فهرست

پس‌گرفتن اینترنت: گزارش راهبرد تقابل (ضد راهبرد) ۲
مقدمه ۲
روایت‌های جعلی، سفسطه و مغلطه ۲
روایت‌های جعلی ۲
تعریف ۳
مثال‌های مهم روایت‌های جعلی در ایران ۳
منابع تغذیه روایت‌های جعلی ۴
الگوهای ارتباطات ۴
توصیه‌ها ۴
سفسطه و مغلطه ۵
تعریف ۵
۱۵ نوع مغلطه ۵
منابع تغذیه و الگوهای ارتباطات ۷
توصیه‌ها ۷
اخبار جعلی و بی‌اعتبار ۸
معرفی ۸
مثال‌های مهم اخبار جعلی در فضای اخبار فارسی ۸
الگوهای اجرای کمپین‌های اخبار جعلی در فضاهای آنلاین فارسی‌زبان ۸
توصیه‌ها ۹
آزار و اذیت و تعرض آنلاین ۹
معرفی ۹
ترول‌ها و تعرض آنلاین ۱۰
عاملان ۱۱
توصیه‌ها (رویکرد چند ذی‌نفعی) ۱۲
حملات سایبری ۱۳
حملات بدافزارها ۱۳
حملات فیشینگ ۱۴
نشت داده‌های وب‌سایت‌ها ۱۵
توصیه‌ها ۱۵
پیوست ۱/ شاخص ریسک ۱۶

پس‌گرفتن اینترنت: گزارش راهبرد تقابل (ضد راهبرد)

مقدمه

این گزارش تلاشی در راستای بررسی کامل چالش‌های موجود در زمینه اطلاعات کلیدی و مهم در فضاهای عمومی آنلاین فارسی‌زبان است. این چالش‌های پیچیده، بازتاب موضوعات گسترده، غالباً در عرصه سیاسی و اجتماعی ایران وجود دارند. این گزارش چهار موضوع محتوایی و فنی را شناسایی کرده که هدفِ حقوق بشر و آزادی بیان و اطلاعات واقع می‌شوند:

۱. روایت‌های جعلی و مغلطه؛
۲. اخبار جعلی و بی‌اعتبار؛
۳. تعرض آنلاین؛
٤. حملات سایبری.

هر موضوع، بازتاب نوعی اِعمال قدرت و اختیار رژیم ایران و حامیان آن در فضای سایبری علیه مخالفان سیاسی، اعضای جامعه مدنی و یا حتی شهروندان معمولی است. بازیگران دولتی از طریق پروپاگاندا، دستکاری مداوم افکار عمومی و ساکت کردن مخالفان، هدف مشترکی را دنبال می‌کنند: **تغییر حقیقت به نفع خودشان**.

کمیته رهبری در فوریه ۲۰۱۹، گزارش‌های طولانی که هر عضو درمورد موضوع تخصصی خود تهیه کرده بود را مورد بررسی و گفتگو قرار داد. گزارش حاضر نسخه مختصری از این گفتگوها و تبادل نظرهای گسترده را ارائه می‌دهد. در این گفتگوها، کمیته برای محتواهای جعلی و آسیب‌زا و اینکه آنها در کجا و چگونه همپوشانی دارند، تفکیک قائل شده است. ما معتقدیم ظهور و بروز بسیاری از مواردی که در اینجا بررسی می‌شود، در زمان تفکیک گفتار آسیب‌زا و جعلی از هم است و به همین دلیل، این اطلاعات ذیل اطلاعات جعلی قرار می‌گیرند. با این حال، این گزارش به دنبال توضیح مفاهیم اصلی اطلاعات جعلی و دستکاری‌شده نیست. درعوض، به بررسی عمیق چهار نوع تهدیدی که در حال حاضر بر حوزه‌های آنلاین فارسی‌زبان حاکم است می‌پردازد.

به همین منظور، هر بخش با معرفی مختصر موضوع آغاز می‌شود، سپس به ارائه تعریف، نمونه‌ها و الگوهای قابل‌توجه در ایران می‌پردازد و در پایان، نتیجه‌گیری شامل مجموعه‌ای از توصیه‌ها برای تولیدات بعدی این پروژه خواهد بود.

روایت‌های جعلی، سفسطه و مغلطه

روایت‌های جعلی

روایت‌های جعلی حاوی مطالب دروغین، گمراه‌کننده و دستکاری‌شده است و انحراف از واقعیت را به گونه‌ای ارائه می‌دهد که تمایز واقعیت از داستان، و حقیقت از دروغ را غیر ممکن می‌سازد. روایات جعلی به مفاهیم و تعصبات عقیدتی متوسل می‌شوند و همین امر مقابله با آن را پیچیده می‌کند.

تحقیقات اولیه ما در مورد میزان آگاهی عمومی کاربران و تولیدکنندگان رسانه‌های ایرانی درباره مفهوم «روایت‌های جعلی» نتایج مثبتی نداشته است. تنها تعداد معدودی از نمونه‌هایی که به طور غیر رسمی مورد بررسی قرار داده‌ایم، از روایات جعلی و راه‌های تمایز آنها با حقیقت اطلاع داشتند. بدتر آنکه هیچ مطلبی در فارسی وجود ندارد و حتی در مورد ترجمه فارسی این اصطلاح، توافق گسترده یا متداولی نیز حاصل نشده است. به منظور تهیه این گزارش و تولیدات بعدی، از اصطلاح فارسی «روایت بدلی (روایت جعلی)» به عنوان نزدیکترین ترجمه استفاده می‌کنیم.

تعریف

در زمینه تولید و انتشار اخبار، روایت جعلی داستانی است که حقیقت را با اطلاعات جعلی ترکیب می‌کند. غالباً هدف ایجاد روایت جعلی، گمراه کردن مخاطب است. سازندگان روایت‌های جعلی متعهد به ارزش‌های روزنامه‌نگاری براساس گزارشگری مبتنی بر واقعیت، صحت و انصاف نیستند و معمولاً تلاش می‌کنند حقیقت را در جهت قانونی‌کردن باطل خود دستکاری کنند. اگرچه روایات جعلی می‌تواند محصول یک شرایط ویژه یا سوءتفاهم از واقعیت باشد، اما شکل‌گیری عمدی روایات دروغین و پیوند دادن وقایع غیر مرتبط با یکدیگر می‌تواند جوهره و اساس یک روایت جعلی عمدی را نشان دهد.

مهم‌ترین تکنیک برای تولید روایت جعلی، تکرار است. انتشار و تکرار یک روایت جعلی در یک بازه زمانی طولانی، آن را معتبرتر می‌کند و بنابراین بیشتر در گفتمان‌های اجتماعی و سیاسی ظهور پیدا می‌کند.

مثال‌های مهم روایت‌های جعلی در ایران

- برانگیختن خشم، ترس و نفرت از طریق روایات جعلی مذهبی، مانند وفات یا شهادت [حضرت] فاطمه (دختر پیامبر اسلام) در گسترش شکاف بین مسلمانان شیعه و سنی بسیار مهم است؛
- مقدس‌سازی چهره‌های سیاسی مانند [حضرت امام] خمینی، با این ادعا که تصویر وی را می‌توان در قسمت‌های تاریک ماه مشاهده کرد. افراد قادرند هنگام مشاهده اشیایی از قبیل لکه‌های جوهر، ابرها، کوه‌ها و غیره، تصاویر آشنایی را شناسایی کنند، اما سازندگان این روایت جعلی از این پدیده روانشناختی بهره بردند تا [حضرت امام] خمینی را به عنوان یک چهره مقدس معرفی کنند و احساسات را در حمایت از انقلاب اسلامی سال ۱۳۵۷تحریک کنند؛
- ایجاد شک و تردید در بین مخالفان رژیم از طریق برانگیختن احساسات ناسیونالیستی، تنش میان هواداران اصلاحات و طرفداران تغییر رژیم را عمیق‌تر می‌کند. روایت جعلی متداول در این زمینه چنین است: «به دلیل بی‌ثباتی در غرب آسیا، عدم وجود جایگزین سیاسی قوی و افزایش فعالیت سیاسی قومیت‌ها، سرنگونی رژیم کنونی منجر به تجزیه ایران می‌شود.»
- مباحث اجتماعی مانند ازدواج کودکان، کانون بسیاری از روایت‌های جعلی با ماهیت سیاسی شده است. طرفداران ازدواج کودکان (غالباً از گروه اصولگراها) برای حمایت از ازدواج کودکان در توییتر و اینستاگرام هشتگ‌هایی را ترویج دادند که منجر به تقویت پیام‌های زیر شد:

نمونه‌های بسیاری از ازدواج‌های موفق کودکان وجود دارد؛

- ازدواج حق طبیعی انسان است؛
- محدود کردن ازدواج برای کودکان، روابط جنسی خارج از ازدواج در بین کودکان و نوجوانان را افزایش می‌دهد؛
- از نظر پزشکی، پذیرش دختران زیر ۱۸ سال قابل قبول است؛
- بارداری زنان مسن بیشتر از بارداری دختران جوان برای سلامتی خطر دارد؛
- محدودیت سن ازدواج باعث افزایش حاملگی و سقط جنین ناخواسته خواهد شد؛
- فقط ۳٪ از ازدواج افراد ۱۰ تا ۱۴ ساله منجر به طلاق شده است. این تعداد بسیار کمتر از ازدواج بزرگسالان است؛
- طبق آمار، میزان مرگ‌ومیر مادران تقریباً صفر است و هیچ ارتباطی بین مرگ نوزاد در زمان تولد و سن مادر وجود ندارد؛
- مطالعه هفت استان ایران که بیشترین تعداد ازدواج کودکان را دارد نشان می‌دهد که رضایت جنسی بین ۶۶ تا ۸۹ درصد است. این مطالعه نشان می‌دهد که بین ازدواج کودکان و کاهش رضایت جنسی رابطه‌ای وجود ندارد؛
- سن بلوغ جنسی در ایران کاهش یافته و ازدواج یک راه‌حل قانونی، چه از نظر شرعی و چه از نظر قوانین داخلی است.

این استدلال‌ها چهار ویژگی دارند:

۱. شامل بخشی از حقیقت هستند به عنوان مثال ازدواج یک حق است؛
۲. افراد مذهبی را هدف قرار داده و با گفتن اینکه ازدواج کودکان می‌تواند مانع از رفتارهای غیر اخلاقی شود، به احساسات آنها متوسل می‌شوند؛
۳. از طریق استفاده از آمار، استدلال‌های علمی ارائه می‌دهند؛
٤. از آنجائیکه استدلال‌ها در ظاهر منطقی به نظر می‌رسد، مردم احتمالاً تمایل به دفاع از آنها را دارند.

منابع تغذیه روایت‌های جعلی

تمایل جمهوری اسلامی برای تأثیرگذاری بر افکار عمومی از طریق دیپلماسی عمومی و رسانه‌های اجتماعی، منجر به اختصاص منابع قدرتمند و سازمان‌یافته به تولید و انتشار روایت‌های جعلی شده است. با این حال، منابع تغذیه روایت‌های جعلی در رسانه‌های اجتماعی فارسی‌زبان به راحتی قابل شناسایی نیستند. آنها از روزنامه‌نگاران طرفدار رژیم گرفته تا کاربران ناشناس و جعلی استفاده می‌کنند. براساس مشاهدات ما در توییتر و اینستاگرام، چند ویژگی مشترک در معروف‌ترین حساب‌ها وجود دارد:

۱. اکثراً کاربران با نام کاربری یا حساب کاربری مردانه هستند؛
۲. در حساب‌های کاربری ناشناس احتمال کمی وجود دارد که از اسامی مذهبی استفاده کنند، چراکه نشان‌دهنده حمایت آنها از رژیم است؛
۳. آنها از نمادهایی استفاده می‌کنند که متعلق به یک گروه خاص ایرانی نیست و جهانی است؛
٤. آنها بیش از تمام پلتفرم‌های رسانه‌های اجتماعی، در توییتر حضور دارند.

الگوهای ارتباطات

۱. آنها معمولاً در رسانه های اجتماعی آرام و مدنی هستند و خود را در ایده‌های مخالف، روادار و شکیبا نشان می‌دهند؛
۲. آنها مشارکت بالا و علاقه زیادی به مباحث و بحث‌های مردمی دارند؛
۳. فعالیت‌های رسانه‌های اجتماعی آنها بسیار سازمان‌یافته و هماهنگ است؛
٤. مراجعه آنها به دین بسیار کم است، اما از داده‌های علمی و منابع معتبر استفاده می‌کنند.

توصیه‌ها

۱. ایجاد و انتشار ابزارهای آموزشی (نمودارها، بازی‌ها، اینفوگرافی‌ها، گرافیک‌های رسانه‌ای، نمایش‌های گرافیکی یا آزمون‌ها) و فیلم‌ها درباره روایت‌های جعلی و نحوه شناسایی آنها؛
۲. اخبار جعلی و روایت‌های دروغین که با دقت انتخاب‌شده، باید به منظور دستیابی به اهداف آموزشی، مورد راستی‌آزمایی و تجزیه‌وتحلیل عمومی قرار بگیرند؛
۳. ایده‌های تبلیغاتی بالقوه دارید؟

سفسطه و مغلطه

تعریف

مغلطه نوعی ارتباط جعلی اما مجاب‌کننده است که یک عبارت، بحث یا ایده نادرست را صحیح جلوه می‌دهد. غالباً در فارسی، مغلطه و سفسطه به جای یکدیگر استفاده می‌شود، اما بهتر آن است که از عبارت مغلطه استفاده کنیم.

۱۵ نوع مغلطه

۱. **شخص‌ستیزی یا حمله به شخص:** دیدگاه یک نفر را براساس خصوصیات شخصی، پیشینه، ظاهر بدنی یا سایر ویژگی‌های غیر مرتبط با استدلال وی، رد یا نقد می‌کند.

مثال: «محسن سازگارا یک جاسوس آمریکایی است و نباید به نظرات او در مورد سیاست ایران توجه کرد.»

۲. **پهلوان پنبه (مرد پوشالی):** شخص به موقعیتی حمله می‌کند که حریف در واقع آن را باور ندارد. او به جای بحث و گفتگو با استدلال واقعی، استدلال حریف را اشتباه توصیف می‌کند و به ایده‌ای حمله می‌کند که حریف هرگز قصد دفاع از آن را نداشته باشد.

مثال: «مردم ایران باید در انتخاب اینکه چه چیزی بپوشند آزاد باشند و هرکسی که می‌خواهد بدون حجاب باشد، باید آزادی انتخاب داشته باشد. استدلال مرد پوشالی در پاسخ می‌تواند این باشد: «این بدان معنا است که مردم باید برهنه بیرون بیایند و کسانی که حجاب دارند نمی‌توانند اعتراض کنند.»

۳. **توسل به جهل:** استفاده از جهل یا فقدان اطلاعات و شواهد، حمایت از استدلال مربوط به آن مسئله است.

مثال: «اگر دستگاه قضایی کسی را محاکمه نکند، پس او بی گناه است.»

٤. **دوراهی جعلی:** شخص گزینه‌های موجود در سناریوی ممکن را محدود می‌کند.

مثال: «اگر رأی دهیم، جنگ وجود نخواهد داشت و اگر رأی ندهیم، جنگ خواهد بود.»

٥. **شیب لغزنده:** این زنجیره معمولی با حرکت از یک فرضیه به ظاهر خوب یا از یک نقطه آغاز می‌شود و از طریق چند گام کوچک، به سمت یک افراط غیرممکن حرکت می‌کند.

مثال: «اگر ما قبول کنیم در مورد موشک‌های بالستیک مذاکره شود، سپس باید در مورد حقوق بشر مذاکره کنیم، پس از آن باید حقوق هم‌جنسگراها را به رسمیت بشناسیم، سپس باید ازدواج با محارم را بپذیریم، آنگاه کل کشور و اسلام نابود می‌شود.»

٦. **استدلال مدور**: دوباره فرضیات شخص را به روشی بیان کنید که به نظر می‌رسد استدلال است بدون اینکه به نتیجه‌گیری جدیدی برسید.

مثال ۱

الف: جمهوری اسلامی بهترین سیستم سیاسی جهان است.

ب: چرا؟

الف: اگر تمام سیستم‌های سیاسی جهان را تجزیه‌وتحلیل کنید، جمهوری اسلامی بهترین نظام است.

مثال ۲

الف: همه کسانی که می‌خواهند رژیم را سرنگون کنند، طرفدار جنگ هستند.

ب: چرا؟

الف: زیرا آنها از سرنگونی رژیم پشتیبانی می‌کنند و جنگ تنها راه انجام این کار است، بنابراین آنها از جنگ پشتیبانی می‌کنند.

۷. **تعمیم ناروا یا شتابزده:** اظهارنظر عمومی بدون شواهد کافی برای حمایت از آنها. افراد دچار ارائه فرضیه‌های غیرقانونی، کلیشه‌سازی، نتیجه‌گیری نادرست، زیاده‌روی یا اغراق می‌شوند.

مثال: «همه دخترانی که از خانه فرار کرده‌اند، مشکلات خانوادگی دارند.»، «شیرازی‌ها تنبل هستند.»، « همه اعضای سپاه فاسد هستند.»؛

۸. **مغالطه شاه ماهی قرمز**[1]: معمولاً با استفاده از احساساتی که به نظر می‌رسد مرتبط با موضوع است، اما در حقیقت چنین نیست، حواس افراد را پرت می‌کند؛

۹. **خودت هم همین‌طور:** «توسل به نفاق» نیز نامیده می‌شود زیرا با اشاره به نفاق در مخالف، از استدلال دور می‌شود. این روش مشکل را حل نمی‌کند، زیرا حتی منافقین هم می‌توانند حقیقت را بگویند. تمرکز بر نفاق شخص دیگر یک روش انحرافی است.

مثال

وزارت امور خارجه آمریکا: «ظلم بهائیان توسط دولت ایران نقض حقوق بشر است.»

وزارت امور خارجه ایران: «خود آمریکا ناقض حقوق بشر است.»؛

۱۰. **مغالطه علتی**: هرگونه تفکیک منطقی هنگام مشخص کردن علت را گویند. مغالطه علت را می‌توان به عنوان یک مقوله مادر برای چندین مغلطه گوناگون درمورد علل تأییدنشده در نظر گرفت؛

۱۱. **هزینه‌های غیر قابل بازگشت:** این عقیده که «به خاطر سرمایه‌گذاری که در این کار یا پروژه کرده‌ایم پس باید آن را ادامه دهیم، بدون اینکه هزینه‌های احتمالی که به واسطه این کار در آینده متحمل خواهیم شد» را درنظر بگیرید. ممکن است پس از اتمام پروژه احساس کنید موفق شده‌اید و حتی ارزش‌ها و سودآوری‌های دیگری نیز به همراه داشته باشد، اما برای توجیه هزینه‌های سرمایه‌گذاری‌شده در آن کافی نیست؛

۱۲. **به درخواست مرجع:** این اتفاق زمانی می‌افتد که از قدرت سوءاستفاده کنیم. این سوءاستفاده از اقتدار می‌تواند از چند طریق اتفاق بیفتد. ما می‌توانیم فقط به مقامات استناد کنیم و از ادله و مستندات دیگر فاصله بگیریم، با این توجیه که نظر متخصص همیشه درست است.

مثال: «جمهوری اسلامی دموکراسی است زیرا مقام معظم رهبری چنین می‌گوید.»؛

۱۳. **معادل‌سازی و ایجاد ابهام:** این اتفاق هنگامی رخ می‌دهد که یک کلمه، عبارت یا جمله به طور عمد برای سردرگمی، فریب یا گمراه‌کردن استفاده می‌شود و به این صورت است که برداشت افراد از چیزی که منظور گوینده است، متفاوت خواهد بود.

مثال: «حزب سیاسی او می‌خواهد هزینه گرانبهای مالیات شما را برای دولت خرج کند، اما حزب سیاسی من در حال برنامه‌ریزی برای سرمایه‌گذاری راهبردی در برنامه‌های مهم است.»؛

۱۴. **درخواست ترحم:** حملات شخصی و درخواست‌های عاطفی، به حقیقی یا جعلی بودن موضوع ارتباط ندارند، اما این روش به میزان حساسیت عاطفی دیگران توجه دارد. طلب ترحم اغلب به عنوان دستکاری عاطفی درنظر گرفته می‌شود.

مثال: «داعش از تلگرام برای برنامه‌ریزی قتل مردم استفاده کرد، بنابراین باید تلگرام را مسدود کنیم.»؛

---

[1] Red Herring

۱۵. **توسل به اکثریت یا مقبولیت:** در این روش شخص فرض می‌کند یک چیز درست است، زیرا افراد دیگر با آن موافق هستند.

مثال:

الف: من فکر می‌کنم علائم خیابانی برابری جنسیتی را رعایت نمی‌کنند.

ب: علائم خیابانی همیشه در همه جا یکسان بوده، بنابراین هیچ مشکلی با آنها وجود ندارد.

منابع تغذیه و الگوهای ارتباطات

با افزایش چالش‌های اجتماعی، بازیگران وابسته به دولت به احتمال زیاد از مغلطه‌های بیشتری در فضاهای عمومی آنلاین فارسی‌زبان استفاده می‌کنند. این امر به طور معمول هنگامی رخ می‌دهد که شکاف بین دولت و ملت افزایش یابد و تعداد بیشتری از مردم مشروعیت و صلاحیت رژیم را به چالش بکشند.

۱. مغلطه‌های سیاسی بیشتر در توییتر متداول هستند، درحالیکه مغلطه‌های مرتبط با موضوع سلامت بیشتر در اینستاگرام منتشر شده است؛

۲. این فعالیت‌ها را نمی‌توان سازمان‌یافته توصیف کرد مگر اینکه یک کمپین آنلاین از سوی کاربران طرفدار رژیم ایجاد شود؛

۳. حامیان رژیم غالباً از مغلطه حمله به اشخاص استفاده می‌کنند؛

٤. کسانی که از مغلطه استفاده می‌کنند، معمولاً روی اظهارات چهره‌های غربی یا غیر ایرانی متمرکز می‌شوند؛

۵. منابع تغذیه مغلطه‌ها، به‌ویژه در توییتر، علاقه چندانی به گسترش بحث‌های خود ندارند. آنها به جای پاسخ دادن به سؤالات، همان بحث را دوباره مطرح می‌کنند.

توصیه‌ها

۱. با استفاده از مثال‌های مربوط به ایران، فیلم‌های کوتاه و دو دقیقه‌ای درباره سفسطه تهیه کنید. (مهم‌ترین روش‌های سفسطه را انتخاب کنید)؛

۲. فیلم‌های اطلاعاتی ایجاد کنید و در آنها نمونه‌هایی از سفسطه‌هایی که شخصیت‌های برجسته ایرانی مانند [آیت‌الله العظمی] خامنه‌ای یا ظریف و سایر شخصیت‌های تاریخی استفاده کرده‌اند را مورد تجزیه و تحلیل قرار دهد؛

۳. برای معرفی نمونه‌هایی از مغلطه‌های سیاسی که از زمان انقلاب اسلامی بیان شده، یک کمپین توئیتری با هشتگ #مغلطه_نکنیم راه‌اندازی کنید. یک کمپین مشابه می‌تواند مباحث مربوط به سلامتی را در اینستاگرام خود مطرح کند (در مورد ایده‌های کمپین مربوط به مغلطه و هشتگ مربوطه در توییتر و اینستاگرام بحث کنید)؛

٤. پوسترهایی با عنوان «نقل قول‌ها – مغلطه‌ها» ایجاد کنید که برجسته‌ترین مغلطه‌های استفاده‌شده در این نقل‌قول‌ها را تحلیل کند؛

۵. با موضوع مغلطه، مسابقه یا بازی ایجاد کنید؛

٦. مغلطه‌های فعلی که با دقت انتخاب شده‌اند، برای اهداف آموزش عمومی مورد بررسی قرار می‌گیرند.

اخبار جعلی و بی‌اعتبار

معرفی

اخبار جعلی به معنی انتشار اطلاعات نادرست و یا گمراه‌کننده است که به سردرگمی و نگرانی عمومی منجر می‌شود و اعتماد به رسانه‌ها را به کلی کاهش می‌دهد. اخبار جعلی تمایل دارند از عناوین دروغین، اما عاطفی به عنوان طعمه برای ایجاد جذابیت و کشش جهت دریافت محتواهای گمراه‌کننده، دستکاری‌شده یا ساختگی استفاده و به طور بالقوه به اهداف خاص آسیب وارد کنند. اخبار غیر معتبر می‌توانند مخاطبان را نسبت به اخبار واقعی که از منابع رسانه‌ای مستقل منتشر می‌شود، بی‌حس و بی‌اعتنا کنند.

اصطلاحات مختلف فارسی مانند «کذب»، «دروغ پراکنی» و «شایعه پراکنی» در اشاره به اصطلاح اخبار جعلی استفاده شده است. به منظور تهیه این گزارش و تولیدات بعدی، از اصطلاح «اخبار جعلی» استفاده می‌کنیم.

مثال‌های مهم اخبار جعلی در فضای اخبار فارسی

۱. **اخبار جعلی:** ادعا می‌شود بر روی درختان در خیابان ولیعصر تهران دستگاه ضبط نصب شده است. به همین ترتیب، وجود دستگاه‌های ردیابی GPS در گذرنامه‌های ایرانی نیز نمونه‌ای از انتشار اخبار جعلی است؛

۲. **اخبار دستکاری‌شده:** در اعتراضاتی که در دی ۹۶ در سراسر ایران صورت گرفت، فیلم‌های قدیمی سال ۸۸ با این ادعا که جدید هستند دوباره منتشر شدند. به تدریج عموم مردم نسبت به صحت هر ویدئویی که از اعتراضات به اشتراک گذاشته شده بود شک کردند و بدین ترتیب در گسترده بودن تظاهرات‌ها تردید کردند؛

۳. **اخبار ساختگی:** ادعاهای مبنی بر تجاوز جنسی به مسیح علی‌نژاد در یک ایستگاه مترو در لندن. نمونه دیگری از ادعاهای بی‌پایه و اساس، تجاوز صادق صبا، مدیر سابق بی‌بی‌سی فارسی به پونه قدوسی، روزنامه‌نگار این خبرگزاری است. در یک جامعه سنتی، نجات‌یافتگان از تجاوز جنسی را همچنان مورد سرزنش قرار می‌دهند، چنین داستان‌هایی می‌توانند بسیار آسیب‌زا و دارای اثرات طولانی‌مدت باشند.

الگوهای اجرای کمپین‌های اخبار جعلی در فضاهای آنلاین فارسی‌زبان

همیشه کمپین‌های اخبار جعلی، علیه فعالان جامعه مدنی، روزنامه‌نگاران و دیگر چهره‌های تأثیرگذار دور از وطن هستند تا بتوانند به سرکوب آزادی بیان و دستکاری افکار عمومی در مورد کار و اعتبار آنها بپردازند. منابع تغذیه این اخبار شامل حساب‌های کاربری دولتی و ناشناس هستند. این کمپین‌ها از روش‌هایی مانند موارد زیر استفاده می‌کنند:

- حساب‌ها و صفحات جعلی در رسانه‌های اجتماعی که لزوماً هم سیاسی نیستند - ممکن است مربوط به هنر، ورزش و غیره باشند. این منابع برای کمپین‌های اخبار جعلی به کار گرفته می‌شوند؛
- این حساب‌های جعلی با درج نظر ذیل محتوای منتشرشده افرادی که هدف آنها هستند، پیام‌های کمپین‌های اخبار جعلی را به طور گسترده پخش می‌کنند. به عنوان مثال، کمپین‌های هماهنگ بارها صفحه فیس‌بوک «چهارشنبه‌های سفید» را هدف قرار داده و مسیح (صاحب صفحه) را متهم کردند که از اسرائیل حمایت مالی دریافت کرده است. بعضی مواقع این اظهارنظرها باعث می‌شد که صحبت از حجاب به حاشیه رانده شود و سؤال از دریافت پول مسیح از اسرائیل موضوع اصلی بحث شود؛
- منابع تغذیه، افرادی که هدفشان هستند را گمراه می‌کنند تا محتوای جعلی به اشتراک بگذارند و از این طریق آنها را تبدیل به عوامل انتشار اطلاعات جعلی می‌کنند و اعتماد عموم مردم را از بین می‌برند.

توصیه‌ها

۱. ایجاد و انتشار پوسترهای آموزشی در مورد نحوه تمایز اخبار جعلی و معتبر. این مباحث می‌توانند شامل بررسی مرجع، بررسی محتوا جهت کشف واقعیت‌ها و تحقیقات بیشتر در مورد هدف این کمپین‌های جعلی باشند؛

۲. تولید فیلم‌ها و انیمیشن‌های آموزشی همراه با تصاویر، صوت و پیام‌رسانی قوی که سواد دیجیتال کاربران را ارتقا بخشد. این تولیدات باید مسئولیت و نقش مخاطب در مقابله با انتشار بیشتر اطلاعات جعلی، دستکاری‌شده و دروغین را برجسته کند. آنها همچنین می‌توانند منابع موثقی را به مخاطبان معرفی کنند که در صورت شک و تردید به آنها مراجعه کنند؛

۳. انتشار نمودارهای گرافیکی رسانه‌ای که نشریات فارسی‌زبان را براساس میزان حقیقت‌محور بودن آنها نشان می‌دهد؛

٤. تجزیه‌وتحلیل کل چرخه و پیامدهای آن با هدف جدا کردن اخبار جعلی و کمپین‌های مشخص‌شده. آشنا کردن کاربران با مثال‌ها و رسانه‌هایی که به احتمال زیاد با آنها آشنا هستند (به عنوان مثال یک فیلم مستند از آیت الله شیرازی که در آن زنان را با حیوانات برابر دانست، در طیف وسیعی به اشتراک گذاشته شد و خشم عمومی را برانگیخت، درحالیکه ویدئوی اصلی به سرزنش کسانی می‌پرداخت که زنان را با حیوانات برابر می‌دانند.)

۵. دعوت از اهداف سابق یا دائمی اخبار جعلی مانند پونه قدوسی و رویا هاکاکیان به منظور به اشتراک گذاشتن داستان‌های خود، تأثیراتی که در زندگی آنها داشته است و نکاتی برای شناسایی داستان‌های دروغین. ما همچنین می‌توانیم واکنش آنها دربرابر نمونه‌های رایج چنین خبرهایی (مانند فیلم مستند آیت الله شیرازی) را ضبط کنیم. این امر ممکن است آنهارا ترغیب کند تا داستان‌های خودشان را نیز مطرح کنند. این جلسات می‌توانند در اینستاگرام و فیس‌بوک به صورت زنده پخش شوند؛

٦. افزایش آگاهی عمومی و ایجاد همدلی از طریق دعوت از کاربران برای به اشتراک گذاشتن اینکه چه نوع داستان‌های جعلی را پذیرفتند، احساس آنها درباره آن چیست و چگونه آموختند که این مورد جعلی است. این جلسات می‌توانند در اینستاگرام و فیس‌بوک به صورت زنده پخش شوند؛

۷. دعوت از افرادی که به دلیل حجم انبوه اطلاعات جعلی که درمورد آنها منتشر شده، تجربه سکوت یا ترک رسانه‌های اجتماعی را دارند و اشتراک حکایات آنها به صورت عمومی یا خصوصی (به عنوان مثال زنانی که در صفحه چهارشنبه‌های سفید عکس بدون حجاب خود را به اشتراک می‌گذارند و به همین دلیل آماج نظرات تند و زننده می‌شوند). این دعوت، فرصتی برای شنیدن این صداها در یک محیط امن فراهم می‌کند. علاوه بر این، ما می‌توانیم بعداً سؤال کنیم که آیا به‌اشتراک‌گذاشتن داستان‌های آنها تغییر و یا پیشرفتی در رنج آنها ایجاد کرده است.

۸. ایجاد یک کمپین در رسانه‌های اجتماعی به منظور افزایش آگاهی در مورد موضوع و تشویق افراد به مشارکت در آن. نامی را برای کمپین انتخاب کنید که هرکس بتواند با آن ارتباط برقرار کند و از استفاده از زبان و لحن نخبگان خودداری کنید.

آزار و اذیت و تعرض آنلاین

معرفی

آزار و اذیت آنلاین (سایبری) شامل بیانات یا اقدامات پیوسته و آزاردهنده در طول یک بازه زمانی پایدار از طریق رسانه‌های اینترنتی است. هدف این تعرضات یک فرد و یا گروهی از افراد خاص هستند و موجب ناراحتی، شرمساری یا تحقیر عاطفی در اهداف می‌شود. آزار و اذیت سایبری شامل انواع رفتارهای آسیب‌زا مانند (۱) ارسال پیام‌های نفرت‌انگیز، افترا، جعل هویت،

داکسینگ[1]، حملات سایبری، (۲) انتشار عمومی آدرس خانه و محل کار و سایر اطلاعات شخصی فرد، (۳) تهدیدهای مربوط به خشونت، مرگ و تجاوز جنسی به قربانیان و یا عزیزانشان است. در بعضی مواقع آزار و اذیت آنلاین می‌تواند به حالت آفلاین، حمله فیزیکی و موارد دیگر ارتقاء یابد. برخی از انواع آزار و اذیت آنلاین، تمایل به سمت رفتار غیر قانونی یا جنایی است. رایج‌ترین مکان‌هایی که آزار و اذیت آنلاین در آنها رخ می‌دهد عبارتند از:

- رسانه‌های اجتماعی، به ویژه اینستاگرام، توییتر و فیس‌بوک که در مورد ایران چندان مهم نیستند؛
- پیام‌رسان‌های فوری (از طریق خدمات ارائه‌دهنده ایمیل مانند گوگل هنگ اوتس[2]، پیام‌رسان‌های رسانه‌های اجتماعی مانند ایمو، اینستاگرام، واتساپ، تلگرام و برنامه‌های دیگر)؛
- پیامک؛
- بخش نظرات وب‌سایت‌ها، پست‌های رسانه‌های اجتماعی و غیره؛
- پست الکترونیک.

ترول‌ها[3] و تعرض آنلاین

آزار و اذیت آنلاین می‌تواند از سوی ترول‌ها و اوباش سایبری ایجاد شود. آنها گفتار و رفتارهای آسیب‌زا را برای اهداف خود تنظیم می‌کنند. در مورد ایران، ترول‌های هماهنگ اغلب با اهداف زیر، به دنبال تسلط بر روایت‌های رسانه‌های اجتماعی و حتی کانال‌های تلویزیونی دولتی هستند:

۱. تضعیف اعتبار قربانیان از طریق دستکاری افکار عمومی؛
۲. ساکت کردن مخالفان؛
۳. جلب توجه و اعتبار برای طرف مقابل (به عنوان مثال مقاله‌های شریعتمداری در روزنامه کیهان، با تکیه بر شواهد بی‌اساس و شخصیت‌های ساختگی و غیر حقیقی در حمایت از داستان‌های دروغین، دستکاری‌شده و جعلی، مشهور شده است).
٤. آزار و اذیت آنلاین ترول‌ها به اشکال مختلف ظاهر می‌شود که از جمله آنها می‌توان به چند نمونه زیر اشاره کرد:

- کمپین‌هایی که هدفشان لکه‌دار کردن سوژه از طریق انتشار روایت‌های دروغین درباره زندگی شخصی و حرفه‌ای یک فرد است و اغلب با استفاده از تصاویر فتوشاپ‌شده به اعتبار آنها خدشه وارد می‌کنند. این پیام‌های نادرست یا غیر دقیق از طریق کمپین‌های رسانه‌های اجتماعی (هشتگ‌های جدید، احیای هشتگ‌های قدیمی یا سرقت هشتگ‌های فعلی) تبلیغ و در رسانه‌ها و وب‌سایت‌های طرفداران رژیم بازیافت و تقویت می‌شوند؛
- انجام بازی‌های دیپلماتیک با قربانیان: در حالیکه ترول‌ها با ارسال پیام‌های ارعاب‌کننده به سوژه حمله می‌کنند، عده‌ای از طریق ارسال پیام‌های مستقیم به هدف نزدیک می‌شوند تا بازی «پلیس خوب» را راه بیاندازند و وانمود کنند که با حسن نیت کمک می‌کنند. این مورد اغلب شامل برقراری ارتباط مناسب با افراد معقول است، به طوری که هدف تصمیم خود را تغییر می‌دهد. پیام اصلی اما همان «موضع خود را در مورد این موضوع تغییر دهید، آن تصویر، ویدئو یا ... را بردارید و من آزار و اذیت را متوقف خواهم کرد» است.

---

[1] Dox/ داکسینگ یا رسواسازی یک حمله سایبری است که شامل جستجوی هویت واقعی کاربر اینترنتی است. پس از جستجوی هویت، مهاجم این اطلاعات شخصی را فاش می‌کند به‌گونه‌ای که دیگران به‌منظور عملی ساختن اقدامات خرابکارانه خود، این اطلاعات را مورد هدف قرار دهند. داکسینگ، درواقع تجزیه و تحلیل اطلاعاتی است که قربانی به‌عنوان پستی در اینترنت قرار داده و مهاجم برای تعیین هویت و اذیت و آزار-های بعدی این شخص، آن‌ها را مورد کنکاش قرار می‌دهد.

[2] Google Hangout/ یکی از بهترین و قدرتمندترین اپلیکیشن‌های چت برای سیستم عامل اندروید می‌باشد که محصولی از شرکت گوگل است.

[3] Troll/ در گفتمان اینترنتی به افرادی گفته می‌شود که با رفتار مخرب در فضای وب به دنبال جلب نظر کاربران، ایجاد تشنج و بیان مطالب محرک و توهین‌آمیز هستند.

- ارائه گزارش‌های اشتباه به پلتفرم‌های رسانه‌های اجتماعی درباره تخلف از استانداردهای جامعه. الگوریتم‌های پلتفرم‌ها به بازی گرفته می‌شوند و به اشتباه منجر به حذف و یا تعلیق خودکار یک حساب کاربری می‌شود. به عنوان مثال، تصویر شادی صدر از نشستن بر روی یک صندلی که دارای تصاویر مذهبی است، در سال ۲۰۱۶ از سوی اینستاگرام حذف شد و قبل از اینکه بتواند عکس را بازگرداند، حدود ۷۲ ساعت از دسترس خارج شد.

عاملان

حساب‌های کاربری وابسته به دولت به طور فزاینده‌ای در توییتر و اینستاگرام حضور دارند و در کمپین‌های حمله علیه جامعه مدنی، روزنامه‌نگاران و افراد دور از وطن شرکت می‌کنند. آنها در انواع گوناگون ظاهر می‌شوند و می‌توانند کاربران معمولی را دچار اشتباه کنند. در حالیکه هیچ روش استانداردی برای تمایز اکانت‌های دولتی وجود ندارد، نشانه‌های مشترک این حساب‌ها در اینستاگرام شامل موارد زیر است:

- آنها بندرت از تصویر انسانی به عنوان تصویر نمایه خود استفاده می‌کنند. بسیاری از آنها تصویر مقام معظم رهبری را به عنوان عکس پروفایل خود قرار می‌دهند که با اصطلاحات مذهبی و آیاتی از قرآن همراه شده است؛
- زبان مورد استفاده این حساب‌ها خشن‌تر و مبتذل‌تر از سایر کاربران است. احتمال زیادی وجود دارد که این حساب‌ها تهدید به مرگ و تجاوز جنسی علیه زنان را منتشر کنند؛
- نام حساب‌ها غالباً دارای تعابیر مذهبی و سیاسی است؛
- استفاده از نام و تصاویر زن در این پروفایل‌ها بسیار نادر است؛
- چندین حساب با همین نام و پسوندهای عددی پی‌درپی، نشان می‌دهد که ممکن است از سوی همان شخص (افراد) ایجاد شده باشد. این امر به ویژه در مواردی رخ می‌دهد که حساب‌های قدیمی به دلیل نقض شروط، از سوی اینستاگرام گزارش و حذف می‌شوند؛
- تصاویر ارسالی در این حساب‌ها اغلب حاکی از یک موضوع مذهبی است. به عنوان مثال، تصاویر زیادی در حرم‌های مقدس شیعیان در شهرهای مذهبی ایران یا عراق گرفته شده است. تعداد قابل‌توجهی از آنها، آشکارا به عنوان «مدافع حرم» شناخته می‌شوند؛
- اغلب حساب‌های کم‌فعالیتی هستند که گفته می‌شود فقط با هدف آزار و اذیت آنلاین ایجاد شده است. کاربرانی که این حساب‌ها دنبال می‌کنند غالباً دنبال‌کنندگان زیادی دارند. در بسیاری از موارد، آنها هیچ دنبال‌کننده و دنبال‌شونده‌ای ندارند و هرگز تصویری را ارسال نکرده‌اند.

این بازیگران در توییتر از روش‌های مختلفی استفاده می‌کنند و در انواع پروفایل‌های گوناگون ظاهر می‌شوند. نام‌ها و روش‌ها پیچیده‌تر هستند. الگوهای مشارکت می‌تواند تا حدی متفاوت باشد و تنها نظارت مداوم بر این حساب‌ها می‌تواند جهت‌گیری سیاسی آنها را نمایان سازد. همچنین این اجتماعات توییتری دارای یک شعبه برون مرزی هستند که محکم و آشکار از [سردار سرلشگر] سلیمانی و رژیم ایران دفاع می‌کنند؛

- علاوه بر این، در تمام پلتفرم‌های رسانه‌های اجتماعی حساب‌های کاربری ناشناسی وجود دارد که از نمادهای ناسیونالیستی ضد جمهوری اسلامی مانند شیر و خورشید استفاده می‌کنند تا خود را به عنوان مخالفان رژیم معرفی کنند. این امر باعث می‌شود استدلال‌های آنها در بحث‌ها و مبارزات انتخابی قابل قبول باشد.

توصیه‌ها (رویکرد چند ذی‌نفعی)

برای کاربران

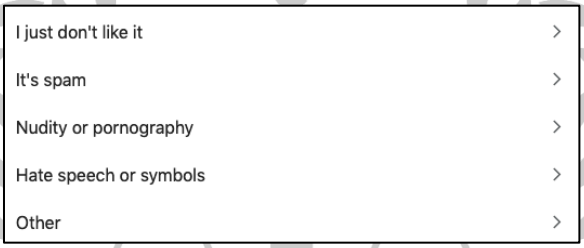
۱. قبل از اینکه بخواهید درگیر بحث‌هایی شوید که ممکن است شما را با ترول و سوءاستفاده درگیر کند، خطرات مربوط به زندگی شخصی و حرفه‌ای خود را با استفاده از شاخص ریسک (به پیوست ۱ مراجعه کنید) ارزیابی کنید؛

۲. نمره ریسک خود را در نظر بگیرید و در صورت امکان، بدون نام بردن از دردسرسازان، درباره آنها صحبت کنید. به جای آن، به سوءاستفاده، جزئیات و حوزه بحث اشاره کنید؛

۳. با سایر ابزارهای کاهش سوءاستفاده آشنا شوید. اگر هدف آزار و اذیت قرار دارید، از ابزارهای دیگری مانند گزارش، مسدود کردن کلیدواژه یا ایموجی، مسدود کردن حساب کاربری و موارد دیگر استفاده کنید. مثلا:

Twitter > Setting > Muted Keywords (add/remove)
Twitter > Setting > Blocked Accounts (add/remove/report)
Twitter > Setting > Muted Accounts (add/remove/report)

Instagram > click on a picture/video > Report Inappropriate > choose from options



به صفحه پروفایل خود در اینستاگرام بروید و ☰ را بزنید؛

در بخش تنظیمات ⚙ را بزنید؛

امنیت و حریم خصوصی را بزنید؛

کنترل کامنت‌ها را بزنید؛

ذیل فیلترینگ کامنت‌ها، فیلتر کردن کیبورد را بزنید؛

گزینه کیبوردهای پیش فرضی که مرتبط با زبان پروفایل شما هستند را انتخاب کنید.

٤. بررسی کنید چه کسی می‌تواند برای شما پیام ارسال کند، شما را در عکس تگ کند، شما را به عنوان مخاطب و غیره اضافه کند و اطمینان حاصل کنید که با این تنظیمات راحت هستید؛

٥. به شبکه پشتیبانی آنلاین خود دسترسی پیدا کنید. نیازی نیست خودتان رنج ببرید. شبکه پشتیبانی می‌تواند به مقابله با آنها بپردازد و یا به سادگی در آنجا حضور داشته باشد؛

٦. آزار و اذیت مداوم آنلاین می‌تواند پیامدهای طولانی‌مدت بر سلامت روانی و احساس امنیت شما داشته باشد. اگر آزار و اذیت منجر به اختلال در عملکرد روزانه شما (احساس پریشانی، مشکل در غذا خوردن یا خوابیدن) شد، گزینه درمان را مدنظر بگیرید.

برای اجتماع و جامعه مدنی

۱. تأثیرگذاران رسانه‌های اجتماعی می‌توانند نقش مهمی در بسیج‌کردن پایگاه‌های خود علیه گفتارهای آسیب‌زا و سوءاستفاده سایبری داشته باشند (مثال اخیر: گزارش و غیر فعال کردن حساب اینستاگرام تتلو)؛

۲. به کاربران در مورد گزینه‌های موجود در سوءاستفاده آنلاین آموزش دهید. یک کمپین با عنوان «بیاموز و به‌اشتراک بگذار»[1] راه‌اندازی کنید که در آن کاربران تجربیات خود را درباره استفاده از ابزارهای ضد سوءاستفاده به‌اشتراک بگذارند. این امر می‌تواند به اندازه بحث «مسدود کردن» مهم و جدی باشد و می‌تواند با هشتگ #بلاک‌کنیم‌یانکنیم عنوان شود، یا به افزایش آگاهی افراد در مورد چگونگی حمایت از کسانیکه مورد آزار و اذیت آنلاین قرار دارند پرداخته شود؛

۳. طرفداران گروه‌های هدف را ترغیب کنید تا از همان قدرت ارتباطی رسانه‌های اجتماعی استفاده کنند و در مقابل رفتاری که دیگران را وادار به سکوت می‌کند بایستند و به انتشار مطلب، محکومیت یا تشکیل یک سازمان علیه آنها بپردازند. این موضوع می‌تواند در قالب یک کمپین در شبکه‌های اجتماعی باشد. به عنوان مثال هشتگ #WeAreAllMasih و درخواست از مردم برای بازتوییت آن؛

٤. ابزار و فیلم‌های آموزشی در مورد چگونگی تشخیص و مقابله با آزار و اذیت آنلاین و حمایت از قربانیان تولید کنید.

حملات سایبری

در طول یک دهه گذشته، هکرهای وابسته به دولت از حملات بدون هدف، به هک‌های هدفمند ارتقا پیدا کرده‌اند. مورد اخیر، طرحی است که در آن، مهاجمان با هدف حملات شخصی، تحقیقات گسترده‌ای در مورد علایق سوژه‌های خود انجام می‌دهند. (به جزئیات بیشتر در گزارش CERTFA، ۲۰۱۸ مراجعه کنید)

چندین آژانس ایرانی مانند وزارت اطلاعات، پلیس سایبری (فتا) و سپاه پاسداران، در زمینه امنیت سایبری فعال هستند. بحث در مورد ارتش سایبری ایران بیشتر مربوط به هکرهای وابسته به سپاه (به‌ویژه واحد اطلاعات) است. با توجه به فعالیت‌های گذشته آنها چنین تصور می‌شود که این هکرها در وهله اول ایرانیان خارج از کشور را هدف قرار می‌دهند، در حالیکه هکرهای وزارت اطلاعات بیشتر افراد داخل ایران را هدف قرار می‌دهند و پلیس فتا مسئول مبارزه با جرایم سایبری مانند پولشویی است.

در زیر تهدیدات حملات سایبری وابسته به دولت، تحت سه دسته تقسیم شده است:

(۱) حملات بدافزارها؛

(۲) حملات فیشینگ؛

(۳) نشت اطلاعات وب‌سایت‌ها.

حملات بدافزارها

بدافزار واژه‌ای است برای انواع ویروس، کرم و نرم‌افزار جاسوسی. دو نوع حمله بدافزاری داریم: عمومی و هدفمند.

حملات عمومی

حملات عمومی غالباً شامل توسعه و توزیع نرم‌افزارهای جاسوسی مربوط به تلفن‌های همراه مردم برای جمع‌آوری اطلاعات شخصی به صورت انبوه و با هدف کلی جمع‌آوری اطلاعات عمومی است. تلگرام طلایی، موبوگرام و اندرومدا[2] از نمونه‌های اخیر چنین حمله‌هایی هستند. (برای تجزیه‌وتحلیل بیشتر به این گزارش مراجعه کنید)

تلگرام طلایی و موبوگرام به ترتیب از سوی وزارت اطلاعات و نیروهای امنیتی و براساس برنامه اصلی تلگرام ساخته شده‌اند. استفاده از این برنامه‌ها کاربران را در معرض خطر نظارت از سوی دولت قرار می‌دهد.

---

[1] Learn & Share campaign

[2] Andromedaa/ برنامه کاربردی برای اندروید و آیفون و آیپد جهت افزایش دنبال‌کننده، لایک و کامنت در اینستاگرام و افزایش عضو در تلگرام

اندرومدا در ابتدا یک پروژه مستقل بود که به منظور کمک به مشتریان در افزایش دنبال‌کنندگان و تعامل در اینستاگرام طراحی شده بود. اندرومدا پس از آن با تسهیل سرقت گسترده اطلاعات حساب کاربری از کاربران اینستاگرام، به یک ابزار نظارتی دولتی تبدیل شد. با استفاده از داده‌های به‌دست‌آمده از این برنامه‌ها و برنامه‌های دیگر، نهادهای دولتی می‌توانند پایگاه داده‌های گسترده‌ای تهیه کنند که دارای اطلاعات مهمی در مورد شهروندان است. این مسئله هنگامی مهم می‌شود که اطلاعات سرقت‌شده متعلق به افراد مشهور و فعال باشد.

حملات هدفمند

حملات هدفمند، سفارشی هستند و هدف آنها آلوده‌کردن دستگاه‌های الکترونیکی سوژه‌های خاص، نظارت بر فعالیت‌های و نفوذ در شبکه‌های اجتماعی و اختصاصی آنها است. معمولاً قبل از حملات، از طریق روش‌های مختلف مهندسی اجتماعی و داده‌کاوی، اطلاعات مربوط به سوژه‌ها به خوبی جمع‌آوری می‌شود. در این حملات، اطلاعات شخصی اهداف مانند شغل، موقعیت جغرافیایی (ساعت کار و خواب)، درگیری‌های حرفه‌ای و ارتباطات (شخصی یا شغلی) برای مهاجمان شناخته شده است.

مثال: فرض کنید که دستگاه روزنامه‌نگار الف آلوده شده است و اطلاعات حساس وی با استفاده از بدافزار از دستگاه تلفن همراه وی سرقت می‌شود. سپس این بدافزار بطور مخفیانه پیوندها و فایل‌های مخرب خود را با استفاده از مخاطبان تلفنی الف، ایمیل و برنامه‌های پیام‌رسان فوری به همکاران او در «خبرگزاری ب» ارسال می‌کند. در نتیجه هکرها می‌توانند از این حمله هدفمند به حساب‌ها و اطلاعات تعدادی از روزنامه‌نگاران در خبرگزاری ب دسترسی داشته باشند.

حملات فیشینگ

در سال‌های اخیر، فیشینگ یکی از اصلی‌ترین و موفق‌ترین روش‌های حمله سایبری از سوی هکرهای وابسته به دولت بوده است. حملات فیشینگ از طریق هر بستر و دستگاهی قابل اجرا هستند. سناریوهای زیر از جمله حملات رایج فیشینگ است:

۱. **ارسال پیوندهای فیشینگ از طریق ایمیل:** رایج‌ترین روشی است که در آن مهاجم تعداد زیادی از کاربران اینترنت را با استفاده از پیوندهای فیشینگ اسپم[۱] می‌کند، که اغلب منجر به ورود به صفحات جعلی می‌شود. این روش در سال‌های اخیر به طور گسترده مورد استفاده قرار نگرفته است، اما در اعتراضات جنبش سبز در سال ۸۸ بسیار رایج بود؛

۲. **ارسال پیوندهای فیشینگ از طریق یک حساب در معرض خطر:** مهاجم برای ارسال لینک‌های فیشینگ به آدرس ایمیل‌های موجود در لیست مخاطبان خود (همکاران ، دوستان و غیره)، از یک ایمیل هک‌شده استفاده می‌کند، بنابراین دامنه عملیات را گسترش می‌دهد. ازآنجائیکه ایمیل از طرف کسی است که آنها می‌شناسند، احتمال کلیک بر روی این پیوندها بسیار بیشتر است؛

۳. **ارسال پیوندهای فیشینگ از طریق پیامک:** این روش از شماره تلفن‌های بین‌المللی برای ارسال لینک‌های فیشینگ استفاده می‌کند. نفوذ به حساب‌های آی کلود آیفون نتیجه این روش است که مستلزم ارسال پیامک‌های جعلی به سوژه‌هایی است که به آنها اطلاع می‌دهد حساب‌های آنها به حالت تعلیق در آمده و نیاز به فعال‌کردن مجدد دارد؛

٤. **مهندسی اجتماعی و کلاهبرداری برای به خطرانداختن کدهای تأیید صحت:** این روش به‌ویژه برای روزنامه‌نگاران خارج از کشور موفقیت‌آمیز بوده است. هکرها به بهانه‌هایی مانند جلسات فوری، اواخر شب تماس تلفنی

---

[۱] Spam/ سوءاستفاده از سیستم انتقال پیام است (شامل اکثر وسایل انتشار رسانه‌ای، سیستم‌های تحویل دیجیتال) جهت ارسال پیام هایی که گیرنده هیچ خواسته یا علاقه‌ای برای دریافت آنها ندارد

می‌گیرند تا هدف را در فاش‌کردن کدهای تأیید صحن خود فریب دهند. با این کار، آنها برای دستیابی به حساب سوژه، دیگر نیاز به دور زدن کدهای دومرحله‌ای تأیید هویت ندارند؛

۵. **حمله هموگرافی:** یکی از پیچیده‌ترین سبک‌ها است که در آن آدرس وب‌سایت کاملاً صحیح به نظر می‌رسد، اما در واقع غیر قانونی است. نمونه اخیر، هک‌کردن حساب‌های مربوط به سازمان «جمعیت امام علی (ع)» در ایران است. مهم‌ترین نکته این است که بازیابی رمزهای عبور گوگل نباید از طریق شماره تلفن انجام شود؛

٦. **استفاده از خدمات قابل اعتماد:** در این رویکرد، هکرها از خدمات رایج برای حملات فیشینگ خود و برای جلب اعتماد اهداف استفاده می‌کنند. آخرین نمونه از این نوع حمله را می‌توان در گزارش CERTFA مشاهده کرد که بیانگر حمله به فعالان سیاسی و افراد حاضر در برجام و تحریم‌های اقتصادی علیه ایران است. در این حملات، هکرهای مورد حمایت دولت از خدمات گوگل استفاده کردند تا اهداف را فریب دهند که صفحه جعلی، همان صفحه حقیقی ورود به جی‌میل آنها بوده است.

نشت داده‌های وب‌سایت‌ها

یکی از اصلی‌ترین آسیب‌پذیری‌های بیشتر سازمان‌ها و طرح‌های جامعه مدنی در ایران، امنیت وب‌سایت‌ها و سرویس‌هایی است که از آنها برای انتشار و توزیع محتوا استفاده می‌کنند. آسیب‌پذیری در سرورهای وب‌سایت‌ها می‌تواند منجر به نشت داده‌های حساس شود. در این حالت، جزئیات همکاران یک وب‌سایت و ارتباط با مخاطبانشان می‌تواند منجر به دستگیری و بازداشت بیشتر شود. کاربران وب‌سایت‌های هک‌شده در معرض خطر حملات بدافزاری و فیشینگ قرار دارند.

وب‌سایت‌های فارسی اغلب پروتکل‌های امنیت سایبری را به طور کامل رعایت نمی‌کنند. تا زمانیکه این وضعیت ادامه داشته باشد، هکرهای تحت حمایت دولت به بهره‌برداری از این آسیب‌پذیری‌ها ادامه خواهند داد. به عنوان مثال، بسیاری از سازمان‌ها و گروه‌های ایرانی برای مدیریت محتوای خود وب‌سایت‌های مبتنی بر WordPress دارند که این امر منجر به ایجاد افزونه‌های منقضی‌شده یا سایر آسیب‌پذیری‌های سیستم شده است.

توصیه‌ها

۱. ایجاد اینفوگرافیک، فیلم و سایر ابزارهای آموزشی درباره برجسته‌ترین روش‌های جرایم سایبری مانند فیشینگ یا مهندسی اجتماعی، خطر استفاده از برنامه‌های کاربردی شخص ثالث[۱]، نصب برنامه‌های غیر آشنا، حملات هموگرافی، استفاده از موبوگرام، تلگرام طلایی و تلگرام اصلی و راه‌هایی برای مقابله از قبیل به‌روزرسانی سیستم‌های مدیریت محتوای وب، رمزهای عبور پیچیده، تأیید دو مرحله‌ای، خاموش کردن برخی از امکانات برنامه‌های محبوب مانند موقعیت مکانی گوگل و واتساپ که می‌توانند علیه کاربران بکار گرفته شوند، دستورالعمل‌های گام‌به‌گام برای دسترسی به اطلاعات حساس در صورت آلوده شدن به بدافزار یا نمونه‌هایی از موبوگرام و تلگرام طلایی، ایجاد و پیروی از پروتکل‌های امنیتی مناسب و داشتن یک نرم‌افزار آنتی‌ویروس که به طور منظم به‌روزرسانی می‌شود؛

۲. ایجاد یک شاخص ریسک که می‌تواند سطح ریسک یک کاربر را براساس چندین عامل مشخص کند. (نمونه سؤالات پیوست ۱ را مشاهده کنید)

---

[۱] Third Party/ سرویس یا برنامه‌ای است که نه شما ساخته‌اید و نه شرکت طرف حساب شما. یا نه شما می‌شناسید و نه شرکت اصلی طرف حساب شما. غالباً از سوی هکرها ایجاد می‌شود بنابراین ابتدا گوگل برای نصب آن هشدار می‌دهد.

۳.ایده‌های تبلیغاتی بالقوه دارید؟

پیوست ۱/ شاخص ریسک

این بخش، سؤالات اولیه و مهم فهرست جامع ریسک را پیشنهاد می‌دهد که افراد می‌توانند به آن مراجعه کرده و امتیاز ریسک خود را ارزیابی کنند. این سؤالات به آنها کمک می‌کند تا درک روشنی از خودشان در زمینه میزان تحمل خطرات ناشی از سوءاستفاده آنلاین و حملات سایبری داشته باشند.

برای شروع، از خود بپرسید: برای شما چه اهمیتی دارد؟ به طور خلاصه: دارایی‌ها، تهدیدات و حفاظت‌هایی که نیاز دارید را بشناسید.

این شاید بیشتر مربوط به کار روزنامه‌نگاران و فعالانی باشد که به صورت مداوم درباره مضامین حساس اجتماعی و سیاسی اظهارنظر می‌کنند. البته نمی‌توان هر عکس‌العمل یا حادثه‌ای را پیش‌بینی کرد. در فضای سایبری، چیزهای غیرقابل پیش‌بینی زیادی وجود دارد، اما موارد آموزنده‌ای نیز وجود دارد که افراد می‌توانند به کار ببرند تا آسیب‌هایی که ممکن است در پی داشته باشد را تا حدودی کاهش دهند. بنابراین، پیش از انتشار هر مورد بحث‌برانگیز یا راه‌اندازی یک کمپین حساس، مجموعه‌ای از سؤالاتی وجود دارد که باید برای آنها پاسخی داشته باشند:

۱. پیامی که می‌خواهید به آن توجه کنید چیست؟

این سؤال بعداً به شما کمک می‌کند به یاد آورید که چرا مورد آزار و اذیت یا حمله قرار گرفته‌اید و راهبرد تقابل آن چیست.

۲. چه کسی یا چه چیزی ممکن است سعی کند به شما حمله کند و یا شما را به عقب براند و چگونه؟

در اواسط حملات، ممکن است بررسی دقیق حساب‌هایی که به شما حمله می‌کنند یا با شما مخالف هستند، به شما کمک کند. بررسی این موضوع ممکن است به تشخیص اینکه چه کسی شما را آزار می‌دهد کمک کند.

۳. در صورت بروز واکنش شدید، از چه چیزی می‌خواهید محافظت کنید و احتمال محافظت از آن چقدر است؟ به عبارت دیگر، به راه‌هایی فکر کنید که پروفایل آنلاین شما علیه شما استفاده شود.

در صورت بروز سوءاستفاده آنلاین، ممکن است دارایی‌های قابل‌توجه مشترک مانند داده‌های شخصی و کاری، ارتباطات و موارد دیگر باعث ایجاد مشکلاتی شود. از خودتان بپرسید که آیا نگران انتشار آنلاین اطلاعات شخصی خود (آدرس منزل، میزان درآمد، اعضای خانواده در ایران و غیره) هستید؟ آیا نگران امنیت جسمی خود هستید؟

دارایی‌هایی که ممکن است نیاز به مراقبت ویژه داشته باشد شامل موارد زیر است:

- اطلاعات کارت اعتباری (خود و اعضای خانواده)؛
- داده‌های بانکی: شماره حساب، شماره‌های مسیریابی، نام کاربری و رمزهای عبور بانکداری الکترونیکی؛
- اطلاعات شناسایی شخصی: شماره تأمین اجتماعی، تاریخ تولد، داده‌های درآمد، شماره گذرنامه، گواهینامه رانندگی یا شماره ملی؛
- مالکیت معنوی؛
- اطلاعات و ارتباطات حساس شخصی یا شغلی: ایمیل و متونی که می‌توانند برای هتک حرمت، باج‌خواهی یا زندانی کردن شما (اگر در داخل ایران هستید) مورد استفاده قرار گیرند؛
- اطلاعات حساس یا فعالیت‌هایی که می‌تواند شما را با کارفرمای خود، دولت، مجریان قانون یا سایر افراد ذی‌نفع دچار مشکل کند؛

- برنامه‌های سفر که می‌تواند برای هدف قرار دادن شما یا افرادی که با شما سفر می‌کنند، مورد استفاده قرار گیرد؛
- سایر داده‌های شغلی یا شخصی که از نظر مالی یا عاطفی ضروری هستند (به عنوان مثال عکس‌های خانوادگی)؛
- هویت شما، اگر تمایل دارید به هر دلیلی برای حفاظت از خودتان در اینترنت ناشناس بمانید؛
- در مورد ریسک چه اقدامی می‌خواهید انجام دهید؟

به عبارت دیگر، برنامه امنیتی شما چیست؟ (جزئیات بیشتر پس از جلسه ما در مورد امنیت دیجیتال در اینجا درج خواهد شد) و چقدر می‌توانید برای انجام دادن یا ندادن آن ایستادگی کنید؟ در صورت عدم موفقیت، عواقب آن چقدر بد است؟

- بعد از هر حادثه، دوباره ارزیابی کنید و بسنجید که چه میزان خطر کاهش یافته است و در آینده چه چیزهایی را می‌توانید بهبود ببخشید.