افغانستان آزاد ــ آزاد افغانستان

AA-AA

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

www.afgazad.com afgazad@gmail.com

Political	سیاسی

فرستنده: فرید پرواز

۲۵ فبروری ۲۰۱۵

کشف پیچیده ترین شبکهٔ هکری جهان
افشای رازهای دو دهه جاسوسی سایبری

گروه هکری «معادله» دارای زیرساخت های ارتباطی و ابزارهای جاسوسی گسترده است زمانی که در سال ۲۰۱۰ بدافزار «استاکس نت»کشف شد متخصصان امنیتی آن را یکی از پیچیده ترین ابزارهای نفوذ کامپیوتری معرفی کردند که تا آن زمان ساخته شده بود . بعداً بدافزارهای Flame و رجین هم به دلیل شباهت هایشان به یک مبداء ساخت مشترک منتسب شدند؛ جائی که صدها نفر ساعت ها روی چنین ابزارهای هوشمند و فوق العاده مخربی کار کرده اند .

حالامتخصصان امنیتی در شرکت کسپرسکی بزرگ ترین شبکهٔ هکر تاریخ اینترنت را کشف کرده اند که استاکس نت، رجین و Flame هم به آنها مرتبط است .به نوشتهٔ کسپرسکی این شبکه دسترسی نامحدودی به منابع مالی و نیروهای انسانی متخصص داشته و دارای انبار بزرگی از ابزارهای مخرب اینترنتی مانند استاکس نت بوده است . کسپرسکی که معتقد است متخصصان آن پس از دو دهه تحقیق توانسته اند این شبکه را کشف کنند نام این شبکه را « معادله» گذاشته است به دلیل آن که اعضای این شبکه علاقهٔ زیادی به رمزگذاری اطلاعات خود دارند . ابزارها و روش های پیچیده و مختلفی که این شبکهٔ هکری برای دسترسی به اطلاعات در اختیار داشته آنقدر پیشرفته است که هنوز گمان می رود فقط بخش کوچکی از دامنهٔ کاری آن مشخص شده باشد . صدها دامنهٔ اینترنتی و سرورهای کمپیوتری در سراسر جهان در اختیار این گروه قرار داشته و اطلاعات از طریق کمپیوترهای قربانیان به این سرورها منتقل می شده است .روش های پیچیدهٔ نفوذ از سایت های اینترنتی گرفته تا فلش های حافظه و هارددیسک ها نام بسیاری از برندهای مختلف (هیتاچی، سامسونگ، وسترن دیجیتال و سی گیت) و سیستم های عامل (ویندوز، مک) و حتی گوشی های موبایلی چون آی فون را به میان کشیده و جهان تکنولوژی را در بهت فرو برده است.

جاسوسی سایبری هدف اول

شرکت امنیتی روسی کسپرسکی معتقد است که زمان شروع فعالیت های این گروه مشخص نیست، اما قدیمی ترین بدافزارهای مشاهده شده به سال ۲۰۰۲ بازمی گردد هر چند اولین دامنه های اینترنتی متعلق به آنها در سال ۲۰۰۱

ثبت شده اند و نشان می دهد این گروه حداقل برای دو دهه فعال بوده است . در همین حال احتمالاً این گروه بزرگ مشخص کنندهٔ این است که از گروه های دیگری تشکیل شده یا با آنها همکاری داشته از جمله گروه هائی که مثلاروی استاکس نت یا Flame کارمی کردند . این گروه اما بر اساس شواهد بسیار زودتر از سایران به این بدافزارها دسترسی داشته است . **گروه معادله** در صنایع و بخش های مختلفی به صورت متمرکز کار می کرده از جمله دولت ها و انستیتوهای دیپلماتیک، مخابرات، فضائی، انرژی، تحقیقات هسته ئی، نظامی، رسانه ها، حمل ونقل، انستیتوهای مالی و شرکت های توسعه دهندهٔ تکنولوژی های رمزنگاری .

کسپرسکی می گوید این گروه تعداد جالب توجهی از ابزارها و بدافزارها را در اختیار داشته که مدام هم به روز می شده اند .این بدافزارها به سادگی گذاشتن یک سی دی درون درایور یا واردکردن حافظهٔ فلش به USB یا دیدن یک صفحهٔ وب روی موبایل، روی کامپیوتر یا شبکهٔ قربانی نصب می شدند و در صورت شناسائی هدف معتبر راه را برای بدافزارهای بزرگ تر بعدی باز می کرده اند و در مرحلهٔ آخر کنترول تمام کامپیوتر و دستگاه را در اختیار می گرفتند .این بدافزارها می توانستند خود را با روش های مختلف درون سیستم مخفی کنند و اطلاعاتی را که به دست می آوردند ابتداء رمزگذاری و سپس در صورت اتصال به اینترنت آن را به سرورها و دامنه های اینترنتی تعیین شده ارسال کنند .این بدافزارها همچنین به سیستم «خود تخریب گر» مجهز بوده و در صورت لزوم و یا پس از دورهٔ مشخص خود را به طور کامل از روی سیستم قربانی حذف می کردند .

متخصصان کسپرسکی با در اختیار گرفتن برخی از دامنه های اینترنتی قدیمی این گروه یا نفوذ به برخی سرورهای آن توانسته اند به روش کار برخی از این ابزارها آگاهی پیدا کنند .کسپرسکی حجم انبوهی از اطلاعاتی از سراسر جهان به سمت معدود سرورهای در اختیارگرفته را تحلیل کرده و معتقد است به احتمال زیاد بخش جالب توجهی از ابعاد کاری شبکه «معادله» هنوز ناشناخته است .

آلودگی هارددیسک ها

بر اساس گزارش کسپرسکی مهم ترین و جدیدترین کشف در زمینهٔ شکل نفوذ تکنولوژی فوق العاده جدید و پیشرفتهٔ مورد استفادهٔ این شبکه در آلوده کردن سیستم نرم افزاری هارددیسک است . کسپرسکی توانسته دو سیستم نرم افزاری آلوده سازی هارددیسک این گروه را تشریح کند که یکی مربوط به سال ۲۰۱۰ و دیگری مربوط به ۲۰۱۳ است . این سیستم نرم افزاری خود را به جای سیستم اصلی جایگزین کرده و داخل هارددیسک پنهان می شود و با فرمت کردن هارددیسک هم از بین نمی رود. سیستم نرم افزاری هارددیسک های ۱۲ شرکت معروف در این عرصه از جمله شرکت های مکستور، وسترن دیجیتال، سامسونگ، سی گیت، توشیبا و میکرون قابل جایگزینی تشخیص داده شدند .

ابزارهای نفوذ حتی قادر به نفوذ از طریق سی دی رام دستگاه نیز بوده اند . به گفتهٔ کسپرسکی در سال ۲۰۰۹ در جریان یک کنفرانس علمی در هوستون به تمامی شرکت کنندگان که شامل دانشمندان و متخصصان می شدند سی دی کنفرانس داده شد که در صورت قرار گرفتن در سی دی رام ابزار نفوذ را به کامپیوتر قربانی منتقل می کرد .

چه کسی پشت معادله است؟

کسپرسکی می گوید: گروه پشت **معادله** افرادی تعلیم دیده اند که بسیار کم اشتباه می کنند، ولی در موارد معدودی آنها ردپایهائی را از خودشان به جای گذاشته اند .این ردپایها اما مربوط به هویت این افراد نمی شود بلکه با نحوهٔ

عملکرد ابزارهایشان مرتبط است .بر این اساس در هر ماه حدود دو هزار قربانی فقط توسط کسپرسکی شناسائی شده اند اما احتمال این که تعداد قربانیان بسیار بیش از این باشد وجود دارد .نکتهٔ مهم دیگر این است که هرچند بخش قابل توجهی از حمله ها و رفتارهای بدافزارهای کشف شدهٔ این گروه نشان دهندهٔ عملکرد گستردهٔ آنها در سیستم عامل های مختلف ویندوز بوده است اما موارد مختلفی از آلودگی به سیستم عامل مک هم مشاهده شده است . همچنین برخی موارد از آلودگی سیستم عامل آیفون اپل (iOS) هم در این زمینه خبر می دهد .

گروه معادله دارای بیش از ۳۰۰ دامنهٔ اینترنتی و بیش از ۱۰۰ سرور در سراسر جهان است .این سرورها در نقاط مختلف جهان قرار دارند؛ از امریکا و انگلستان گرفته تا ایتالیا، المان، هالند، پاناما، کاستاریکا، مالزی، کلمبیا و چک . تمامی دامنه های این گروه توسط دو شرکت مشهور فروش دامنه ثبت شده اند و اطلاعات صاحب دامنه ها به دلیل اعمال محافظت اطلاعات غیر قابل دستیابی است.

ایران هدف اصلی

بر اساس گزارش کسپرسکی بیش از ۳۰ کشور جهان هدف اصلی گروه «معادله» قرار داشته که ایران و روسیه در صدر آنها بوده اند .سوریه، افغانستان، قزاقستان، بلجیم، سومالی، هنگ کنگ، لیبیا، امارات، عراق، نیجریه، مکزیک، امریکا، فلسطین، فرانسه، المان، سنگاپور، قطر ، پاکستان، سویس، انگلستان، هند، برزیل و ...از کشورهای دیگری بودند که این گونه حمله ها در آنها مشاهده شده است .

نکتهٔ مهم این است که به دلیل این که این بدافزارها دارای سیستم خودنابودگر هستند، عملا نمی توان مشخص کرد چه حجم اطلاعاتی و دقیقاً از چه بخش هائی مورد سرقت واقع شده است.

مشاهدات کسپرسکی نشان می دهد که سه کشور مورد این حمله قرار نگرفته اند؛ اردن، ترکیه و مصر .این یعنی **گروه معادله** به طور عمدی اطلاعات مربوط به آی پی های این سه کشور را جمع آوری نکرده است .

از طرف دیگر رمزگذاری پیشرفتهٔ این گروه تعجب متخصصان امنیتی را برانگیخته است .این گروه از تکنولوژی رمزگذاری که به اصطلاح RC5 نامیده می شود، استفاده کرده است .این تکنولوژی توسط فردی به نام رونالد ریوست در فاصله سال های ۱۹۹۴ تا ۱۹۹۸ کشف شد و ویژگی آن مقاوم بودن بسیار آن دربرابر شکستن رمز است . کسپرسکی می گوید که **گروه معادله** را در جریان مطالعه روی ویروس رجین کشف کرده است . کسپرسکی یک کامپیوتر در کشوری در خاورمیانه قرار داده و از این طریق حمله ها به آن را شناسائی می کند . به گفتهٔ این شرکت امنیتی روسی، اطلاعات به دست آمده نشان داد که این گروه کامپیوترهائی را هدف قرار داده که قبلاً مورد حمله بدافزار رجین هم قرار گفته بودند.

چه کسی یا چه کشوری پشت حمله هاست

کسپرسکی به هیچ کشور یا سازمانی پشت سر این گروه هکری اشاره نمی کند .هرچند در کل گزارش این شرکت به یک سازمان بزرگ و افراد متخصص دارای برنامهٔ وسیع با سرمایه گذاری نامحدود اشاره می شو د .

برخی خبرگزاری ها از جمله رویتر و روزنامهٔ نیویورک تایمز از آژانس امنیت ملی امریکا به عنوان سازمان دهندهٔ اصلی نام برده اند .از سوی دیگر اما با توجه به نوع آلودگی و تمایل به دریافت اطلاعات می توان تصور کرد که چه نوع نهادهائی از چه کشورهائی پشت این حمله ها قرار دارند.

***

دنیای اقتصاد:

روزنامۀ دنیای اقتصاد، شماره ۳٤۲۳ به تاریخ ۹۳/۱۱/۳۰، صفحه ۲۵ (بازار دیجیتال)