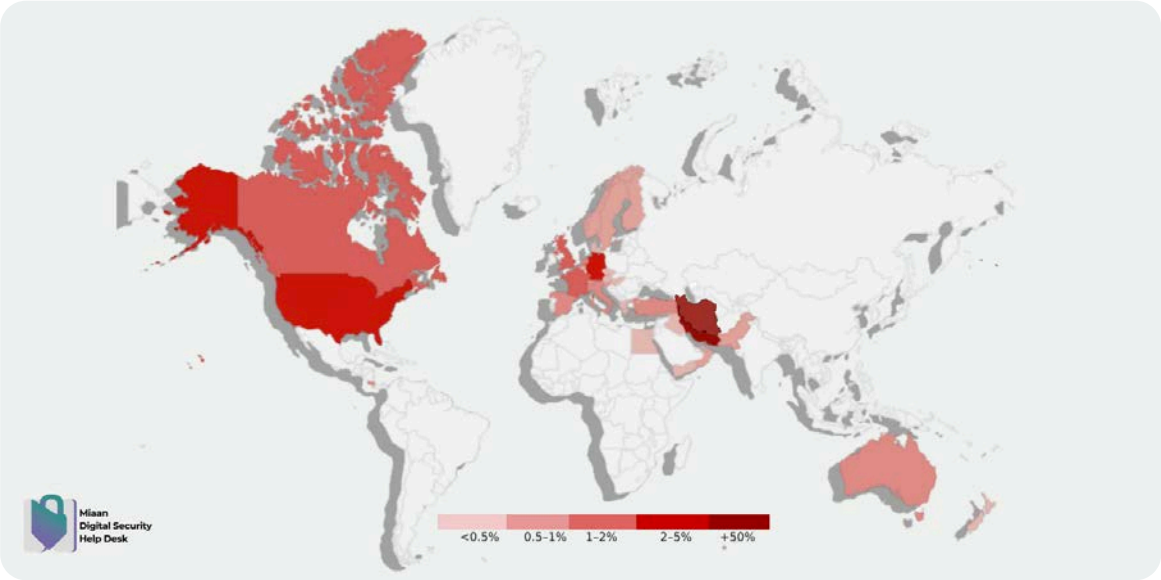
- همراه‌کردن مسدودسازی سیم‌کارت با تماس یا تهدید نهادهای امنیتی و مشروط‌کردن بازگشت دسترسی به حذف مطالب، ارائه تعهد یا توقف فعالیت عمومی.

این موارد نشان می‌دهند که سرکوب دیگر به یک حوزه محدود نمی‌ماند: کنش فرد در فضای عمومی می‌تواند به محرومیت دیجیتال منجر شود و فعالیت او در فضای مجازی نیز می‌تواند برخورد قضایی، توقیف کسب‌وکار یا فشار برای تغییر رفتار در جامعه را در پی داشته باشد. به این ترتیب، قطع ارتباطات و توقیف حساب‌ها به حلقه اتصال سرکوب آنلاین و آفلاین تبدیل شده‌اند؛ ابزاری برای تحمیل هنجارهای حکومتی، واداشتن افراد به حذف یا انتشار محتوا و جلوگیری از اطلاع‌رسانی درباره برخوردهای امنیتی.

سرکوب فراسرزمینی: آمار و ترندها

ماهیت تهدیدهای سایبری جمهوری اسلامی علیه اهداف خارج از مرزهای ایران در دوره مورد بررسی تغییر قابل‌توجهی یافته است. اگرچه نزدیک به ۱۶٪ از تمامی پرونده‌های ثبت‌شده در بازه شش‌ماهه ۲ فروردین تا ۳۱ شهریور ۱۴۰۵ به فعالان مدنی، روزنامه‌نگاران و سازمان‌های ایرانی مستقر در خارج از کشور مربوط بوده، حملات ثبت‌شده پیچیده‌تر، هدفمندتر و چندمرحله‌ای‌تر شده‌اند. جعل هویت، مهندسی اجتماعی شخصی‌سازی‌شده، استفاده از محتوای صوتی مشکوک به دست‌کاری مصنوعی، زیرساخت‌های موقت، توزیع بدافزار و تلاش برای تصاحب حساب از مهم‌ترین مؤلفه‌های این تغییر بوده‌اند.

- **نقشه توزیع اهداف فرامرزی:** کشورهای هدف در این دوره به‌ترتیب شامل ایالات متحده آمریکا با ۳۰ پرونده، آلمان با ۲۶ پرونده، بریتانیا با ۱۸ پرونده، فرانسه با ۱۶ پرونده و کانادا با ۱۲ پرونده بوده‌اند. این پنج کشور در مجموع ۱۰۲ پرونده، معادل ۶۴٫۶٪ از ۱۵۸ پرونده ثبت‌شده برای اهداف خارج از ایران، را تشکیل می‌دهند.



در مقایسه با دوره پیشین، ایالات متحده از جایگاه دوم به نخست و آلمان از جایگاه پنجم به دوم رسیده‌اند. بریتانیا از رتبه نخست به سوم منتقل شده و فرانسه از جایگاه ششم به چهارم رسیده است. تمرکز بر پرونده‌های مرتبط با حملات سایبری، تصویر متفاوتی ارائه می‌کند. اهداف خارج از ایران ۶۶٫۷٪ از پرونده‌های حمله سایبری مربوط به فعالان دیاسپورای ایرانی بوده است. در این زیرمجموعه، ایالات متحده، بریتانیا و آلمان هرکدام با پنج پرونده بیشترین تعداد را داشته‌اند و پس از آنها ایتالیا با سه پرونده قرار گرفته است. فرانسه، سوئد، اسلوونی و اسپانیا نیز هرکدام یک پرونده داشته‌اند. در مجموع، ایالات متحده، بریتانیا و آلمان ۱۵ مورد، معادل ۶۸٫۲٪ از ۲۲ پرونده حمله سایبری مرتبط با اهداف خارج از ایران، را به خود اختصاص داده‌اند.

روزنامه‌نگاران با هفت مورد، پرتکرارترین گروه هدف در پرونده‌های مرتبط با حملات سایبری بوده‌اند. سازمان‌های حقوق دیجیتال با پنج ثبت و فعالان سیاسی با سه مورد در جایگاه‌های بعدی قرار

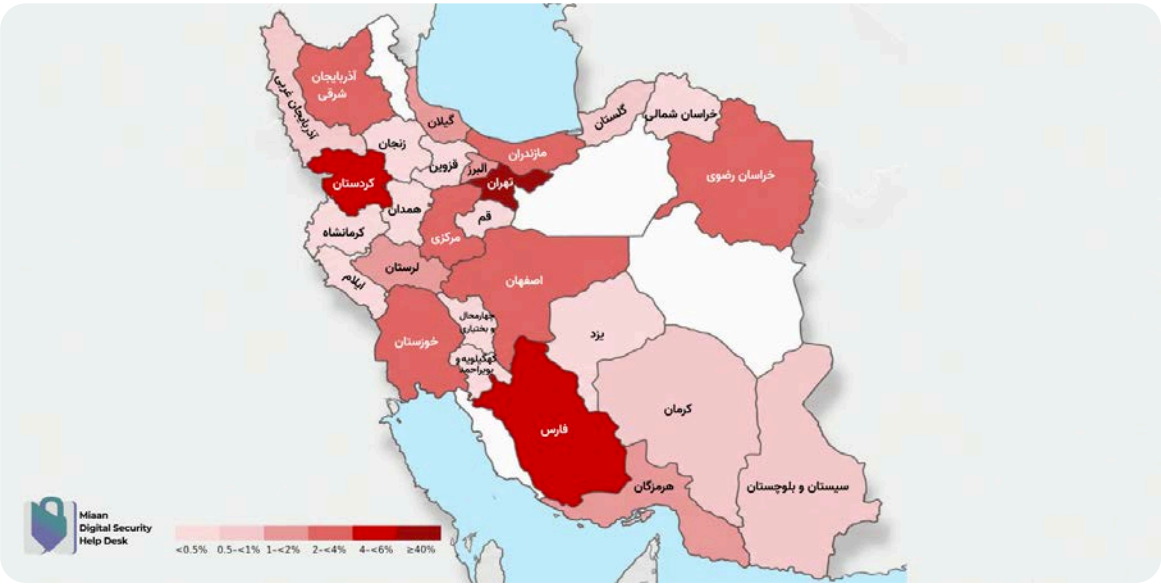
داشته‌اند. هدف‌گیری روزنامه‌نگاران، رسانه‌ها و سازمان‌های حقوق دیجیتال نشان می‌دهد بخش رسانه‌ای و شبکه‌های مدنی مرتبط با ایران همچنان از اهداف اصلی حملات فرامرزی‌اند.

درخواست‌های ثبت‌شده از سوی فعالان مدنی، روزنامه‌نگاران و سازمان‌های ایرانی مستقر در خارج از کشور شامل موارد زیر بوده‌اند:

- بررسی پیام‌ها، پیوندها و صفحات مشکوک به فیشینگ و سرقت اطلاعات ورود؛
- مقابله با تلاش برای دریافت کد احراز هویت و تصاحب حساب‌های تلگرام، اینستاگرام و سایر خدمات آنلاین؛
- بازیابی و ایمن‌سازی حساب‌های تصاحب‌شده یا در معرض نفوذ، از جمله بررسی نشست‌ها و تلاش‌های ورود غیرمجاز؛
- شناسایی، گزارش و حذف حساب‌ها، کانال‌ها یا صفحات جعلی که با نام فعالان، روزنامه‌نگاران، مدیران رسانه یا سازمان‌های مدنی فعالیت می‌کردند؛
- بررسی فایل‌ها، برنامه‌های اندرویدی و پیوندهای مشکوک به بدافزار که از طریق پیام‌رسان‌ها یا حساب‌های آشنا ارسال شده بودند؛
- تحلیل پیام‌های صوتی مشکوک به تولید یا دست‌کاری مصنوعی که برای جعل هویت، تهدید یا ایجاد اختلاف استفاده شده بودند؛
- مقابله با داکسینگ، افشای اطلاعات شخصی و تهدید فعالان دیاسپورا در وب‌سایت‌ها، کانال‌های تلگرامی و حساب‌های اینستاگرامی؛
- رسیدگی به آزار سازمان‌یافته، تهدیدهای آنلاین، فشار روانی و فراخوان برای حمله یا خشونت علیه فعالان و اعضای خانواده آنان؛
- گزارش و پیگیری انتشار محتوای خصوصی، تصاویر جنسی بدون رضایت و محتوای جعلی یا دیپ‌فیک با هدف تخریب اعتبار؛

- بررسی احتمال دسترسی مهاجم به پیام‌های خصوصی، مخاطبان، کانال‌های سازمانی یا شبکه ارتباطی قربانی؛
- رسیدگی به سوءاستفاده از حساب‌های تصاحب‌شده دوستان، همکاران یا مخاطبان برای هدف‌گیری زنجیره‌ای اعضای یک شبکه؛
- بررسی سوءاستفاده از نام، دامنه یا زیرساخت سازمان‌ها و مقابله با آسیب وارد شده به اعتبار دیجیتال آنها؛
- مقابله با افزایش مصنوعی دنبال‌کننده، گزارش‌دهی هماهنگ و تلاش برای ایجاد محدودیت یا حذف حساب‌ها و کانال‌ها؛
- ارائه راهنمایی‌های امنیتی، از جمله فعال‌سازی تأیید دومرحله‌ای، استفاده از گذرواژه مستقل، کنترل نشست‌های فعال و راستی‌آزمایی هویت از کانالی جداگانه.

تهدیدهای داخلی: جغرافیای سرکوب در ایران



در بازه شش‌ماهه ۲ فروردین تا ۳۱ شهریور ۱۴۰۵، معادل ۸۲٫۵٪ از مجموع موارد ثبت‌شده در هلپ‌دسک به افراد و سازمان‌های داخل ایران مربوط بوده است. این سهم در مقایسه با دوره پیشین بیش از ۱۰ واحد درصد افزایش یافته است. افزایش سهم پرونده‌های داخلی بیش از همه با درخواست‌های مرتبط با امنیت حساب، بسته‌شدن یا بازیابی حساب و اقدامات اضطراری پس از بازداشت و توقیف دستگاه هم‌زمان بوده است.

- **توزیع استانی:** تهران با ۴۰٫۶٪ همچنان بیشترین سهم را در میان پرونده‌های داخل ایران داشته است. سهم تهران در مقایسه با ۴۷٪ دوره پیشین، ۶٫۴ واحد درصد کاهش یافته است؛ بااین‌حال، فاصله آن با سایر استان‌ها همچنان قابل‌توجه است. پس از تهران، کردستان با ۵٫۷٪، فارس با ۴٫۱٪، مازندران با ۳٫۷٪، مرکزی با ۳٫۶٪، اصفهان با ۳٫۳٪، آذربایجان شرقی با ۳٫۱٪، خراسان

رضوی با ۲٫۸٪ و خوزستان با ۲٫۳٪ قرار گرفته‌اند. در این دوره نزدیک به ۲۰ درصد از پرونده‌های مربوط به داخل ایران بدون اشاره به استان، ثبت شده‌اند.

- **افراد:** امنیت و دسترسی به حساب‌ها مهم‌ترین نیاز ثبت‌شده در دوره بوده و پرونده‌های این حوزه حدود ۷۵٫۹٪ از تمامی پرونده‌های داخلی را تشکیل داده‌اند. در کل پرونده‌های مرتبط با حساب، بسته‌شدن حساب با ۵۱٪، فعال‌سازی مجدد با ۲۵٫۲٪، اعتراض به تعلیق با ۱۱٫۵٪ و بازیابی حساب با ۷٫۶٪ مهم‌ترین انواع درخواست بوده‌اند. اینستاگرام نیز با ۴۶٫۲٪ پرتکرارترین پلتفرم در پرونده‌های مرتبط با حساب بوده است.
- **توقیف دستگاه به‌عنوان ابزار محروم‌سازی دیجیتال:** حدود ۳٫۴٪ از پرونده‌های ثبت‌شده در این دوره به توقیف تلفن همراه یا سایر دستگاه‌های دیجیتال مربوط بوده است. توقیف دستگاه به جمهوری اسلامی امکان می‌دهد بدون نگهداری طولانی‌مدت فرد در بازداشت و پذیرش هزینه‌های سیاسی، اجرایی و حقوقی آن، دسترسی او را به ارتباطات، حساب‌های آنلاین، ابزارهای کاری و شبکه حمایتی‌اش مختل یا مسدود کند. در چنین شرایطی، حتی پس از آزادی فرد، نداشتن دستگاه یا نگرانی از دسترسی نهادهای امنیتی به اطلاعات آن می‌تواند فعالیت حرفه‌ای، رسانه‌ای یا مدنی او را متوقف کند.
- **تقاضا برای پشتیبانی استارلینک:** حدود ۶٫۵٪ از درخواست‌های ثبت‌شده در این دوره به پشتیبانی استارلینک مربوط بوده است. حجم این درخواست‌ها را می‌توان نشانه‌ای از گسترش استفاده از اینترنت ماهواره‌ای و افزایش تمایل کاربران به دسترسی از مسیری خارج از زیرساخت ارتباطی تحت کنترل حکومت دانست. محدودیت‌های مستمر، قطع و اختلال اینترنت، فیلترینگ گسترده و نگرانی از نظارت یا مسدود شدن ارتباطات، اعتماد بخشی از کاربران را به پایداری و امنیت اینترنت داخل کشور کاهش داده و تقاضا برای راهکارهای ارتباطی جایگزین را افزایش داده است.

بهزاد اکبری، معاون وزیر ارتباطات و مدیرعامل شرکت ارتباطات زیرساخت، در شهریور ۱۴۰۵ اعلام کرده بود که تعداد پایانه‌ها و کاربران استارلینک در ایران افزایش یافته و این رشد از زمان جنگ و در پی

محدودیت‌های اینترنتی شدت گرفته است. او همچنین تأکید کرد که آثار استفاده از این سرویس در ترافیک شبکه کشور قابل مشاهده است، هرچند آمار دقیق کاربران تنها در اختیار اسپیس‌ایکس قرار دارد.

توزیع جنسیتی

در کل دوره، مردان ۵۵٫۱٪ و زنان ۳۹٪ از پرونده‌های ثبت‌شده را تشکیل داده‌اند.با وجود سهم بیشتر مردان در مجموع دوره، فاصله میان زنان و مردان به‌تدریج کاهش یافته و در پایان دوره، سهم زنان از مردان بیشتر شده است.



در ابتدای دوره، سهم مردان ۶۷٫۱٪ و سهم زنان ۲۷٫۱٪ بود. سهم زنان در نیمه فروردین تا نیمه اردیبهشت به ۳۴٫۴٪، در نیمه اردیبهشت تا نیمه خرداد به ۳۴٫۷٪، در نیمه خرداد تا نیمه تیر به

۴۱٫۸٪ و در نیمه تیر تا نیمه مرداد به ۴۳٫۴٪ افزایش یافت. این سهم در نیمه مرداد تا نیمه شهریور اندکی کاهش یافت و به ۴۲٫۱٪ رسید، اما در بازه ۱۰ تا ۳۱ شهریور به ۴۸٫۱٪ افزایش یافت. در همین بازه پایانی، سهم مردان ۴۴٫۲٪ بود؛ در نتیجه، زنان برای نخستین بار در طول دوره سهم بیشتری از پرونده‌های ثبت‌شده داشتند.

الگوی جنسیتی بر اساس نوع درخواست نیز متفاوت بوده است. در پرونده‌های مدیریت محتوا، زنان با ۴۸٫۴٪ سهم بیشتری از مردان با ۲۸٫۱٪ داشته‌اند. در مقابل، در پرونده‌های مرتبط با حملات سایبری، مردان ۶۹٪ و زنان ۲۴٫۱٪ از افراد هدف را تشکیل داده‌اند و ۶٫۹٪ نیز با جنسیت نامشخص ثبت شده‌اند.

افزایش سهم زنان با افزایش پرونده‌های آزار جنسیت‌محور، افشای اطلاعات شخصی، انتشار محتوای خصوصی بدون رضایت و تولید تصاویر و ویدئوهای جنسی جعلی هم‌زمان بوده است.

دامنه فشار دیجیتال؛ از معترضان تا نهادهای مدنی

در پرونده‌های فردی این دوره، معترضان پرتکرارترین گروه بوده‌اند؛ در پرونده‌های سازمانی نیز سازمان‌های حقوق بشر بیشترین سهم را داشته‌اند و پس از آن‌ها، سازمان‌های مرتبط با اقلیت قومی کرد، حقوق دیجیتال و حقوق زنان قرار گرفته‌اند.



- **گروه‌های فردی:** در تصویر کلی دوره، معترضان با ۲۲٫۹٪ از پرونده‌های مربوط به افراد، پرتکرارترین گروه بوده‌اند. پس از آنان، فعالان سیاسی با ۱۲٫۸٪، معترضان فعال در شبکه‌های اجتماعی با ۷٫۷٪، روزنامه‌نگاران با ۶٫۹٪ و هنرمندان با ۶٪ قرار گرفته‌اند. این ترکیب نشان می‌دهد فشار دیجیتال علاوه بر فعالان سیاسی شناخته‌شده، افراد درگیر اعتراضات و شهروندانی را که فعالیت اعتراضی خود را در شبکه‌های اجتماعی دنبال کرده‌اند نیز در بر گرفته است.
- **سازمان‌ها:** در میان پرونده‌های سازمانی ثبت‌شده در کل دوره، سازمان‌های حقوق بشر با ۲۳٫۲٪ بیشترین سهم را داشته‌اند. سازمان‌های مرتبط با اقلیت قومی کرد با ۱۸٫۳٪، سازمان‌های حقوق دیجیتال با ۱۲٫۲٪ و سازمان‌های حقوق زنان با ۹٫۸٪ در رتبه‌های بعدی قرار گرفته‌اند.

تحلیل حملات سایبری

بررسی پرونده‌های مرتبط با حملات سایبری نشان می‌دهد که الگوی غالب تهدید در این دوره بیش از آنکه بر بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری متکی باشد، بر مهندسی اجتماعی، جعل هویت و سوءاستفاده از روابط اعتماد استوار بوده است.



- انواع حمله: فیشینگ با ۴۷٫۱٪ رایج‌ترین روش حمله در این دوره بوده و جعل هویت با ۲۳٫۵٪ در جایگاه دوم قرار گرفته است. این دو روش در مجموع ۷۰٫۶٪ از برچسب‌های حمله را تشکیل می‌دهند و نقش محوری مهندسی اجتماعی و سوءاستفاده از اعتماد را نشان می‌دهند. بدافزار با ۱۴٫۷٪، تصاحب حساب یا افشای اعتبارنامه با ۸٫۸٪ و اخلال در دسترسی و اعتبار زیرساخت و افزایش مصنوعی دنبال‌کننده هرکدام با ۲٫۹٪ در رتبه‌های بعدی قرار داشته‌اند.

- گروه‌های هدف: روزنامه‌نگاران با ۲۰٫۶٪ پرتکرارترین گروه هدف بوده‌اند. سازمان‌های حقوق دیجیتال با ۱۴٫۷٪ و فعالان سیاسی با ۸٫۸٪ در جایگاه‌های بعدی قرار گرفته‌اند. فعالان حقوق بشر، سازمان‌های قومی، رسانه‌ها و خبرگزاری‌ها، هنرمندان، فعالان حقوق دیجیتال، معترضان و فعالان بلوچ نیز هرکدام ۵٫۹٪ از ثبت‌های مرتبط با گروه هدف را تشکیل داده‌اند. تجمیع روزنامه‌نگاران با رسانه‌ها و خبرگزاری‌ها نشان می‌دهد بخش رسانه‌ای همچنان یکی از برجسته‌ترین اهداف حملات این دوره بوده است.
- کانال‌ها و پلتفرم‌ها: تلگرام با حضور در ۵۱٫۵٪ از پرونده‌ها، مهم‌ترین بستر ثبت‌شده در زنجیره حمله بوده است. واتس‌اپ با ۱۵٫۲٪، اینستاگرام با ۱۲٫۱٪، ایکس یا توییتر و جیمیل هر کدام با ۹٫۱٪ و وب سایت‌ها با ۳٪ در رتبه‌های بعدی قرار داشته‌اند. کاربرد تلگرام به فیشینگ محدود نبوده و توزیع بدافزار، جعل حساب یا کانال، فروش جعلی وی‌پی‌ان و استفاده از حساب‌های تصاحب‌شده را نیز شامل شده است. در برخی موارد، کانال آغاز حمله با دارایی مورد هدف متفاوت بوده است؛ برای نمونه، حمله از واتس‌اپ آغاز شده، اما هدف نهایی تصاحب حساب تلگرام بوده است.
- توزیع جغرافیایی: اهداف خارج از ایران ۶۶٫۷٪ از پرونده‌های مرتبط با حملات سایبری را تشکیل داده‌اند؛ در مقابل، ۲۷٫۳٪ از پرونده‌ها به افراد یا سازمان‌های داخل ایران مربوط بوده. ایالات متحده آمریکا، بریتانیا و آلمان هر کدام با ۱۵٫۲٪ بیشترین سهم را داشته‌اند و ایتالیا با ۹٫۱٪ در جایگاه بعدی قرار گرفته است. فرانسه، سوئد، اسلوونی و اسپانیا نیز هرکدام ۳٪ از پرونده‌ها را تشکیل داده‌اند.

تمرکز پرونده‌ها بر اهداف خارج از ایران و حضور پررنگ روزنامه‌نگاران، رسانه‌ها، فعالان سیاسی و سازمان‌های حقوق دیجیتال، با الگوی سرکوب فرامرزی دیجیتال سازگار است. پیامد این حملات نیز

می‌تواند از تصاحب یک حساب فراتر رود و دسترسی به مخاطبان، مکالمات و شبکه‌های حرفه‌ای قربانی، هدف‌گیری زنجیره‌ای افراد مرتبط و آسیب به اعتبار سازمان‌ها را در پی داشته باشد.

استفاده از هوش مصنوعی در جعل هویت و عملیات چندمنظوره علیه شبکه‌های فعالان مدنی

در دوره بررسی‌شده، چند مورد جعل هویت هدفمند را ثبت شد که از طریق واتس‌اپ و تلگرام انجام شده‌اند. مهاجمان با استفاده از نام، تصویر و موقعیت حرفه‌ای افراد مورد اعتماد، حساب‌های جعلی ایجاد کرده و با فعالان، روزنامه‌نگاران و اعضای شبکه‌های مدنی با فایل‌های صوتی جعل شده توسط هوش مصنوعی تماس گرفته‌اند.

این حملات یک هدف واحد نداشته‌اند. بخشی از موارد برای سرقت کد احراز هویت و تصاحب حساب تلگرام طراحی شده‌اند؛ در موارد دیگر، پیام‌های صوتی برای تهدید، ارعاب یا انتساب سخنان اختلاف‌برانگیز به افراد شناخته‌شده استفاده شده‌اند. بنابراین، این مجموعه را نمی‌توان صرفاً یک کمپین فیشینگ دانست. الگوی مشاهده‌شده ترکیبی از فیشینگ هدفمند، جعل هویت، تهدید و اخلال در اعتماد میان اعضای شبکه هدف است.

در شاخه فیشینگ، مهاجم پس از برقراری ارتباط و ایجاد اعتماد، پیوندی را با پوشش دعوت به جلسه ارسال کرده است. صفحه مقصد از قربانی می‌خواسته کدی را که از تلگرام دریافت کرده، به‌عنوان «کد ورود به جلسه» وارد کند. در دست‌کم یک پرونده، تحویل این کد به ایجاد دسترسی غیرمجاز به حساب تلگرام منجر شده است.

در شاخه اخلالی، مهاجم الزاماً به‌دنبال سرقت حساب نبوده است. پیام صوتی تهدیدآمیز یا صدای منتسب به یک فرد دیگر می‌تواند برای ایجاد ترس، تخریب اعتبار یا برهم‌زدن روابط درون شبکه

استفاده شود. موفقیت این شاخه به کلیک یا نفوذ فنی وابسته نیست؛ تغییر رفتار قربانی، ایجاد بی‌اعتمادی یا قطع ارتباط نیز می‌تواند نتیجه مطلوب مهاجم باشد.

یافته‌های اصلی

- حساب‌های جعلی واتس‌اپ و تلگرام با استفاده از هویت افراد مورد اعتماد ساخته شده‌اند.
- پیام‌ها متناسب با موقعیت حرفه‌ای یا شبکه ارتباطی قربانی تنظیم شده‌اند.
- در شاخه فیشینگ، پوشش اصلی حمله دعوت به جلسه یا گفت‌وگوی حرفه‌ای بوده است.
- مهاجم از یک صفحه تحت کنترل خود برای دریافت کد احراز هویت تلگرام استفاده کرده است.
- دست‌کم یک مورد دسترسی غیرمجاز به حساب تلگرام تأیید شده است.
- در تمامی پرونده‌ها پیام صوتی برای تقویت جعل هویت استفاده شده است.
- مواردی از پیام صوتی تهدیدآمیز یا محتوای منتسب به دیگران با هدف احتمالی ایجاد اختلاف نیز گزارش شده است.
- در این خوشه، تحویل بدافزار یا بهره‌برداری از آسیب‌پذیری نرم‌افزاری مستند نشده است.
- در این کمپین با استفاده از روش‌های مهندسی اجتماعی هویت و صدای فردی جعل شده بود که بیشترین ضریب جلب اعتماد در سوژه هدف را داشته باشد.

فیشینگ چندمرحله‌ای و سوءاستفاده از اعتماد

حملات فیشینگ مشاهده‌شده از الگوی «اعتمادسازی طولانی» پیروی می‌کنند. پیوند فیشینگ لزوماً در نخستین پیام ارسال نشده است. مهاجم ابتدا با جعل هویت یک فرد مرتبط با حوزه کاری قربانی، زمینه‌ای قابل‌باور برای ارتباط ایجاد کرده و سپس مکالمه را به دعوت به جلسه یا همکاری هدایت کرده است.

این روش چهار مرحله اصلی داشته است:

۱. ایجاد حساب جعلی با نام و تصویر فرد مورد اعتماد؛

۲. آغاز مکالمه از طریق واتس‌اپ یا تلگرام؛

۳. ارسال دعوت به جلسه و پیوند صفحه تحت کنترل مهاجم؛

۴. دریافت کد احراز هویت تلگرام و استفاده از آن برای ورود به حساب.

در این زنجیره، کد احراز هویت از مسیر مخابراتی رهگیری نشده است. مهاجم فرایند ورود به تلگرام را آغاز کرده و قربانی را متقاعد کرده است کد معتبر دریافتی را در صفحه جعلی وارد کند. بنابراین، عامل اصلی موفقیت حمله نه یک آسیب‌پذیری در تلگرام، بلکه بازتعریف فریبکارانه کاربرد کد احراز هویت بوده است.

این الگو با فیشینگ‌های چندمرحله‌ای توصیف‌شده در گزارش‌های پیشین فیلتربان هم‌خوانی دارد: مهاجم پیش از ارائه پیوند، با استفاده از یک دعوت حرفه‌ای یا سازمانی رابطه‌ای ظاهراً معتبر می‌سازد و پس از ایجاد اعتماد، درخواست حساس را مطرح می‌کند.

استفاده از پیام صوتی و نقش احتمالی هوش مصنوعی

پیام صوتی در این عملیات دست‌کم سه کارکرد متمایز داشته است:

تقویت جعل هویت

صدای منتسب به فرد مورد اعتماد می‌تواند به‌عنوان مدرک ظاهری هویت عمل کند. این روش به‌ویژه زمانی مؤثر است که قربانی شماره فرستنده را نمی‌شناسد، اما صدا یا شیوه بیان فرد جعل‌شده برای

او آشنا به نظر می‌رسد.

تهدید و ارعاب

در برخی موارد، محتوای صوتی ماهیت تهدید آمیز داشته است. در چنین سناریویی، هدف می‌تواند ایجاد ترس، فشار روانی، کاهش فعالیت عمومی یا القای توانایی مهاجم برای دسترسی به قربانی باشد.

ایجاد اختلاف و آسیب اعتباری

صدای جعل‌شده می‌تواند برای انتساب سخنان توهین‌آمیز، محرمانه یا اختلاف‌برانگیز به یک فرد استفاده شود. انتشار چنین محتوایی ممکن است موجب بی‌اعتمادی، قطع همکاری یا تنش میان اعضای یک شبکه شود، حتی اگر هیچ حسابی تصاحب نشده باشد.

نقش هوش مصنوعی در زنجیره عملیات

داده‌های موجود نشان نمی‌دهند که هوش مصنوعی کنترل کامل عملیات را بر عهده داشته است. نقش محتمل آن در افزایش کیفیت، سرعت و مقیاس تولید محتوای فریبکارانه قرار دارد.



هوش مصنوعی در اینجا یک روش نفوذ مستقل ایجاد نکرده است. دسترسی به حساب همچنان به دریافت کد معتبر تلگرام وابسته بوده، اما محتوای مصنوعی می‌توانسته احتمال اعتماد قربانی و ادامه تعامل را افزایش دهد.

زیرساخت مورد استفاده

در موارد فیشینگ، پیوندهایی با عمر کوتاه و صفحات تحت کنترل مهاجم مشاهده شده‌اند. بخشی از این زیرساخت از خدمات وب و تونل‌های کلادفلر استفاده کرده است. چنین خدماتی امکان راه‌اندازی سریع صفحه، استفاده از HTTPS و تعویض آسان نشانی را فراهم می‌کنند.

استفاده از کلادفلر به‌تنهایی شاخص فعالیت مخرب نیست. این زیرساخت تنها زمانی ارزش تحلیلی

پیدا می‌کند که با سایر مؤلفه‌ها همراه باشد:

- تماس از حساب جعلی؛
- جعل هویت یک فرد مورد اعتماد؛
- دعوت غیر منتظره به جلسه؛
- ارسال پیوند کوتاه‌عمر؛
- درخواست کد تلگرام در صفحه‌ای خارج از تلگرام؛
- ایجاد نشست جدید پس از تحویل کد.

پیامد عملیاتی

مهم‌ترین پیامد فنی تأییدشده، دسترسی غیرمجاز به یک حساب تلگرام است. چنین دسترسی‌ای می‌تواند مهاجم را به مخاطبان، مکالمات در دسترس، روابط حرفه‌ای و هویت‌های قابل هدف‌گیری بعدی برساند؛ بااین‌حال، در داده موجود، مدت نشست، دامنه اطلاعات مشاهده‌شده و فعالیت مهاجم پس از ورود مستند نشده است.

پیامدهای شاخه اخلالی ماهیتی متفاوت دارند. در این شاخه، اثر عملیات ممکن است شامل موارد زیر باشد:

- ایجاد ترس یا فشار روانی؛
- آسیب به اعتبار فرد جعل‌شده؛
- ایجاد بی‌اعتمادی در شبکه هدف؛
- قطع یا کاهش ارتباط میان افراد؛
- خودسانسوری یا توقف فعالیت؛
- آماده‌سازی قربانی برای حمله بعدی.

این پیامدها نباید با معیارهای فنی فیشینگ سنجیده شوند. برای مثال، حمله‌ای که به تصاحب حساب منجر نشده اما باعث قطع همکاری یا انتشار یک فایل صوتی جعلی شده، ممکن است از منظر اخلال اطلاعاتی موفق باشد.

یافته‌های هلپ‌دسک درباره سوءاستفاده از تلگرام در عملیات مخرب

هلپ‌دسک در بازه زمانی مورد بررسی سه دسته حمله مرتبط با توزیع برنامه‌های اندرویدی مشکوک از طریق تلگرام دریافت کرده است. در هر سه دسته، مهاجم از یک موضوع متناسب با شرایط یا علایق هدف برای ترغیب او به نصب فایل APK استفاده کرده است: خدمات دولتی، دسترسی به اینترنت آزاد و تصاویر شخصی.

شواهد موجود نشان می‌دهد که تلگرام در این پرونده‌ها دست‌کم به‌عنوان مسیر تماس با هدف و تحویل فایل یا لینک مخرب استفاده شده است. در یکی از نمونه‌ها، یک رشته با ساختار توکن API بات تلگرام نیز داخل فایل APK مشاهده شد که احتمال استفاده از تلگرام در مراحل بعدی عملیات را مطرح می‌کند.

الگوی مشترک در مرحله دسترسی اولیه

در هر سه پرونده، حمله با یک پیام تلگرامی آغاز شده است. مهاجمان از دو روش اعتمادسازی استفاده کرده‌اند:

- ارسال پیام از حسابی که هدف آن را می‌شناخته است؛
- ارائه برنامه با پوششی متناسب با نیاز یا شرایط هدف.

در پرونده «جهاد کشاورزی»، اعتبار یک نهاد دولتی جعل شده است. در پرونده Starlink/VPN، مهاجم از نیاز کاربران داخل ایران به ابزارهای دور زدن محدودیت اینترنت استفاده کرده است. در پرونده «عکس یادگاری»، پیام با استفاده از یک رابطه شخصی و محتوای عاطفی طراحی شده است.

این الگو نشان می‌دهد که مهاجمان تنها به ویژگی فنی بدافزار متکی نیستند. بخش مهم عملیات، متقاعد کردن هدف به نصب برنامه‌ای خارج از فروشگاه رسمی است. ارسال پیام از حساب یک دوست یا مخاطب قدیمی می‌تواند نشانه تصاحب حساب باشد، اما اطلاعات موجود برای اثبات هک‌شدن این حساب‌ها کافی نیست.

قابلیت‌های بالقوه برنامه‌ها

دو نمونه‌ای که Manifest آنها قابل بررسی بود، مجوزهای گسترده‌ای درخواست می‌کردند. این مجوزها می‌توانند امکان اقدامات زیر را فراهم کنند:

- خواندن پیامک‌ها و کدهای تأیید؛
- ارسال پیامک از دستگاه قربانی؛
- دسترسی به شماره تلفن و اطلاعات دستگاه؛
- مشاهده یا تغییر مخاطبان؛
- دسترسی به تصاویر و فایل‌های ذخیره‌شده؛
- مشاهده برنامه‌های نصب‌شده؛
- برقراری تماس تلفنی؛
- اجرای سرویس در پس‌زمینه؛
- آغاز فعالیت پس از روشن‌شدن دوباره دستگاه؛

- برقراری ارتباط اینترنتی با زیرساخت خارجی.

وجود این مجوزها به‌تنهایی ثابت نمی‌کند که همه این قابلیت‌ها عملاً استفاده شده‌اند. بااین‌حال، ترکیب مجوزهای پیامک، مخاطبان، اینترنت، اجرای پس‌زمینه و راه‌اندازی خودکار با پوشش جعلی و روش توزیع هدفمند، خطر جاسوسی، سرقت حساب و ادامه انتشار حمله از طریق مخاطبان قربانی را افزایش می‌دهد.

مشاهده رشته شبیه توکن بات تلگرام

در فایل APK مربوط به Starlink/VPN، یک رشته با قالب توکن API بات تلگرام در مسیر assets/lb.txt مشاهده شد. هنگام آزمایش، اعتبارسنجی زنده آن با پاسخ ۴۰۱ Unauthorized مواجه شد. این نتیجه می‌تواند به معنی لغو، تعویض یا غیرفعال‌بودن توکن در زمان بررسی باشد.

این یافته مهم است، زیرا توکن بات می‌تواند برای احراز هویت برنامه نزد API تلگرام و برقراری ارتباط خودکار استفاده شود. کاربرد احتمالی آن می‌تواند شامل ارسال اطلاعات دستگاه، دریافت تنظیمات یا فرمان و گزارش وضعیت نصب باشد. بااین‌حال، صرف مشاهده یک رشته شبیه توکن، استفاده عملی از آن را ثابت نمی‌کند. برای تایید باید فراخوانی‌های API تلگرام در کد، ترافیک شبکه یا بخش اصلی رمزگشایی‌شده برنامه مشاهده شود.

توکن کامل نباید در گزارش‌های عمومی منتشر شود. بخش عددی آن، هشدارهای زمانی، مسیر فایل و سایر اطلاعات لازم را می‌توان به‌صورت محدود و از طریق یک کانال امن برای بررسی در اختیار تلگرام قرار داد.

پنهان‌سازی و مقاومت در برابر تحلیل

دو نمونه از روش‌هایی برای دشوارکردن تحلیل استفاده کرده‌اند. APK مربوط به Starlink/VPN دارای لایه بسته‌بندی بومی مشابه DPT، دارایی‌های مبهم‌شده، بارگذاری‌های وابسته به معماری دستگاه و حفاظت ZipCrypto بود. فایل «عکس یادگاری» نیز به‌گونه‌ای مبهم‌سازی شده بود که تحلیل‌گران نتوانستند Manifest و قابلیت‌های اصلی آن را به‌طور کامل استخراج کنند.

این روش‌ها احتمالاً با هدف پنهان‌کردن بخش اصلی برنامه، جلوگیری از شناسایی سریع و افزایش هزینه تحلیل استفاده شده‌اند. بااین‌حال، شباهت در روش پنهان‌سازی یا استفاده از ابزارهای عمومی بسته‌بندی، برای نسبت‌دادن نمونه‌ها به یک عامل تهدید مشترک کافی نیست.

ارزیابی اطلاعاتی

- در هر سه پرونده از تلگرام برای تماس با هدف و ارسال فایل یا لینک APK استفاده شده است.
- نمونه‌های «جهاد کشاورزی» و Starlink/VPN مجوزهای حساسی با قابلیت بالقوه جاسوسی، سرقت اطلاعات یا ماندگاری درخواست می‌کنند.
- نمونه Starlink/VPN دارای یک رشته با قالب توکن بات تلگرام بوده و توکن در زمان آزمایش معتبر نبوده است.
- حساب‌های آشنای استفاده‌شده برای ارسال فایل ممکن است تصاحب شده باشند.
- برنامه‌ها برای جمع‌آوری اطلاعات یا حفظ دسترسی در دستگاه قربانی طراحی شده‌اند.
- توکن مشاهده‌شده در نمونه Starlink/VPN عملاً برای فرماندهی و کنترل استفاده شده است.
- سه پرونده هلپ‌دسک به یک عامل تهدید یا عملیات مشترک مرتبط هستند.

- پرونده‌های هلپ‌دسک ارتباط مستقیمی با Small Sieve یا گزارش‌های عمومی درباره DCHSpy دارند.

پرونده‌های مورد بررسی نشان می‌دهند که تلگرام در عملیات هدفمند علیه فعالان، معترضان و روزنامه‌نگاران می‌تواند چند نقش داشته باشد: ایجاد تماس اولیه، سوءاستفاده از اعتماد میان مخاطبان، انتقال فایل APK، هدایت قربانی به زیرساخت دانلود و احتمالاً فراهم‌کردن یک کانال خودکار برای ارتباط برنامه با عامل تهدید.

مهم‌ترین الگوی مشترک، ترکیب مهندسی اجتماعی متناسب با شرایط هدف و برنامه‌های اندرویدی خارج از فروشگاه رسمی است. مشاهده رشته شبیه توکن بات تلگرام در یکی از نمونه‌ها، احتمال استفاده از API تلگرام در مراحل بعدی عملیات را مطرح می‌کند، اما این فرضیه هنوز به شواهد رفتاری یا شبکه‌ای بیشتری نیاز دارد.

آزار جنسیت‌محور و افشای اطلاعات شخصی

بررسی پرونده‌های این دوره نشان می‌دهد شبکه‌ای از کانال‌ها، گروه‌ها، ربات‌ها و حساب‌ها در تلگرام و سایر پلتفرم‌ها برای افشای اطلاعات شخصی، تهدید فعالان، آزار هدفمند زنان و انتشار محتوای خصوصی یا جنسی بدون رضایت استفاده شده‌اند. در این فعالیت‌ها، انتشار اطلاعات شناسایی‌کننده با محتوای تحقیرآمیز، تهدید و فراخوان برای آزار همراه شده و مرز میان خشونت دیجیتال، تخریب اعتبار و تهدید فیزیکی را کمرنگ کرده است.



بخشی از این شبکه‌ها تصاویر زنان مخالف حجاب اجباری را منتشر کرده، اطلاعات خصوصی آنان و اعضای خانواده‌شان را جمع‌آوری کرده و مخاطبان خود را به آزار آنلاین یا اقدام خشونت‌آمیز تشویق کرده‌اند. تصاویر و ویدئوهای جنسی جعلی یا تولیدشده با هوش مصنوعی نیز برای تحقیر، ارعاب، تخریب اعتبار و افزایش فشار روانی بر قربانیان به کار رفته‌اند.

- **گسترش شبکه‌های محتوای بدون رضایت:** در بازه ۱۰ مرداد تا ۹ شهریور ۱۴۰۵، تعداد موارد مرتبط با انتشار محتوای خصوصی یا جنسی بدون رضایت، در مقایسه با دوره ۱۰ تیر تا ۹ مرداد، بین ۴٫۴٪ تا ۱۴٫۷٪ افزایش یافته است.
- **افزایش دامنه مخاطبان:** شمار مشترکان شبکه‌های انتشار محتوای بدون رضایت در دوره دوم نسبت به دوره قبل بین ۲۲٫۲٪ تا ۲۷٫۸٪ رشد کرده است. افزایش سریع‌تر مخاطبان نسبت به

تعداد دارایی‌ها نشان می‌دهد شبکه‌های موجود علاوه بر گسترش ساختاری، توانسته‌اند دامنه دسترسی و توزیع محتوای خود را نیز افزایش دهند.

- **سوءاستفاده از افراد زیر سن قانونی:** مخاطبان شبکه جداگانه مرتبط با سوءاستفاده از افراد زیر سن قانونی، معادل حدود ۴٫۳٪ تا ۴٫۵٪ از شمار مخاطبان شبکه بزرگ‌تر انتشار محتوای بدون رضایت در همان دوره بوده‌اند.

این روند نشان می‌دهد آزار جنسیت‌محور صرفاً مجموعه‌ای از حملات پراکنده علیه افراد نبوده، بلکه از زیرساخت‌های شبکه‌ای و مخاطبان گسترده برای جمع‌آوری اطلاعات، انتشار محتوا و تشدید فشار بر قربانیان استفاده کرده است. داکسینگ در این الگو می‌تواند زمینه آزار هماهنگ، تهدید اعضای خانواده، تعقیب خارج از فضای آنلاین و افزایش خطر خشونت فیزیکی را فراهم کند. محتوای جنسی جعلی نیز حتی بدون نفوذ به حساب یا دستگاه قربانی می‌تواند به آسیب اعتباری، خودسانسوری، کاهش فعالیت عمومی و فشار روانی منجر شود.

شاخص‌های نفوذ

دامنه‌های آلوده

- louisebatterseldom[.]com
- Hbscity[.]com
- ruv[.]de/service/doi/doi-check?id=XXXXX&v۲=XXXX
- Wajobfocus[.]com
- Domainlicense[.]my
- Datadataprotect[.]org
- Internetregisteredinternet[.]org

- Ct[.]ws
- votingglobal[.]ct[.]ws/en
- rfdedghmlktgfdklo[.]sfo۳[.]digitaloceanspaces[.]com/۱[.]html
- praxisioak[.]click

لینک‌های آلوده

- rfdedghmlktgfdklo[.]sfo۳.digitaloceanspaces[.]com/۱[.]html
- Reproduction-sudden-generators-inspections[.]trycloudflare[.]com
- Examine-hopefully-batch-peers[.]trycloudflare[.]com
- Counting-retailer-special-islamic[.]trycloudflare[.]com
- www[.]google.com/url?q=https%۳A%۲F%۲Fpraxisioak[.]click%۲F۸۳E۷%۲F&sa=D&source=calendar&ust=۱۷۸۹۸۴۲۳۶۰۰۰۰۰۰۰&usg=AOvVaw۳mRetNnUv۷wOBmfT۱no۶Lt

آی‌پی ها

۲۰۹.۸۵.۲۲۰.۶۹

۱۰۴.۲۱.۴۱.۱۲۷

۴۴.۲۳۹.۴۶.۷۳

۵۲.۲۰۲.۱۹۹.۲۰۹

۳۱.۲۲.۴.۲۳۴

۲۰۹.۸۵.۲۲۰.۴۱

۱۳۸.۶۸.۳۴.۱۶۱

۱۷۲.۶۷.۱۹۴.۱۵۵

۱۰۴.۲۱.۵۲.۲۸

راه‌های ارتباطی

- bantaruland@gmail[.]com
- pwp-cbf۳۴۹b۷۹f۱۱۷۰۷۵b۰۵۳۳c۶e۹b۵۷be۰۱@privacyguardian[.]org
- ۵۴۲۲۱bb۳۳۷۱۵۴d۱۱۸۱۵f۴b۶۸b۲۷۶۴۱a۲.protect@withheldforprivacy[.]com
- catalinatnucsfsjq۴۶۲۲۴@gmail[.]com
- katulisbrian@yahoo[.]com
- amirasmar.aratlantic@yahoo[.]com

اپلیکیشن‌های آلوده

LnDP۸nXsjQ[.]apk

SHA-۲۵۶:
۴e۶d۷f۵۳۷۳۳a۷۷a۹۸۹۰۸۸۱۶۰b۶۸c۸۴۹۰a۲۴۸dd۹c۶۳cf۴f۰d۳۲۴۷۱۲۲۰۶f۹f۰fd۴

Vision-۳۵۸۸۶[.]apk

Md۵: ۴f۱f۲c۶۱f۳۹b۱۱۴۸۴۰۱ef۸b۳a۹۱۵eec۵

Sha۲۵۶:

a۱۰۷۷d۸d۷b۱ccaa۸۷۲۲۹a۱۸dacb۸۸۹۷۱۷۸۷۵۷۵۳۴c۰۲۹e۶aee۳۳۴۶df۰۸۷ecf۰۷۸

Vision[.]apk

Md۵: ۱f۲ec۲b۰f۷۸c۷۱۶۰۹۱۱۷ba۸f۱f۱fd۳۵d

the English version

/english