بررسی جرایم سایبری

ترجمه: زکیه عزتی

میزان استفاده از اینترنت طی سال‌های اخیر به‌طور تصاعدی افزایش پیدا کرده است. برخی تحقیقات نشان می‌دهد که تعداد کاربران اینترنت در مقایسه با کاربران رادیو و کامپیوتر به شدت افزایش یافته است. بر اساس این تحقیق، اگر رقم ۵۰ میلیون نفر تعداد کاربر را در نظر بگیریم، در مورد رادیو در طول ۳۸ سال، کامپیوتر در طول ۱۶ سال و اینترنت تنها در طول ٤ سال تعداد کاربران به این رقم رسیده است. بین سال‌های ۲۰۰۰ تا ۲۰۰۵، کاربری اینترنت (قیاس تعداد افرادی که به طور منظم به اینترنت دستیابی دارند) ۱۸۲ درصد افزایش یافته است. براساس گزارشی در سال ۲۰۰۰، به طور کلی ۱۳۵ کشور به اینترنت دسترسی داشته، ٥٤ شهر در جهان از جمله کاربران اصلی اینترنتند و روزانه ۷۲ میلیون نفر از این تکنولوژی استفاده می‌کنند. هیچ منطقه‌ای به سرعت منطقه خاورمیانه در افزایش استفاده از اینترنت نمی‌رسد (٤٥٤ درصد) و هیچ کشوری درون منطقه خاورمیانه، به اندازه ایران این پیشرفت را نداشته است. (۲/۹۰۰ درصد افزایش بین سال‌های ۲۰۰۰ تا ۲۰۰۵)، در حال حاضر در ایران حدود ۷ میلیون و ۵۰۰ هزار (بالغ بر ۱۰ درصد جمعیت این کشور) کاربر اینترنت وجود دارد. به موازات افزایش تعداد کاربران اینترنت، میزان خرید و فروش کالا و خدمات از طریق اینترنت و یا بهتر بگوئیم تجارت الکترونیکی نیز در حال افزایش است. مجموع ارزش تجارت الکترونیک در جهان طی سال ۲۰۰۵، یک تریلیون دلار تخمین زده شده است و پیش‌بینی می‌شود ارزش تجارت الکترونیکی در ایران از رقم یک میلیارد و ٤۰۰ میلیون دلار در سال ۲۰۰۳ به ۱۲ میلیارد و ۸۰۰ میلیون دلار تا پایان سال ۲۰۰٦ افزایش یافته باشد.

متأسفانه به موازات افزایش کاربری اینترنت و تجارت الکترونیکی شاهد افزایش خاصی در میزان جرائم سایبری نیز بوده‌ایم. تحقیقات نشان می‌دهد که در سال ۲۰۰٤ میزان جرائم سایبری، اشاعه ویروس ۵۰ درصد و کلاهبرداری ۳۰ درصد، افزایش داشته است. شایان ذکر است که هیچ‌گونه آمار دقیقی از میزان جرائم سایبری در ایران وجود ندارد، تنها می‌توان گفت که با توجه به حوادث مستند اخیر، این جرایم به‌طور چشمگیری در حال افزایش است. حال پیش از هر چیز به تعریف دقیق جرایم سایبری می‌پردازیم:

تعریف

جرم سایبری به یک جرم کیفری اطلاق می‌شود که با ظهور تکنولوژی کامپیوتر امکان‌پذیر می‌باشد و به عبارتی دیگر می‌توان گفت: به واقع جرم سایبری یک جرم سنتی است که با کمک استفاده از کامپیوتر، فوق‌العاده دگرگون و تغییر یافته به‌گونه‌ای که مأموران اجرای قانون برای کشف و بررسی این جرم نیاز به درک و شناخت اساسی از کامپیوترها دارند. گروهی از دانشمندان معتقدند سایر دستگاه‌های فناوری اطلاعات از جمله موبایل و برخی دستگاه‌های الکترونیکی نیز در جرایم سایبری دخیل هستند.

تاریخچه

اولین جرم سایبری در سال ۱۸۲۰ و در فرانسه به وقوع پیوست. اگر به این نکته توجه کنیم که «چرتکه» دستگاهی که به نظر حتی سریع‌تر از کامپیوتر نیز کار می‌کند از ۳۵۰۰ سال پیش از میلاد در هند، ژاپن و چین وجود داشته، درمی‌یابیم تاریخ مربوط به اولین جرم سایبری چندان هم دور نیست. در سال ۱۸۲۰ «جوسف ماری جکوارد» یک کارخانه‌دار منسوجات در فرانسه، دستگاه پارچه‌بافی اختراع کرد که امکان تکرار یک سری فعالیت‌ها برای تولید تاروپود پارچه را فراهم می‌کرد. کارگران این کارخانه احساس ناراحتی کرده و امنیت شغلی خود را در خطر دیدند، لذا با انجام خراب‌کاری سعی در عدم استفاده از این تکنولوژی برآمدند و این اولین جرم سایبری ثبت شده به شمار می‌رود.

انواع جرایم سایبری

قبل از هر چیز باید متذکر شویم که هر اقدام غیرقانونی مرتبط با کامپیوتر را نمی‌توان به عنوان جرم سایبری و یا جرم کامپیوتری به شمار آورد. جرم فردی که از رمز یک تلفن دزدیده شده برای مکالمه رایگان استفاده می‌کند، حتی اگرچه این شماره به وسیله یک کامپیوتر پردازش شود، کلاهبرداری است نه یک جرم کامپیوتری. جرم فردی که ۲۰۰ دلار از بانک خودکار (ATM) یک کمپانی پول به جیب می‌زند، اختلاس است نه جرم سایبری. حال برای روشن شدن انواع جرایم سایبری، آن را به ۲ بخش دسته‌بندی می‌کنیم:

۱- جرائمی که در آن خود کامپیوتر مورد هدف قرار می‌گیرد و یا «جرائم کامپیوتری».

۲- جرائمی که در آن از کامپیوتر به عنوان ابزاری برای ارتکاب به یک جرم سنتی استفاده می‌شود. یا «جرائم مرتبط با کامپیوتر».

جرائم کامپیوتری

این نوع جرائم شامل اقداماتی برای صدمه وارد کردن و یا دزدیدن اطلاعات کامپیوتر می‌باشد. «هک کردن» را می‌توان به عنوان مهمترین و معروف‌ترین نمونه برای جرم کامپیوتری مثال زد. در توضیح اقدام «هکرها» چنین می‌توان گفت که افراد مذکور بدون اجازه و با پیدا کردن یک راه پنهانی در کامپیوتر شخصی یک فرد دیگر به جست‌وجو پرداخته و اطلاعات آن را دزدیده و یا تغییر می‌دهند. از جمله دیگر جرائم کامپیوتری می‌توان به موارد زیر اشاره کرد:

◄ایجاد حریق عمدی (مورد هدف قرار دادن یک مرکز کامپیوترای برای صدمه زدن به کامپیوترها از طریق ایجاد حریق عمدی).

◄اخاذی (تهدید به صدمه زدن به کامپیوتر برای گرفتن پول)

◄سرقت (ورود غیرقانونی به مکانی برای دزدیدن قطعات کامپیوتر)

◄توطئه (افرادی که بر روی کامپیوتر مرتکب یک اقدام غیرقانونی شوند)

◄جاسوسی / کارشناسی (دزدی اسرار و تخریب سوابق ذخیره شده رقبای خود در کامپیوتر)

◄جعل (صدور مدارک و یا اطلاعات جعلی از طریق کامپیوتر)

◄سرقت کلان (دزدی قطعات کامپیوتر)

◄تخریب اموال از روی سوءنیت (تخریب سخت‌افزار و نرم‌افزار کامپیوتر)

◄قتل (دستکاری تجهیزات پزشکیکامپیوتری که برای ادامه حیات بیمار به او وصل شده است)

◄دریافت اموال دزدی (پذیرفتن کالا و یا خدمات دزدی [و شناخته شده] از طریق کامپیوتر)

جرائم مرتبط با کامپیوتر

این نوع جرائم شامل تغییر کلی یک جرم سنتی به وسیله استفاده از اینترنت می‌باشد. برای نمونه می‌توان به موارد زیر اشاره کرد:

◄کلاهبرداری اینترنتی (درج آگهی جعلی، کلاهبرداری از طریق کارت‌های اعتباری، پول‌شوئی)

◄هرزه‌نگاری در رابطه با کودکان به صورت آنلاین / اغوای کودکان (استثمار جنسی، بروز احساسات شدید برای اغوای کودکان با هدف تجاوز به آنها)

◄فروش اینترنتی داروهای قابل تجویز با نسخه و مواد مخدر (قاچاق)

◄فروش اینترنتی اسلحه گرم.

◄شرط‌بندی اینترنتی (بخت‌آزمایی، تجارت غیرقانونی از طریق شرط‌بندی)

◄فروش اینترنتی مواد الکی (قاچاق نوشابه الکلی)
◄کلاهبرداری اوراق بهادار به صورت آنلاین (نقض عمل اوراق بهادار یا اوراق مالکیت)
◄دزدی انتشاراتی، دزدی اموال فکری (تکثیر غیرمجاز، تجارت از طریق کپی اطلاعات محرمانه شخصی و غیرشخصی)
◄جعل (استفاده از کامپیوتر برای نمونه‌برداری و ساخت اسناد و ابزار جعلی)
◄تجاوز به ایمیل (پست الکترونیکی) افراد: تعقیب، مخفیانه افراد از طریق اینترنت و ایمیل برای آسیب‌رسانی به وی.
◄فرستادن ایمیل برای کاربر و معرفی خود به عنوان یک نمایندگی سازمان‌یافته و مشروع، با هدف دزدی اطلاعات شخصی وی از جمله کلمه عبور، شماره حساب بانکی و غیره.
◄جرم IRC: وقوع جرم در فضای چت اینترنت.
◄رد و عدم ارائه خدمات: اقدامی در جهت قطع ارتباط بین کاربر و اینترنت
◄اشاعه ویروس: یک نرم‌افزار سوء که خود را به سایر نرم‌افزارها می‌چسباند (ویروس کرمک؛ یک برنامه کامپیوتری است که به وسیله کپی کردن خود در شبکه منتشر می‌شود - اسب تروی و یا وسیله نفوذ، یک برنامه کامپیوتری که به ظاهر کمک‌ساز به چشم می‌آید اما در حقیقت برای از بین‌بردن اطلاعات ساخته شده است - باکتری از جمله نرم‌افزارهای ویران‌کننده به شمار می‌رود.

تحقیقات مقدماتی و کشف جرم

اغلب مسئولان قضائی و اجرائی در خصوص مسئولیت بررسی و کشف چگونگی جرائم سایبری دچار آشفتگی و سردرگمی می‌شوند چرا که اولاً کشف منبع اصلی این نوع جرائم فوق‌العاده مشکل بوده و مستلزم برخورداری از مهارت بالایی در زمینه دانش کامپیوتر می‌باشد. ثانیاً اینترنت از نظر مکانی و زمانی بی‌حد و مرز بوده و به راحتی نمی‌توان گفت که یک جرم سایبری از کجا آغاز و در کجا خاتمه یافته است. البته کشف جرایم مرتبط با کامپیوتر در مقایسه با خود جرایم کامپیوتری (که در بالا به انواع آنها اشاره شد) کمی آسانتر است. شایان ذکر است که ارائه‌کنندگان خدمات اینترنتی (ISP) بیشتر از هر کسانی می‌توانند به کشف این جرم کمک کنند تا آنجائی که باید بگوئیم بسیاری از این افراد در آمریکا به عنوان کارشناسان رسمی و عاملان دولتی با ماموران FBI در کشف این نوع جرائم همکاری نزدیک دارند. همزمان با پیشرفته شدن نرم‌افزار و سخت‌افزار کامپیوتر، بازرسان ویژه تحقیق جرایم سایبری نیز باید دانش خود در زمینه علوم مختلف کامپیوتری را بالا ببرند تا بتوانند از پس پرونده‌های پیچیده سایبری برآیند. نکته دیگر قابل ذکر اینکه، قبل از پیدا کردن عامل جرم سایبری، نحوه گزارش و تشخیص نوع جرائم مهم است. و اما به‌طورکلی چنین می‌توان گفت: که تحقیقات جرائم سایبری شامل گردآوری، تحلیل و بررسی شواهد دیجیتال می‌باشد. شواهد دیجیتال ممکن است در هارد دیسک‌های کامپیوتر، موبایل، سی‌دی، دی‌وی‌دی، فلاپی و... پیدا شود. همچنین شواهد دیجیتال و آثار جرائم اینترنتی می‌تواند در فایل‌های رمزدار، فایل‌های محافظت‌شده دارای کلمه عبور (password)، هارد دیسک‌های فرمت‌شده، ایمیل‌های پاک‌شده، رونوشت‌های چت و غیره نیز نمایان باشد.

حال به بررسی ۲ پرونده که در آنها یکی از انواع جرایم سایبری به وقوع پیوسته می‌پردازیم:

۱- موضوع پرونده: ایجاد شرح حال موهن، هند

◄ دختر جوانی از افراد ناشناسی که ایمیلی به نام وی ایجاد کرده و در آن او را فاحشه تلفنی معرفی کرده بودند، شکایت کرد. در پی ارسال چند پیام از ایمیل مذکور به ۵ سایت مختلف، دختر جوان از سوی مردان زیادی مورد آزار تلفنی قرار گرفته بود.

تحقیقات: دختر جوان با راهنمایی پلیس کلمه عبوری ساخته و به وسیله آن وارد ۵ سایت مذکور شد. بدین ترتیب بازرسان با استفاده از کلمه عبوری مشابه به صفحات اینترنتی سایت‌های مذکور که پیام‌های ایمیل مذکور درج شده بود، دسترسی یافتند. پیام‌ها برای ۵ گروه ارسال شده بود که یکی از آنها یک گروه دولتی بود. تیم بازپرسی دستورات لازم برای ورود به سایت گروه دولتی مذکور و همچنین پیام وارده به سایت آنها را دریافت کرده تا بدین ترتیب IP (یک سری شماره که با نقطه از هم جدا شده و معرف کامپیوتر و معرف کامپیوتر متصل به اینترنت است) استفاده شده برای ارسال پیام را شناسایی کنند. با کمک سایت‌های اینترنتی قابل دسترس دولتی یک ISP (ارائه‌کنندگان خدمات اینترنتی) معرفی شد. بازرسان از ارائه‌کنندگان خدمات اینترنتی درخواست کردند تا جزئیات کامپیوتری با آدرس IP در زمان ارسال پیام‌ها را پیدا کنند.

ارائه‌کنندگان خدمات اینترنتی مذکور نام و آدرس ۲ کافی‌نت را در مومبای به بازرسان پلیس تحویل دادند. تیم بازپرسی فهرست اسامی واردشوندگان به کافی‌نت‌ها را بررسی کرده و متوجه شدند که امضای شاکی نیز در بین آنها دیده می‌شود. لذا بازجوئی گسترده‌ای از شاکی به عمل آوردند. در طول یکی از جلسات بازجوئی، شاکی عنوان کرد وی درخواست ازدواج با یکی از همکلاسی‌های سابق خود را رد کرده است. بدین ترتیب همکلاسی وی به عنوان متهم اصلی مطرح شد. بازپرسان با کمک پلیس مومبای مظنون اصلی را دستگیر و موبایل وی را توقیف کردند. پس از بررسی سیم‌کارت تلفن همراه متهم، مشخص شده که شماره تلفن شاکی که در پیام‌های اینترنتی نیز درج شده بود در حافظه تلفن وی ذخیره شده است. صاحبان کافی‌نت‌ها نیز متهم را شناسایی کرده و اذعان داشتند وی یکی از مشتریان دائم آنهاست.

محکومیت: متهم به ۲ سال حبس و پرداخت مقادیری جریمه محکوم شد.

۲- موضوع پرونده: کلاهبرداری بلیت آنلاین قطار دهلی‌نو، هند

◄ گروهی از افراد ناشناس با استفاده از کارت‌های اعتباری دزدی، از تسهیلات ارائه بلیت قطار به صورت آنلاین استفاده کرده و بیش از ۵۰ بلیت رزرو کرده‌اند. محل تحویل بلیت‌ها را نیز مناطق مختلفی اعلام کرده‌اند.

تحقیقات: از مشخصات کارت‌های اعتباری که از حساب آنها پول برداشت شده بود، لیستی تهیه و سپس یک برنامه «patch» روی سیستم وب‌سایت شرکت فروش بلیت قطار نصب شد تا در صورت استفاده دوباره متهم از مشخصات کارت‌های مذکور، کلمه عبور و یا محل قبلی دریافت بلیت، علائم هشداردهنده روشن شود.

در فاصله‌ای که برنامه patch بر روی سیستم شرکت مذکور نصب شده بود، علائم هشداردهنده به صدار درآمدند که نشان داد متهم از مشخصات یکی از ۱۲ کارت اعتباری ربوده شده برای خرید بیش از ۲ بلیت استفاده کرده و آدرس حیدرآباد را درج کرده است. متهم در حین دریافت بلیت‌های قطار از دست پیک، دستگیر شد.

کارت‌های اعتباری دزدیده شده از چندین بانک که متهم از آنها برای رزرو قلابی بلیت‌های قطار استفاده می‌کرد، تحویل گرفته شد. همچنین در طول بازبینی از منزل وی ۲۵ بلیت هواپیما نیز پیدا شد.

روند به روز شدن قوانین سایبری در کشورها

در مورد قوانین سایبری به تصویب درآمده در جهان، (دسامبر ۲۰۰۰)، از ۵۲ کشور تحقیقی به عمل آمد که نشان می‌داد قوانین سایبری ۳۳ کشور از جمله ایران، ایتالیا، اردن، بلغارستان، باکو و.... به هیچ وجه به روز نشده است. قوانین ۹ کشور از جمله برزیل، شیلی، چین، چک، دانمارک و... نسبتا به روز و قوانین ۱۰ کشور از جمله استرالیا، کانادا، استونی، هند، ژاپن و... کاملاً به روز شده است.

در خصوص کشور خودمان ایران باید بگوئیم که مقامات رسمی کشور تصویب قانون و انجام سایر اقدامات لازمه علیه جرائم سایبری را مقدمه‌ای برای مبارزه با این جرم چه در سطح داخلی و چه بین‌المللی می‌دانند.

معرفی جرائم سایبری به عنوان یکی از موضوعات کلیدی مطرح شونده در «کمیسیون سیاست‌گذاری جنایی و اصلاح قوانین کیفری» دلیل مستندی بر ادعای مذکور می‌باشد. انتخاب این موضوع به عنوان یکی از موضوعات مطرح‌شده در کمیسیون مذکور نشان می‌دهد که دولت نیاز به مبارزه با این نوع جرائم را بسیار ضروری خوانده و آگاه است که با همکاری‌های بین‌المللی و به‌کارگیری بهترین تجربیات بین‌المللی تحقق این هدف را تسهیل خواهد کرد.

اهداف اساسی این پروژه شامل: تقویت دستگاه قضائی و ظرفیت‌های اجرایی قانونی کشور در رابطه با جرایم سایبری، تهیه آماری در مورد وقوع این نوع جرایم در کشور، توسعه یک مکانیسم پاسخگویی ایده‌آل به این نوع جرایم و سرانجام ارتقاء آگاهی عمومی از جرایم سایبری در میان جمعیت کاربر اینترنت می‌باشد.

پی‌نوشت:

www.unodc.org
www.neiassociates.org
www.faculty.ncwc.edu
www.cybercrime.planetindia.net
www.cybecellmumbai.com
www.papers.ssrn.com
www.asialaws.org
www.lexcyber.com
www.mcconnelinteriational.com