گزارش مشاوره ای کمیته حمایت از روزنامه نگاران: استفاده از نرم افزار جاسوسی پگاسوس به منظور هدف قراردادن خبرنگاران و جامعه مدنی

در گزارشی که توسط سیتیزن لب Citizen Lab در روز ۲۷ شهریور مصادف با ۱۸ سپتامبر منتشر شده است ، Citizen Lab گزارش می دهد که توانسته به کارگیری این جاسوس افزار را در بیش از ۴۵ کشور جهان ردیابی کند. پگاسوس نرم افزار جاسوسی است که برای هدف قراردادن گوشی های تلفن همراه طراحی شده است. این نرم افزار جاسوسی می تواند گوشی تلفن همراه را به یک ایستگاه ردیابی و شنود تبدیل کند.

براساس این گزارش، این نرم افزار علیه گروه وسیعی از خبرنگاران و فعالان جامعه مدنی در مکزیک، عربستان سعودی، بحرین، مراکش، توگو، اسرائیل، ایالات متحده آمریکا و امارات متحده عربی به کار گرفته شده است.

محققان قبلاً توانسته بودند به کارگیری نرم افزار جاسوسی پگاسوس را در دفعات گسترده شناسایی کنند که از آن جمله می توان به کارگیری این نرم افزار را علیه خبرنگاران در مکزیک و همچنین علیه فعالان حقوق بشر در عربستان سعودی اشاره کرد.

به کارگیری این جاسوس افزار در بیش از ۴۵ کشور جهان پیامدهای مهمی را برای خبرنگاران هم از نظر امنیت خود خبرنگاران و همچنین امنیت منابع خبری آنها به همراه داشته است.

این جاسوس افزار، این قدرت را به شنودکنندگان می دهد تا بتوانند تمامی اطلاعات فعلی و اطلاعاتی را که در آینده به روی گوشی تلفن وجود دارد را شنود، ضبط و جمع آوری کنند. این عملکرد تمامی تماس ها، اطلاعات اپلیکیشن های پیامکی و اطلاعات لحظه به لحظه مکان شخص را شامل می شود. این جاسوس افزار همچنین قادر است از فاصله زیاد، دوربین و میکروفن گوشی را فعال کرده و خبرنگار موردنظر و محیط پیرامون او را تحت نظارت و بررسی قرار دهد.

پگاسوس قابلیت نصب به روی سیستم های عامل اندروید، بلک بری او اس و آی او اس را دارد و این در حالی است که فرد مورد هدف، هرگز متوجه نصب این نرم افزار به روی گوشی خود نخواهد شد.

خبرنگاران تنها در موارد محدود و فقط درحالی که یک متخصص امور فنی گوشی همراه آنان را بررسی کند، متوجه نصب این نرم افزار خواهند شد.

پگاسوس از راه های مختلف می تواند به روی گوشی همراه نصب شود. خبرنگاران باید از این روش ها آگاه باشند تا بتوانند اقدامات لازم را در جهت جلوگیری و همچنین حفظ امنیت خود و منابع خبریشان اتخاذ کنند.

- **حملات فیشینگ یا سرقت آنلاین با طراحی ویژه**

در این روش فیشرها و یا سارقان آنلاین پیام های ویژه ای را برای هدف قراردادن یک خبرنگار خاص طراحی میکنند. این پیام ها معمولاً اضطراری هستند و یک لینک (پیوند) و یا یک سند را برای خبرنگار ارسال می کنند. متن این پیام ها خبرنگار را ترغیب می کند که به روی لینک کلیک کند. این پیام ها معمولاً در اشکال مختلف از جمله پیامک، ایمیل، پیامک در اپلیکیشن های ارتباطی همچون واتس اپ، یا از طریق شبکه های اجتماعی به خبرنگار مورد نظر ارسال می شوند. هنگامی که خبرنگار به روی لینک کلیک می کند، جاسوس افزار در همان زمان به روی گوشی تلفن همراه او نصب می شود.

تحقیقات سیتیزن لب و عفو بین الملل نشان می دهد که این پیام ها به اشکال زیر هستند:

- پیام هایی که به نظر میرسند از یک ارگان شناخته شده همچون سفارت و یا یک خبرگزاری محلی ارسال شده اند.
- پیام های هشدار دهنده، که هشدار می دهند شخص مورد نظر ممکن است در معرض تهدید امنیتی باشد.
- پیام هایی که موضوعات مربوط به کار روزمره همچون پوشش خبری یک مراسم را شامل می شوند.
- پیام هایی که موضوعات شخصی از قبیل عکس هایی از اعضای خانواده و شریک زندگی خبرنگار را شامل می شوند.
- پیام های مالی همچون پیامک خرید، کارت اعتباری بانکی یا دیگر اطلاعات بانکی شخص مورد نظر.

این پیام های مشکوک همچنین ممکن است از شماره های ناشناس ارسال شوند.

فیشرها (سارقان اطلاعات) می توانند تلفن های شخصی و کاری را هدف قرار دهند. به منظور حمایت بهتر از خود و منابع انسانی و خبری خود خبرنگاران باید:

- لینک دریافت کرده را از طریق راه های ارتباطی دیگر با منابع خود بررسی کنند. این عمل بهتر است از طریق ویدئو و نوار صدا انجام شود.
- اگر منبع ارسال کننده لینک ناشناس است، راه های ارتباطی دیگر نیز ممکن است کارساز نباشد. زیرا این راه های ارتباطی نیز ممکن است توسط دشمن مخدوش شده باشند.
- اگر لینک دریافت شده توسط سرویس های کوتاه کننده لینک همچون TinyURL و Bitly کوتاه شده است، آن را با استفاده از سرویس های برگرداننده لینک URLEX و Link Expander به صورت اصلی بازگردانید. اگر لینک پس از برگردانده شدن به صورت اولیه (اصلی) مشکوک به نظر می رسد، مثلاً صورت مخدوش آدرس وب سایت یک خبرگزاری است، اما صحیح نیست، به روی آن کلیک نکنید و آن را به آدرس phishtank@cpj.org ارسال کنید.
- اگر احساس میکنید لازم است به روی لینک کلیک کنید از وسیله الکترونیکی اصلی همچون رایانه شخصی خود استفاده نکنید. لینک موردنظر را در یک وسیله الکترونیکی دیگر باز کنید که اطلاعات حساس و یا اطلاعات تماس منابع شما در آن ذخیره نشده باشد. (به خاطر داشته باشید که این عمل به تنهایی نمی تواند جاسوس افزار را غیرفعال کند.) باطری وسیله الکترونیکی را که لینک در آن باز شده است، خارج کنید و آن را خاموش نگه دارید.
- از یک مرورگر دیگر به روی تلفن خود استفاده کنید. تحقیقات نشان می دهد که پگاسوس معمولاً مرورگر پیشفرض وسیله الکترونیکی را هدف قرار می دهد. مرورگر پیشفرض در سرویس عامل آندروید، کروم و در آی او اس، سافاری است. از یک مرورگر جایگزین همچون فایرفاکس استفاده کرده و لینک خود را در آن باز کنید. به خاطر داشته باشید که هیچ ضمانتی وجود ندارد که جاسوس افزار پگاسوس مرورگر جایگزین را هدف قرار ندهد.

❖ **نصب دستی جاسوس افزار پگاسوس توسط دشمن**

این جاسوس افزار قابلیت نصب دستی را به روی گوشی تلفن همراه دارد. این وضعیت هنگامی اتفاق می افتد که فیشر (دشمن) به گوشی شما دسترسی داشته باشد. به منظور مقابله با این تهدید موارد زیر را رعایت کنید:

- گوشی تلفن همراه خود را هرگز رها نکنید و از در اختیاردادن به افراد دیگر جداً خودداری کنید.
- مطمئن باشید که در تمامی زمان ها در هنگام عبور از مرز و یا بازرسی امنیتی می توانید گوشی خود را زیر نظر داشته باشید. پیش از تحویل دادن گوشی به ماموران امنیتی، حتماً آن را خاموش کنید. همچنین سعی کنید یک کد امنیتی پیچیده که شامل حروف و اعداد است را برای گوشی خود انتخاب کنید. به خاطر داشته باشید که اگر گوشی شما از شما دور شده باشد، احتمال می رود که به جاسوس افزار آلوده شده باشد.

اگر باور دارید که گوشی تلفن همراه شما به جاسوس افزار پگاسوس آلوده شده است، به سرعت از استفاده از آن خودداری کنید و گوشی دیگری تهیه کنید. در چنین شرایطی گوشی را در محلی دورتر از خود، اطلاعات و یا محیط پیرامون خود نگه دارید. اگر به متخصص فنی دسترسی دارید سریعاً از وی درخواست کمک کنید. اگر ارگان خبری شما متخصص فنی ندارد و یا شما یک خبرنگار آزاد هستید، به سرعت با خط کمک رسان Access Now Helpline تماس بگیرید.

کمیته حمایت از روزنامه نگاران با سایر همکاران خود مشغول کار به روی جاسوس افزار پگاسوس است تا بتواند میزان دقیق آثرات مخرب این بدافزار و میزان تهدید آن را برای خبرنگاران بررسی کند.

اگر اخیراً پیام مشکوکی دریافت کرده اید که ممکن است شما را هدف حمله جاسوس افزار پگاسوس قرارداده باشد، لطفاً آن پیام را به phishtank@cpj.org ارسال کنید.

مطمئن باشید که اطلاعات شما به صورت محرمانه نگهداری خواهد شد.

به منظور دریافت اطلاعات بیشتر درباره امنیت فن آوری، قسمت راهنمای امنیتی کمیته حمایت از خبرنگاران Technology Security را مطالعه کنید. برای مشاهده اطلاعات امنیت دیجیتال به قسمت Resource Centre مراجعه کنید.

با تشکر از Citizen Lab برای به اشتراک گذاردن این اطلاعات ارزشمند