افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــاد بدین بوم و بر زنده یک تن مــباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com afgazad@gmail.com

Scientific	علمی

نویسنده: یوناز رِست در روزنامهٔ برلینر سایتونگ، ۲۲ فبروری ۲۰۱۴
برگردان از: حمید بهشتی

۰۴ مارچ ۲۰۱۴

برده داری و جاسوسی در اینترنت

کامپیوترِ من ، دشمنِ من!

هرگز تجسس در قلمرو شخصی افراد به این سادگی نبوده است. حول محور اینترنت بازاری میلیاردی در خدمت چشم چران ها، جنایتکاران و سازمان های جاسوسی به وجود آمده است.

مردی به اطاق او می نگرد و او را نظارت می کند، حتّا زمانی که او اطمینان دارد که تنهاست. کاسیدی وُلف، یک خانم ۱۹ ساله از اهالی کالیفرنیا با موهای طلائی و چشمان درشت آبی رنگ بر این کار از خودِ تجاوزگر آگاه می گردد. وی از او ایمیلی دریافت می دارد به ضمیمه عکس های لخت خود. آن مرد در عرض ماه ها، عکس های مزبور را با دوربین لب تاپ کاسیدی ولف برداشته است، در خفا و بدون آن که او ملتفت شود.

او این پیام را نیز از فرستنده دریافت می دارد: «حال این قضیه اتفاق می افتد، یا تو یکی از مواردی را که در زیر آمده انجام می دهی یا این که من این تصاویر و بسیاری تصاویر دیگر را در سایت ها و کانال هائی که تو حضور داری در معرض دید عموم قرار می دهم. و آنگاه همه قادر خواهند بود آنها را مشاهده نمایند و تو به جای این آرزویت که مدل عکاسی شوی تبدیل به ستارهٔ شهوت انگیزی خواهی شد».

کاسدی ولف برای جلوگیری از این که آن عکس ها منتشر شوند باید به آن مردِ زورگو تصاویر لخت دیگری از خود را ارسال نماید و برایش یک ویدیوی لختی با کیفیت مرغوب از خود گرفته و در ارتباط ویدیوئی اسکایپ هر کاری را که او طالب است انجام دهد. آن مرد در ایمیلی می نویسد: «من دارم بر این ایمیل نظارت می کنم و می دانم که تو چه زمان آن را باز کرده ای».

کاسیدی ولف در سایت خودش در تویتر می بیند که تصویر نیمه لختی از او گذاشته شده است. آن را شخص تجاوزگر به نمایش گذارده و کُدهای کاسیدی را نیز نزد یاهو و شرکت خدمات اینترنتی بلوگِر موسوم به تامبلِر تغییر داده است. حال دیگر هویت دیجیتال ولف به شخص تجاوزگر تعلق دارد.

«من دلرحم نیستم»

کاسیدی ولف یکی از افراد بسیاری است که به این مشکل مبتلا می باشند. آن مرد به ۱۵۰ لب تاپ رخنه کرده است. نوباوه ای به نام ایرین به او نوشت: «من اکنون اسکایپ خود را می بندم. لطفاً رعایت کن که من تازه ۱۷ سالم شده است. بیا و دلرحم باش». او پاسخ می دهد: «من دلرحم نیستم» و هنگامی که یکی دیگر از قربانیان از او خواهش می کند مجبورش نکند چهرهٔ خود را نشان دهد، پاسخ می دهد: «تو هر عضوی از پیکرت را که می گویم باید نشان دهی».
تجسس نوباوگان برای فرد تجاوزگر فقط اندکی بیش از ایجاد یک ایمیل جدید کار می برد و برای این کار احتیاجی هم به اطلاعات فنّی ویژه ندارد. کافیست نرم افزاری را داشته باشد بنام RAT که کوتاه شدهٔ Remote Administration Tool است به معنی نرم افزار مواظبت از راه دور. تکنیکرها برای برطرف نمودن اشکالات کامپیتوی، از راه دور و بدون این که در محل حضور یابند از آن استفاده می کنند. نرم افزارهای مطمئن به گونه ای ساخته شده اند که پیش از انجامِ دخالت باید کاربر اجازهٔ ورود را داده باشد. اما کسی که به حریمِ کاسیدی ولف تجاوز نموده است از نرم افزاری استفاده می کند که تقریباً با آن فرقی ندارد، با این تفاوت که کنترول دستگاه را کاملاً در اختیار او قرار می دهد، بدون این که برای اینکار به اجازهٔ طرف نیازی داشته باشد.
برای تهیهٔ نرم افزار مزبور کافیست که او از موتورِ جست و جوی گوگل استفاده نماید. و تقریباً یک دوجین از انواع مختلف آن هست. برخی از آنها رایگان بوده و بقیه تا ۲۵۰ دلار می باشند. سازندگان آنها طبق معمول اشاره می کنند که از آن نرم افزارها فقط در محدودهٔ قانونی بایست استفاده شود. اما اسامی آن نرم افزارها فاش می سازند که برای چه کار می توان از آنها استفاده نمود. اسامی آنها از جمله نام گیاهان سمّی بوده یا در آنها از واژهٔ تاریک یا سیاه استفاده شده است.
راه نصب آنها را در ویدیوهای موجود در یوتیوب می توان مشاهده نمود که به المانی هم هست. بیش از چهار دقیقه طول نمی کشد که آدم تمامی گزینه های لازم را فعال نموده و نرم افزار نفوذی را به راه اندازد. کافیست که یک بار به لب تاپ شخصی رخنه شود، از آن پس لب تاپ مزبور به تجاوزگر متعلق است.
لب تاپ شخص مورد نظر به تجاوزگر می گوید: حاضر به دریافت دستورات شما هستم. آنگاه تجاوزگر نرم افزاری را در مقابل خویش می یابد که با برنامه های ویندوز هیچ تفاوت ظاهری نداشته و به همان سادگی می توان با آن کار کرد. کافیست که در ردیف فرمان های نرم افزار یک کلیک کند تا دوربین (وب کام) لب تاپ آغاز به عکس برداری از شخصی که در طرف مقابل نشسته است، بنماید. شخص متجاوز به حریم کاسیدی ولف فهرستی از دوربین های موجود را در اختیار دارد که بدون آن که قربانیانِ او خبردار شوند می تواند دوربین او را در اختیار خود گیرد. کاسیدی ولف می گوید که هیچ ملتفتِ نورِ دوربین خود نشده بوده.

این هیولا هنوز بچه است

یک کلیک دیگر در نرم افزار تجسسی میکروفن لب تاپ آلوده را فعال می نماید. هرگاه کاسیدی ولف با دوستان خویش گفت و گو می کند، تجاوزگر می تواند سخنان آنها را بشنود، هر آنچه در اطاق گفته شود ضبط شده و انتقال می یابد. به همین سادگی تجاوزگر می تواند هر چه را کاسیدی ولف تایپ می کند ضبط نماید. بدین صورت وی می تواند کلیدهای رمز او در تویتر را دریافت نموده و تصاویری را در سایت های او بگذارد. او همواره می تواند از هرچه که تارنمای کاسیدی نشان دهد عکسبرداری نموده، در پرونده های او جست وجو، نرم افزارها و وبسایت هائی را احضار و مورد استفاده قرار دهد، می تواند حافظهٔ هارد دیسک او را پاک کند و لب تاپ را خاموش نماید. کمپیوترِ وی متعلق به اوست.

برخی از تجاوزکاران، همزمان صدها و گاهی هزاران کامپیوتر آلوده را تحت نظارت دارند. کسی که به حریم یک خانم دانشجو تجاوز نموده بود به او پیام می دهد: «من می دانم که هم اکنون تو با پولیس صحبت می کردی». پولیس مخفی FBI نزد آن شخص ۹۰۰ گفت و گو و ۱۵۰۰۰ ویدیوی ضبط شده از ۲۳۰ لب تاپ آلوده را یافت.

کاسیدی ولف به سراغ پولیس می رود. FBI با اندکی صرف وقت به هویت آن مرد پی می برد زیرا توانائی فنی او کمتر از آن بوده است که بتواند خود را مخفی نماید. نام او جارِد جِیمز آبراهامز می باشد، مردیست ۱۹ ساله با موی بور و سیمائی کودکانه.

کاسیدی ولف هنگامی که جایزۀ مسابقۀ زیبائی نوباوگان امریکا را می برد تصمیم می گیرد در مورد وضع خود به سخن آید. او یکی از معدود کسانی است که تجاوز به حریم خود در اینترنت را علنی نموده اند. اما رسانه های امریکا گزارش کرده اند که پولیس مخفی FBI برای مقابله با تمامی مواردِ تجاوزِ اینترنتی لازم دیده است واحد مبارزه با جنایات در شبکه را توسعه دهد. مواردی که علنی گشته اند به نظر کارشناسان فقط رأس هرم را نشان می دهند.

یکی از مسؤولان اتحادیۀ حفاظت اطلاعات در المان به نام توماس فلوس همواره در مدارس در بارۀ خطرات موجود در اینترنت سخنرانی می کند. به گفتۀ او همیشه پس از سخنان او نوباوگانی به وی مراجعه کرده و از رفتار غیر معمول لب تاپ هایشان گزارش می کنند. اما به ندرت کار به پولیس و شکایت می کشد. زیرا شرم به آنها اجازۀ اینکار را نمی دهند. یکی از موارد استثنائی، دختر ۱۶ ساله ای است که توماس فلوس پس از سخنرانی، نرم افزاری نفوذی را در لب تاپ او کشف می کند. از آنجائی که پدرِ آن دختر یکی از افراد پولیس بود کار به اعلام جرم کشید. سپس هنگامی که مأموران در سال ۲۰۱۰ در ایالت راین لندِ المان مرد ۴۴ ساله ای را دستگیر می کنند، وی در حال مشاهدۀ تصاویری از چند اطاق متعلق به کودکان بوده است. بازجویان به ۳ میلیون تصویر که وی مخفیانه گرفته بوده دست می یابند، تصاویر دختران، پسران و زنانی در حمام، در تختخواب، در آبریزگاه و یا در حال پوشیدن لباس.

شبیه خدمات تیلفونی برای سارقین بانک

به گفتۀ یکی از کارشناسان تکنولوژی اطلاعات در شرکتِ «مک افی» به نام «راج زمانی» تقاضا برای نرم افزار تجسسی آنچنان شدید است که بازار فوق العاده ای را به وجود آورده است. راج که آستین های خود را بالا کشیده است در اطاق یکی از دفاتر در طبقۀ بالای ساختمانی معمولی در نزدیکی لندن مشغول به کار است. او که چهل وچند سال سن دارد ریاست تیمی از محققان جنایات اینترنیت را برای پولیس یوروپل بر عهده دارد. آنها براینترنت برای شناسائی روش ها و خدمات ممنوعه نظارت می کنند. معاملات مربوطه سالانه بالغ بر میلیاردها دالر می باشد.

آنچه تازگی دارد اینست که تا چه اندازه موانع برطرف گشته و کار ساده شده است، «به طوری که هر کس – و واقعاً هم: هر کس – می تواند در اینترنت جنایتکار گردد». آنچه را «زمانی» و تیم او مشاهده می کنند، دیگر هیچ وجهِ مشترکی با تصویری که از جنایتکاران اینترنتی گزارش می شود، ندارد. آنها کارشناسان شبکۀ اینترنت با اطلاعاتی فوق العاده و توانائی های غیر عادی هستند. راج زمانی آن را با یک هرم مقایسه می کند. «در رأس هرم همچنان افراد بسیار آزموده می باشند. اما تغییری که مشاهده می شود این است که قاعدۀ هرم وسعت یافته است». گونۀ تازه ای از جنایتکاران اینترنتی به عرصۀ معامله رونق بخشیده اند: «تیپّی که دارای توانائی فنّی اندک بوده، آنچه را آنها برای حملات بسیار پیچیدۀ خودکار و سیستماتیک، برای اعمال زور، تهدید و اخاذی لازم دارند می توانند در اینترنت ابتیاع نمایند».

و تازه نرم افزار نفوذی به حریم بانوان فقط یکی از امکانات مزبور است. اطلاعات کارت های بانکی، ایمیل های اغوا کننده به همۀ زبان ها، سرقت اطلاعات در شبکه های صنعتی. تیم های تولید حرفه ئی مجموعه ای از نرم افزارهای

نفوذی را که روزانه و هفتگی قابل اجاره می باشند، عرضه می کنند. همانند نمونهٔ بازار آمازون، توصیهٔ کالا نیز صورت می گیرد: هر که مایل به خرید شبکه ای از کامپیوتر باشد، به موازات آن به او نرم افزار نفوذی نیز عرضه می گردد. از جملهٔ خدمات این که توضیحِ واژه های اولیه ضمیمه می شود. حتّا کسانی که تا چندی پیش نمی دانستند ترویان (مهاجم مخفی) چیست نیز ترغیب می شوند. حمایت لازم از راه ارتباط کامپیوتری نیز عرضه می گردد. به گفتهٔ راج زمانی «مانند این است که مثلاً سارق بانک در دنیای واقعی هنگامی که می خواهد بداند چگونه گاو صندوق را باز کند به خدمات تیلفونی زنگ بزند».

عرصه های محفوظی برای معاملات موجود اند که فقط کسانی به آنها راه می یابند که بزه کاران دیگر ضامن آنها شده باشند. اما محصولاتی را که برای همگان می باشند میتوان توسط گوگل یافت. راج زمانی لب تاپ خود را که روی میزش قرار دارد باز کرده و به دنبال خدماتی می گردد که توسط آن می توان سایت رقیب را معلق ساخت. از جملهٔ اولین یافته ها یک ویدیو در یوتیوب می باشد. مرد جوانی جلوی دیواری سفید ایستاده: «اگر مایل هستید که رقیب خود را در اینترنت خاموش و به اصطلاح آف لاین کنید خواستهٔ شما تحقق می یابد». او قول می دهد که با ۴ سال تجربه ای که در توبره دارد، مراجعه به او کار اشتباهی نیست. «با پرداخت دستکم ساعتی ۵ دالر می توان وبسایت ها را از شبکه بیرون کرد و اگر خواست شما باشد برای روزهای متمادی».

به همان گونه که تکنیکرهای شرکت تله کوم در صورت لزوم در ازای پرداخت وجهی، ارتباط میان دستگاهِ روترِ شما با اینترنت را (برای انتقال اطلاعات به کامپیوتر) تنظیم می کنند، بزه کاران اینترنتی نیز در قبال دریافت وجهی، گونه ای از خدمات را برای نصب نرم افزار تجسسی عرضه می نمایند. پشتیبانی ۲۴ ساعته برای نرم افزاری که تجاوزگر به حریم کاسیدی ولف نمود در ازای پرداخت ۳,۹۹ دالر، آنهم برای استفادهٔ تمام عمر. پرداخت وجه همانگونه که برای بازار آمازون یا زلاندو صورت می گیرد، توسط خدمات پی پال است.

رخنه به دایرهٔ دوستان با کپی کردن و افزودن

آبراهامز در ماه مه ۲۰۱۲ پیش از آن که به کاسیدی ولف ایمیل بفرستد، در عرصهٔ بازار اینترنت آلوده نمودن لب تاپ او را گزارش می کند. حال وی قصد دارد از ورودیهٔ لب تاپِ او استفاده کرده و به دوست دخترهای او نیز دسترسی یابد. اما نمی داند اینکار را چگونه صورت دهد. آبراهامز در پیامی می نویسد: «من قصد دارم توسط فیس بوک پیامی به دوست دخترهای او ارسال کنم. اما نمی دانم چه بنویسم تا آنها نرم افزار مزبور را در کامپیوتر خود پیاده کنند. پس از دو ساعت پاسخ او می رسد: جمله ای را بنویس مانند این که: «آهای، من عکس مشترکمان را دو ساعت پیش دریافت نمودم. به نظرم چنین است که عکس مال دیروز باشد».

در درون تصویر مزبور – بدون این که دوستان کاسیدی ولف بدانند - نرم افزار تجسسی مخفی می باشد. اگر یکی از آنها بر روی لینک مزبور کلیک کند، دستگاه او نیز آلوده می گردد. مزوّرانه این است: هنگامی که تجاوزگر به کامپیوتر یکی از آنها راه یافته باشد، آنگاه کار ساده ایست که از اعتماد سایرین استفاده کرده و به آنها نیز رخنه نماید. چند تن از قربانیان چشم چران های اینترنتی روند کار را نزد خود مرور کرده و به این نتیجه می رسند که باید نرم افزار تجسسی را از یکی از اقوام یا دوستان خویش دریافت کرده باشد.

برای دسترسی به نوباوگانِ دیگر، مجموعه هائی از نرم افزار در بازار هست. در این نرم افزارها همهٔ آنچه که آدم برای ایجاد یک هویت جعلی در فیس بوک و یا عرصه های گفت و گوی زنان لازم دارد، موجود است، به اضافه پیامی که دختران را ترغیب به برقراری ارتباط نماید: «آهای، لطفاً از این که من تو را به لیست دوستان خود افزوده ام وحشت نکن». این پیام نیز به همراه نرم افزار توسط عرضه کننده ارسال می گردد که فقط کافیست با کپی و افزودن به

شخص مورد نظر ارسال گردد. «اما مثل این که توخیلی توپّی (کول هستی)، این است که من تو را به لیست دوستان خود افزودم». سایر کاربران نیز پیام مزبور را ضبط می کنند تا بتوانند در پیام های خود از آن استفاده نمایند. به گفتهٔ یکی از چشم چران های راهِ دور «در غیر اینصورت خیلی زحمت دارد آدم هربار بخواهد این جملات را خودش تایپ کند».

کسانی که نمی خواهند به خودشان زحمت داده و خود به کمپیوتر خانم ها نفوذ کنند، می توانند رمزِ ورود به کمپیوتر های آلوده را ابتیاع نمایند. «سلِیوز»، یعنی بردگان. این صفتی است که به دستگاه های تحت تسلط داده می شود. در زبان کمپیوتر دستگاهی را که تحت تسلط کمپیوترِ دیگر درآمده باشد اینچنین توصیف می کنند. اما در عرصهٔ گفتار واقعاً شبیه برده داری است. «گِرلز سلِیوز» یعنی دختران برده به معامله گذاشته می شوند. هر چهار رمزِ ورود به کمپیوتر دختران بی خبر به بهای ۵ دالر. یکی دیگر هر ده نشانی را یکجا می فروشد به یک دالر یا ۱۰۰ نشانی را به ۸ دالر. برخی تصویر آن دختران را هم برای ترغیب خریدار نشان می دهند و آنها را به حراج می گذارند. برخی دیگر «بردگان» خود را با یک دیگر تعویض می کنند یا که به صورت ضمیمه، مجانی با خدمات دیگر عرضه می نمایند.

استتار دولت ها و نرم افزار تجسسی ارزان

اما همهٔ آنها به دختران و زنان راغب نیستند. زیرا کاربرانِ مرد نیز ممکن است هدف تحمیل و سوء استفاده قرار گیرند. یک جوان ۱۷ ساله در امریکا به وسیلهٔ ویدیوئی که توسط دوربین کمپیوتر او گرفته شد، تحت فشار قرار گرفت. او چنان مستأصل شده بود که یادگارهای گرانبهای خانوادگی را که ۱۰۰ هزار دالر ارزش داشت، سرقت نمود تا از انتشار آن ویدیو جلوگیری نماید. در انگلستان جوان ۱۷ سالهٔ دیگری پس از آن که تهدید به این شد که ویدیوئی را که از او گرفته بودند منتشر سازند، دست به خودکشی زد.

برخی این کار را برای وقت گذرانی انجام می دهند. در یوتیوب ویدیوهای بیشماری هست که توسط تجاورگران به نمایش گذاشته شده است. به این کار «گیج کردن بردگان» گویند. در این ویدیوها تجاوزکاران قربانیان خود را با تصاویر بسیار خشونت باری که در کمپیوترهای آنان به نمایش می گذارند به وحشت می افکنند. در یکی از این ویدیوهای یوتیوب، تارنمایِ تجاوزکاری به نمایش گذاشته می شود با کمنتارهای لفظی وی. تجاورکار به لب تاپ یک پسربچه تصویر یک آدمِ جن زده را نشان می دهد که پوست بدن و دندانهایش از بدن او جدا می شوند. از طریق دوربین فیلم برداری لب تاپِ آن پسربچه دیده می شود که چگونه او هنگامی که پیکر طرف ورم کرده و می ترکد، از فرط وحشت با دستان خویش بر چهره اش می کوبد. آنگاه وی گریه کنان از مقابل لب تاپ فرار می کند و در پشتِ سرِ او به گوش می رسد چگونه فرد تجاوزکار قاه قاه می خندد.

سازمان های جاسوسی نیز به امکانات تجسس توسط نرم افزار ارزان قیمت پی برده اند. دقیقاً توسط همان نرم افزار تجسسی که آبراهامز برای اعمال فشار بر کاسیدی ولف مورد استفاده قرار داد. کنشگران حقوق بشر و مخالفان رژیم سوریه نیز به همین گونه تحت فشار قرار گرفتند که به احتمال قوی توسط دولت سوریه صورت گرفته است. تجاوزگران برای تجسس میان مخالفان درست نظیر همان تاکتیک هائی را به کار گرفتند که چشم چران ها توسط دوربینِ کمپیوتر. گفته می شود برخی از آنها را پس از دستگیری مجبور کرده اند اسم رمز کمپیوتر خود را به آنها بگویند. سپس تجاوزگران توانسته اند از طریق استفاده از پروفایل آنها (هویت آنها در اینترنت) نرم افزار تجسسی را در شبکهٔ آنها نصب نمایند.

آنها در فیس بوک متعلق به یکی از گروه های مخالف، لینکِ مطلبی را قرار دادند که مدعی نشان دادن چگونگی کشته شدن یکی از مخالفان رژیم بود. اما در حقیقت در پس آن لینک، یک نرم افزار تجسسی نهفته بود. به یکی از گروه های

کنشگر حقوق بشر ایمیلی رسید با لینکی به یک ویدیو. هنگامی که یکی از اعضای گروه بر روی ویدیوی مزبور کلیک کرد، چگونگی کشه شدن یک غیرنظامی توسط سربازان رژیم را مشاهده نمود. اما همزمان با آن در خفا نرم افزار مراقبت کننده بر کامپیوتر وی نصب گشت.

این موارد را آقای مورگان مارکی بوار تجزیه و تحلیل نمود. او که یکی از اهای زلاند نو می باشد از جملهٔ تعقیب کنندگان نرم افزار تجسسی است. او بر روی حملاتی که به کنشگران حقوق بشر انجام می شود برای یکی از مؤسسات تحقیقاتی دانشگاه تورنتو کار می کند. مارکی بوار می گوید برای مأموران امنیتی استفاده از نرم افزارهای شایعِ مراقبتی جذابیت دارد. زیرا که این را لو نمی دهد که چه کسی در پشت حملات تجسسی قرار دارد. اما در بازار نرم افزار گونه های بسیار خطرناک تری هم یافت می شوند. ادارات دولتی نیازی به استفاده از نرم افزارهای ارزان قیمت ندارند. آنها قادرند از عرضه کنندگانی که مانند بوتیک های گران قیمت می باشند، آنچه را لازم دارند تهیه نمایند. امکان مراقبتِ باب میل آنها با فرم و ظاهری مطلوب به آنها عرضه می گردد. در اینگونه مغازه های مرغوب به گفتهٔ اهل فن سالانه معادل ۵ میلیارد دالر معامله می شود.

گروه المانی-انگلیسی گاما، یک پای ماجرا

علائه شهابی در انگلستان به مدرسه رفته و در لندن زندگی می کند. او مادر یک کودک سه ساله می باشد و روزنامه نگار و استاد علم اقتصاد بوده، دکترای خود را در کالج امپریال لندن به پایان رسانده است. در فیس بوک تصویری هست که او و شوهرش را نشان می دهد که در ضیافتی که برای مدیران جوان بر پا شده بود با پرنس چارلز گفت و گو می کنند. چارلز فنجانی چای در دست داشته و او با روسری بر سر و آرایشی ملایم می باشد.

این کنشگر جوانِ حقوق بشر تحت مراقبت رژیم بحرین قرار گرفت زیرا در تحقیقاتی خشونت و شکنجه توسط پولیس را مستند ساخته بود. هنگامی که او و چند روزنامه نگار در اپریل ۲۰۱۲ در یکی از روستاهای بحرین در حال تحقیقات بودند، بارها علائمی را مشاهده کردند حاکی از این که او تحت نظر می باشد. ناگهان یک هلیکوپتر پولیس بر بالای سر آنها به پرواز در آمد. هنگامی که ماشین روزنامه نگاران برای رفتن به حرک در آمد، خودرو آنها را نفرات پولیس در اونیفرم نظامی و اسلحه به دست تعقیب و در حالی که نقاب بر چهره داشتند ماشین آنها را متوقف نموده او را ساعت های متمادی نگاه داشته و مورد بازجوئی قرار دادند.

پس از چند هفته شکارچی نرم افزار تجسسی، مورگان مارکی بوار، چند تا از ایمیل هائی را که برای علائه شهابی رسیده بود بررسی می نماید. لحن گفتار یکی از ایمیل ها که ادعا شده بود از جانب یکی از کارکنان خبرگزاری الجزیره می باشد به نظر او مشکوک می رسد. مورگان مارکی بوار ابتداء تصور می کرد با عملکرد یکی از نرم افزارهای ارزان قیمتی روبه روست که برای کنشگران سوری هم به کار برده بودند. اما او سپس با حواس جمع تر به موضوع توجه نمود.

نرم افزار تجسسی مزبور، خود پی می برد که مورد بررسی قرار گرفته است و به گفتهٔ مورگان مارکی بوار خود را مخفی می نمود. این نرم افزار برای مخفی نمودن خود از روش های متعدد استفاده می نماید. با اینحال شکارچی نرم افزارهای تجسسی موفق می شود نرام افزار مزبور را مورد بررسی قرار دهد. هنگامی که او در کدهای نرم افزار با واژهٔ فین سپای "Finspy„ مواجه می گردد، پی می برد که گوهر نادری را کشف نموده است.

آن نرم افزار از محصولات شرکت المانی- انگلیسی گروه گاما می باشد. در آگهی تبلیغاتی شرکت مزبور بر مراقبت لحظه به لحظه توسط دوربین وب کام و میکروفن تأکید می گردد. پس از سقوط مبارک در مصر، فین سپای مورد توجه افکار عمومی قرار گرفت. هنگامی که تظاهر کنندگان به سازمان مخابرات مصر حمله نمودند در میان تمام شلوغی ها

مدارک این نرم افزار شنودی را یافتند. برگِ خریدِ فین سپای نشان دهندهٔ بهائی بالغ بر ۳۸۸۶۰۸ یورو بود. اما شرکت مزبور فروش آن را حاشا می کند. تا آن زمان هیچکس نتوانسته بود نرم افزار مزبور را بررسی نماید- تا این که مارکی بوار با آن مواجه گشت.

همانگونه که یک زیست شناس، حشرهٔ جدیدی را بررسی می نماید، مارکی بوار نیز نرم افزار تجسسی مزبور را کالبد شکافی نمود. بدینصورت او اطلاعاتی را به دست آورد که توسط آنها می تواند کامپیوترهائی را رد گیری نماید که نرم افزار خسارت بارِ مزبور اطلاعات قربانیان خود را به آنها می فرستد. فهرست کشورهائی که نرم افزار تجسسی مزبور در آنها به شنود و تجسس می پردازد دراز است: قطر، پاکستان و ترکمنستان از جملهٔ ۲۰ کشوری هستند که مارکی بوار در لیستی نام آنها را یافت و این حاکی از زیرساختِ جهانی یک شرکت خصوصی دارای شبکهٔ مراقبت است که او به افشای آن موفق گشت. علائه شهابی می گوید: نرم افزارهای تجارتی در نقشِ اِن اِس اِی کشورهای در حال توسعه می باشند.

هر که در میدان دید نرم افزارهای آنان قرار گیرد، هیچ شانسی برای محافظت از خود ندارد. برنامه های ضد ویروس نیز غالباً توان تشخیص این نرم افزارهای خسارت بار را ندارند. حتّا شرکت تکنولوژی اطلاعاتی زیمانتک نیز توصیه می کند که عدسی دوربین وب کام خود را مسدود نمائید.

آلوده شدن با کلیک برای مراجعه به سایت ها

مشکل تولید کنندگان نرم افزارهای محافظتی در این است که تجاوزکاران به همان وسایلی مجهز می باشند که مدافعان در اختیار دارند. خدماتی در اختیار تجاوزکاران می باشد که در ازای پرداخت چند سنت آنها می توانند برنامه های ضد ویروسِ به روز شده را آزمایش نمایند. بدینصورت آنها قادرند نرم افزارهای خسارت بار را آنچنان تغییر دهند که دیگر قابل کشف نباشند و نتیجهٔ آن سیلِ رشد یابنده ای از نرم افزارهای خسارت بار می باشد. شرکت «مَک اَفی» روزانه ۶۰۰۰۰ نوع جدید عامل نفوذی را تشخیص داده و در جمع، تعداد آنها به بیش از ۱۷۰ میلیون فایل (پروندهٔ اطلاعاتی) بالغ است.

برای به دام افتادن قربانیان، کافیست آنها به یک سایت معمولی مراجعه نمایند. چشم چرانِ از راه دوری که در تماس با آبراهامز بود، برای وی کُدِ سایتِ یکی از ادارات را ارسال نمود که مخاطبِ آن کودکان تجاوز شده بودند. او به سایرِ چشم چرانهایِ راهِ دور پیامی می دهد: «من اکنون به جمعی دیگر از دختران برده دسترسی یافته ام» و البته همهٔ آنها دخترانی هستند که یک مشکل دارند (همهٔ آنها مورد تجاوز قرار گرفته و مبتلا به بیماری لاغری می باشند). حتّا وبسایت های خبری دارای شهرت جهانی نظیر یاهو یا اِن بی سی زمانی در خدمتِ شیوعِ نرم افزارهای خسارت بار بوده اند. سایت خبری لس انجلس تایمز نیز هفته های مدید در خدمت آنها قرار داشت. به هنگام ورود، نرم افزار خسارت آور به دنبال این می گردد که از کدام ضعفِ امنیتی در کمپیوتر مقابل می تواند بهره برداری و آن را آلوده سازد. نرم افزارهای تجارتیِ تجسسی مانند «فین سپای» نیز به همین گونه قادرند خود را نصب نمایند. کنشگر حقوق بشر، علائه شهابی، براین باور است که رژیم بحرین نیز دیگر ایمیل های مشکوک ضمیمه بر نرم افزارهای تجسسی را ارسال نمی نماید. بلکه طرف مقابل را به هنگام ورود به وبسایت ها آلوده می کند. سازمان اِن اِس اِی نیر از روش های مشابه استفاده می نماید.

چشم چران های از راه دور و نیز جنایتکاران و سازمان های جاسوسی برای این که افراد هدف خود را مورد تجسس قرار دهند گهگاه از روش های مشترکی استفاده می کنند. سوء استفادهٔ شخصی نیز همانگونه در ادارات دولتی صورت می گیرد که جارِد آبراهامز که به حریم کاسیدی ولف تجاوز نمود، انجام داد. این است که مأموران سازمان های

جاسوسی برای تجسس در حریم دوست دختر سابق یا همسر خود از تکنیک های معمولِ مراقبت دولتی استفاده می نمایند. و این دیگر به اندازه ای شیوع یافته است که نزد «اِن اِس اِی» واژۀ ویژه ای برای آن به کار می برند LOVEINT روشنگری عشقی.

کلید واژه ها: اینترنت، دیجیتال، برده داری، قلمرو شخصی، سازمان امنیت، جاسوسی، نرم افزار

منبع:

http://www.berliner-zeitung.de/digital/cyberkriminalitaet-mein-computer--mein-feind,10808718,26304608.html