بدافزار Shamoon دوباره عربستان سعودی را هدف قرار داده است

پس از گذشت 5 سال که بدافزار Shamoon خرابی عظیمی را برای غول نفت دنیا، عربستان سعودی به بار آورد، این بدافزار دوباره بازگشته است. در سال 2012 بود که این بدافزار دیسک 30 هزار رایانه در عربستان سعودی را از بین برد و تلاش داشت تولید نفت در این کشور را از بین ببرد. اینک این بدافزار دوباره پدیدار شده و ظاهراً چند سازمان در این منطقه را هدف قرار داده است.

شرکت FireEye دو روز پیش گزارش داد در اواسط ماه نوامبر گروه پاسخ به رویداد این شرکت و شرکت جرم‌شناسی Mandiant به وقوع اولین رخداد بدافزار Shamoon نسخه‌ی 2.0 در منطقه‌ی عربستان سعودی پاسخ داده‌اند. از آن موقع تاکنون این شرکت‌ها وقوع چند رخداد دیگر در این منطقه را گزارش داده‌اند.

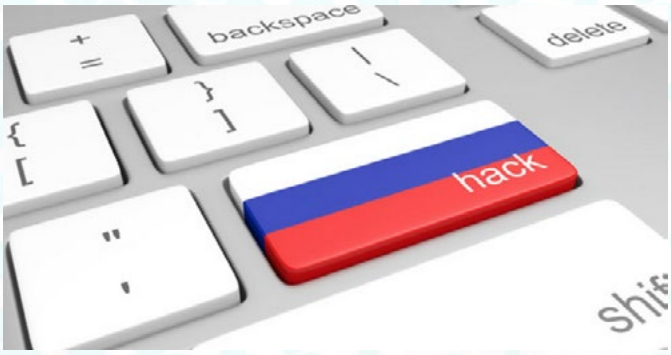
همزمان سیمانتک نیز گزارش داد که بدافزار Shamoon که در سال 2012 در حملات علیه بخش انرژی عربستان سعودی استفاده شده بود، به‌طور شگفت‌آوری بازگشته و در موج جدیدی از حملات، برخی سازمان‌های این منطقه را هدف قرار داده است.

بدافزار Shamoon نسخه‌ی 2.0 یک نسخه‌ی جدید از بدافزار اصلی است و محققان حدس می‌زنند به دلیل شباهت روش این بدافزار با بدافزار قبلی، مهاجمان همان افراد قبلی باشند. در سال 2012 گروهی که خود را «برش شمشیر عدالت» می‌نامید، مسئولیت این حمله را به عهده گرفت ولی اجماع عمومی این بود که این حملات توسط نفوذگرانِ تحت حمایت دولت ایران انجام می‌شود.

مؤلفه‌های بدافزار Shamoon 2.0 همان مؤلفه‌های بدافزار اصلی است. این بدافزار از ابزار تجاری RawDisk برای از بین بردن دیسک‌ها استفاده می‌کند. این ابزار برای دسترسی مستقیم به پرونده‌ها، دیسک‌ها و پارتیشن‌های مختلف استفاده می‌شود. این ابزار بر روی یکی از روش‌های رونویسی، قابل پیکربندی است:

- در روش اول با استفاده از یک کلید تصادفی و RC4 رمزنگاری انجام می‌شود.
- روش دوم رونویسی محتوا، با رشته‌های تصادفی یکسان است که این رشته‌ی تصادفی برای رمزنگاری نیز می‌تواند استفاده شود.
- در روش سوم پرونده‌ها و جداول پارتیشن با تصویر JPEG رونویسی می‌شود.

حملات جاسوسی علیه مؤسسات مالی روسیه توسط سرویس‌های اطلاعاتی خارجی



روسیه روز جمعه اعلام کرد که متوجه شده است برخی سرویس‌های اطلاعاتی خارجی، برنامه‌هایی برای حمله‌ی سایبری به مؤسسات مالی این کشور دارند.

سرویس اطلاعاتی FBS در بیانیه‌ای اعلام کرد که اطلاعاتی بدست آورده که نشان می‌دهد سرویس‌های امنیتی خارجی قصد دارند از تاریخ 15 آذر ماه حملات سایبری علیه روسیه را شروع کنند. در این بیانیه آمده است عمده‌ی این فعالیت‌های مخرب قصد دارند سامانه‌ی مالی روسیه را بی‌ثبات کرده و بانک‌ها را هدف قرار دهند.

این ادعا پس از حمله به 5 بانک مهم روسی در ماه نوامبر مطرح شده است. کسپرسکی نیز گزارش داده است که دستگاه‌های مهاجم در 30 کشور مختلف از جمله آمریکا قرار دارند. بزرگ‌ترین بانک روسیه که تحت حمایت دولت نیز هست با نام Sberbank، اعلام کرده که به سامانه‌های این بانک نفوذ شده ولی خوشبختانه اختلالی در عملکرد اصلی این سامانه بوجود نیامده است.

با این حال خود روسیه نیز در چند ماه اخیر به نفوذهای بزرگی متهم شده است. به‌طور مثال آمریکا در نفوذهای ماه اکتبر مربوط به انتخابات ریاست جمهوری، مسکو را مقصر اصلی می‌داند.

روز سه‌شنبه نیز آنجلا مرکل، صدراعظم آلمان اعلام کرد که نفوذهای روسیه دیگر بسیار عادی شده و به بخشی از زندگی روزمره تبدیل شده است. آژانس اطلاعاتی انگلیس نیز هشدار داده که روسیه در حال تبدیل شدن به نفوذگری ماهر در عرصه‌ی فضای مجازی است و از این طریق سیاست‌های خارجی خود را اعمال می‌کند.

FBS در خصوص اینکه سرویس‌های اطلاعاتی کدام کشورها حملاتی علیه بانک‌های روسیه انجام داده‌اند، چیزی نگفت ولی عنوان کرد که کارگزارها و مراکز فرماندهی این حملات بر روی سرویس میزبانی وب شرکت اوکراینی BlazingFast است که در هلند مستقر شده‌اند.

FBS همچنین می‌گوید انتشار مطالب تحریک‌آمیز راجع‌به بحران در سامانه‌های بانکی روسیه برنامه‌ریزی شده بود تا در شبکه‌های اجتماعی، وبلاگ‌ها و پیامک‌های تلفن همراه منتشر شود.

توصیه کارشناسان به دونالد ترامپ: آموزش ۱۰۰ هزار نفوذگر برای دفاع از آمریکا

به رئیس جمهور منتخب آمریکا، دونالد ترامپ توصیه شده است تا ۱۰۰ هزار نفوذگر را تربیت کرده و استخدام کند. هدف اصلی از آموزش این افراد، بیشتر نفوذ است ولی برای عملیات دفاعی نیز می‌توانند کاربرد داشته باشند.

کارشناسان امنیتی اشاره کرده‌اند که در زمان تصدی ریاست جمهوری توسط دونالد ترامپ، امنیت سایبری باید در رأس اولویت‌های او قرار بگیرد. علاوه بر این محققان به ترامپ توصیه کرده‌اند تنها به تربیت نفوذگران برای مقابله با تهدیدهای سایبری نپردازد بلکه نفوذگرانی را تربیت کند که در سطح بین‌المللی توانایی حمله‌ی سایبری و نفوذ نیز داشته باشند. این امر امنیت سایبری آمریکا را بهتر تضمین می‌کند.

امنیت سایبری باید اولویت اصلی ترامپ باشد

کمیسیون بهبود امنیت سایبری اشاره کرده است که آمریکا برای بهبود وضعیت امنیت سایبری باید متخصصان امنیتی را آموزش دهد که تنها برای بخش دولتی کار کنند و جذب بخش‌های خصوصی نشوند. این مسئله در چند سال اخیر به مشکل بسیار بزرگی تبدیل شده است.

همچنین در گزارش محققان امنیتی آمده است، حقوقی که شرکت‌های خصوصی به کارشناسان امنیتی می‌دهند بسیار بیشتر از حقوقی است که دولت آمریکا پرداخت می‌کند. از دونالد ترامپ خواسته شده است تا در سال اول ریاست جمهوری خود حتماً به این مسئله نیز رسیدگی کند.

به ترامپ توصیه شده است تا بر روی آموزش این نفوذگران از نزدیک نظارت و کنترل داشته باشد تا آموزش به این افراد با مهارت‌های پایین و بی‌کیفیت انجام نشود. پیشنهاد شده رئیس جمهور یک برنامه‌ی کاری برای امنیت سایبری بین‌المللی ایجاد کند تا از وقوع چنین اتفاقی پیشگیری شود.

گروه ناشناس‌ها از جان مک‌آفی می‌خواهد مشاور امنیتی ترامپ شود

به دونالد ترامپ توصیه شده است یک مشاور امنیتی برای خود استخدام کند تا در ماه‌های اول ریاست جمهوری به او در تعیین استراتژی های امنیت سایبری کمک کند. کارشناسان به ترامپ پیشنهاد داده‌اند متخصصان امنیتی که در شرکت‌های به‌نام و بزرگ کار می‌کنند را به آمریکا آورده و استخدام کند.

نفوذ به شبکه‌ی ارتش کره‌ی جنوبی توسط کره‌ی شمالی

گفته می‌شود کره‌ی شمالی به شبکه‌ی ارتش کره‌ی جنوبی حمله کرده تا به شبکه‌ی اینترانت و اطلاعات محرمانه‌ی این ارتش دست یابد.

وزارت دفاع کره‌ی جنوبی امروز اعلام کرد که این حمله در تاریخ 2 مهر رخ داده و سامانه‌های ارائه‌دهنده‌ی به‌روزرسانی را هدف قرار داده است. اگرچه دولت کره‌ی جنوبی هنوز مطمئن نیست که این حمله توسط کره‌ی شمالی انجام شده باشد ولی وزارت دفاع این کشور می‌گوید شواهدی پیدا کرده که نشان می‌دهد این حمله، مشابه حملات قبلی کره‌ی شمالی است.

وزارت دفاع در مصاحبه‌ای به خبرگزاری‌ها گفته است: «ارتش گروهی را برای بررسی این حمله تشکیل داد و یافته‌ها نشان می‌دهد برخی از داده‌های ارتش همچون اطلاعات محرمانه و نظامی در این حمله به سرقت رفته است. به نظر می‌رسد این حمله کار کره‌ی شمالی بوده باشد.» به نظر می‌رسد این حمله از سمت کارگزارهای مستقر در چین انجام شده باشد ولی ارتش می‌گوید شواهدی مبنی بر دخالت چین در این حمله مشاهده نشده است.

وزارت دفاع تأیید کرده که اطلاعات ارتشی و نظامی به سرقت رفته ولی در خصوص نتایج بدست آمده از تحقیقات، جزئیاتی ارائه نکرده است. این وزارت‌خانه گفته است: «ما نمی‌توانیم جزئیات اطلاعات به سرقت رفته را بازگو کنیم چرا که این اطلاعات می‌تواند در جنگ سایبری برای کره‌ی شمالی یک مزیت محسوب شود.»

به نظر می‌رسد بدافزاری که در این حمله استفاده شده، در مرداد ماه بر روی سامانه‌های هدف نصب شده است ولی هنوز مشخص نیست چرا نفوذگران کره‌ی شمالی تا تاریخ 2 مهر برای انجام حمله منتظر مانده‌اند.

به گزارش وزارت دفاع کره‌ی جنوبی، رایانه‌های ارتش به اینترنت نیز متصل نبوده‌اند ولی بدلیل بی‌دقتی و تخطی از مقررات توسط کارکنان، نفوذگران توانسته‌اند به اینترانت نفوذ کرده و از راه دور کنترل کامل شبکه را در دست گیرند.

کره‌ی جنوبی کارمندان خود را ملزم می‌کند در صورتی که اطلاعات طبقه‌بندی شده بر روی سامانه‌هایشان وجود نداشت به اینترنت متصل شوند و وقتی کارشان تمام شد، تمامی داده‌ها را حذف کنند. با وجود تمامی این محدودیت‌ها، نفوذگران توانستند پس از آلوده کردن چند کارگزار به اطلاعات محرمانه و نظامی دست یابند در حالی‌که بر روی این کارگزارها اطلاعات مهمی وجود نداشت.