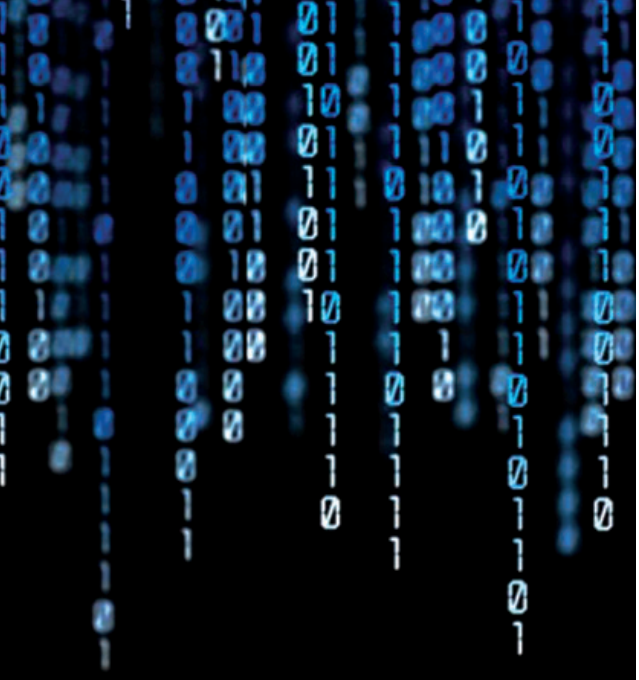
آیا برای حمله فلیم بعدی آماده ایم؟

میزگرد بررسی حمله سایبری شعله آتش (فلیم) با حضور کارشناسان

- آیا در شرایط جنگ سایبری هستیم؟
- شعله آتش از ۲۰۱۰ شروع شده است
- این جدی ترین هشدار سایبری است که ما تا به حال اعلام کرده ایم
- تا حدود زیادی ویروس ها شناسایی و پاک سازی شدند



آیا در شرایط جنگ سایبری هستیم؟

علیرضا صالحی

روز یک حمله سایبری به وسعت و پیچیدگی استاکس‌نت در سال ۲۰۱۰، کارشناسان را با مفهوم واقعی جنگ سایبری آشنا کرد.

جنگی که در آن زیرساخت‌های داده‌ای و در مفهومی وسیع‌تر، زیرساخت‌های سایبری یک کشور مورد هجوم قرار می‌گیرند و در آن همانند جنگ‌های کلاسیک، ابتدا جمع‌آوری داده‌های حیاتی مورد نیاز و سپس ضربه زدن به اهداف مورد نظر انجام می‌گیرد.

استاکس‌نت با خود مفهوم جنگ سایبری را در سطحی عمومی مطرح و اکنون، نسل بعدی آن یعنی فلیم (شعله آتش) مفهومی دیگر تحت عنوان سلاح سایبری را معرفی می‌کند. اگر نگاهی به اظهارنظرهای کارشناسان و متخصصان امنیت طی دو سال گذشته و به ویژه با شیوع بدافزار استاکس‌نت داشته باشیم، در می‌یابیم که همگان کم وبیش در مورد جنگ‌های سایبری آینده هشدار داده‌اند.

بروز حمله سایبری به وزارت نفت که به آشکارسازی بدافزار فلیم انجامید، ما را با این حقیقت روبه‌رو ساخت که جنگ سایبری را دیگر نه تنها به عنوان یک احتمال که به عنوان واقعیتی عینی باید پذیرفت.

سرمایه‌گذاری دولتی، پیچیدگی فوق‌العاده بالا، هوشمندی در طراحی و روش تکثیر، تنوع عملکرد، ثبت هرگونه فعالیت کاربران، آنالیز ترافیک شبکه، بسترسازی برای فعالیت‌های مخرب آتی، ایجاد سکوی توسعه بدافزارهای آتی، قرار گرفتن در حالت نهفته، انجام عکس‌العمل متناسب با نوع آنتی‌ویروس نصب‌شده روی سیستم، هدف قراردادن یک کشور یا یک صنعت خاص در یک کشور خاص، تخریب نوع یا انواعی از سخت‌افزارهای عمومی یا خاص و... تنها نمونه‌هایی از توانایی‌ها یا ویژگی‌های بدافزار فلیم است.

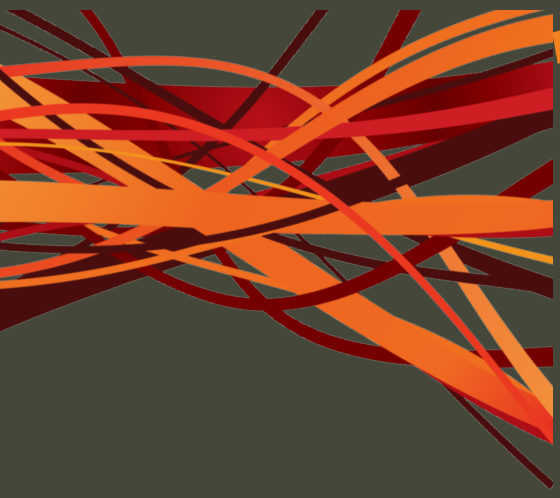
بدافزاری که از آن به عنوان جعبه ابزار بدافزاری یا یک سلاح واقعی سایبری نام برده می‌شود. خوشبختانه تجربه استاکس‌نت، سبب شد که مرکزی مانند ماهر که وظیفه پایش فضای سایبری و شناخت آسیب‌های آن را برعهده دارد، به خوبی وارد عمل شود و با تحلیل اطلاعات موجود و در زمان نسبتا مناسب، نسبت به این رخداد واکنش نشان دهد.

اما این رخداد ابعاد نگران‌کننده دیگری را نیز در بردارد. شروع نامشخص فعالیت این بدافزار که بین دو تا هشت سال قبل تخمین زده می‌شود، ما را مطمئن می‌کند که این بدافزار، اولین و آخرین این سلاح‌ها نبوده و نخواهد بود. پیچیدگی ابعاد طراحی این سلاح سایبری که به بیان ساده صدبرابر بیشتر از یک بدافزار متعارف و ۲۰ برابر بیش از استاکس‌نت بوده است، این پیام را می‌رساند که باید منتظر سلاح‌هایی با تخریب بسیار بیشتر و تنوع عملکرد و گستردگی وسیع‌تر باشیم.

ضمنا با توجه به اینکه سلاح سایبری کشف شده (فلیم) مربوط به تکنیک‌های طراحی چند سال قبل است، پیشرفت تکنیک‌های تولید بدافزارهای حال حاضر و آتی دور از انتظار نخواهد بود. حال با توجه به آنچه گفته شد، آیا تصور گزافی است که کشورمان را در شرایط جنگ سایبری فرض کنیم؟

این یادداشت قبلا در روزنامه شرق شماره ۱۵۴۴ تحت عنوان «شعله آتش به ما چه می‌گوید» منتشر شده است.

افتانا
پایگاه خبری افتانا
ویژه‌نامه افتانا/فلیم
۲ تیرماه ۱۳۹۱
www.aftana.ir



"شعله" آتش از ۲۰۱۰ روشن شده است

Flame یا شعله آتش نام سلاح سایبری نهان در شبکه‌های ایران و چند کشور منطقه است که فعالیت مخرب و جمع‌آوری اطلاعات را از سال ۲۰۱۰ میلادی آغاز کرده است.

به گزارش افتانا (پایگاه خبری امنیت اطلاعات)، پیرو انتشار گزارش مرکز ماهر در مورد تحلیل حمله سایبری به وزارت نفت و شناسایی بدافزاری به نام Flame یا شعله آتش شرکت کسپرسکی با تایید فعالیت آن، ابعاد جدیدی از آن را مشخص ساخته‌است.

براساس این گزارش، این بدافزار که با عنوان سلاح سایبری از آن نام‌برده شده‌است، پیچیده‌ترین جعبه‌ابزار فعالیت غیرمجاز سایبری است که تاکنون شناخته شده است و حتی از استاکس نت نیز پیچیده‌تر است.

این بدافزار ترافیک شبکه را تحلیل می‌کند، از صفحات نمایش عکس می‌گیرد، مکالمات صوتی تحت شبکه را ضبط می‌کند، ضرب کلیدها را ثبت می‌کند و درنهایت داده‌ها را به مرکز کنترل خودش ارسال می‌کند.

این گزارش می‌افزاید ایران بیشترین آسیب را از سال ۲۰۱۰ تاکنون از این بدافزار متحمل شده و احتمالا هدف ۱۸۹ حمله واقع شده‌است. ضمن آنکه رژیم صهیونیستی با ۹۸ حمله، سودان با ۳۲ حمله، سوریه با ۳۰حمله، لبنان با ۱۸ حمله ، عربستان سعودی با ۱۰ حمله و مصر با ۵حمله، دیگر هدف‌های این بدافزار بوده‌اند.

الکساندر گوستف، از تحلیلگران آزمایشگاه کسپرسکی معتقد است که این سلاح سایبری بر روی هیچ صنعت خاصی نشانه روی نشده و صرفا به کار جمع‌آوری داده‌های مهم در هر شبکه‌ای مشغول بوده است و ابزاری با قابلیت جمع‌آوری همه انواع داده‌های حساس بوده است.

وی می‌افزاید آزمایشگاه کسپرسکی پس از اعلام درخواست اتحادیه جهانی مخابرات مبنی بر شناسایی عامل پاک شدن داده‌ها در شبکه‌های چند کشور خاورمیانه وارد عمل شده و اقدام به تهیه و انتشار این گزارش نموده است.

گوستف می‌افزاید این بدافزار که با نام وایپر (Wiper) نیز شناخته می‌شود حجمی در حدود ۲۰ مگابایت دارد و نام دیگر آن Flame.Worm.Win32 است.

گزارش کسپرسکی تاکید دارد که این بدافزار که مجموعه کاملی از همه ابزارهای جاسوسی و جمع‌آوری اطلاعات است، شباهت‌های بسیاری به استاکس نت و دوکو دارد ولیکن به نظر می‌رسد که توسط گروه‌های متفاوتی نوشته شده‌اند و احتمالا به موازات یکدیگر توسعه یافته‌اند.

کارشناسان کسپرسکی با تاکید بر اینکه این بدافزار در حقیقت یک سلاح سایبری بسیار پیچیده‌است، از انجام تحقیقات بیشتر بر روی آن خبر داده‌اند.

افتانا
پایگاه خبری افتانا
ویژه‌نامه افتانا/ فلیم
تیرماه ۱۳۹۱

کسپرسکی
نسخه فارسی
www.irkaspersky.com

این حمله توسط بدافزاری با نام Flame صورت گرفته است

در پی بررسیهای تخصصی انجام شده توسط کارشناسان مرکز ماهر و در ادامه تحقیقات صورت گرفته پیرامون حملات هدفمند استاکس نت و دیوکیو، این مرکز برای نخستین بار اقدام به انتشار اطلاعات آخرین نمونه از حملات این خانواده می نماید.

به گزارش افتانا (پایگاه خبری امنیت فناوری اطلاعات)، در پی بررسی‌های تخصصی انجام شده طی چند ماه گذشته توسط کارشناسان مرکز ماهر و در ادامه تحقیقات صورت گرفته از سال ۲۰۱۰ پیرامون حملات هدفمند سازمان دهی شده استاکس نت و دیوکیو، این مرکز برای نخستین بار اقدام به انتشار اطلاعات آخرین نمونه از حملات این خانواده‌می‌نماید.

این حمله توسط بدافزاری که از این پس با نام Flame (شعله آتش) معرفی خواهد شد صورت می‌گیرد. این نام برگرفته از محتویات رمزگشایی شده فایل‌های اصلی بدافزار است. این بدافزار در واقع پلتفرمی است که قابلیت دریافت و نصب ابزارهای گوناگون جهت فعالیت‌های مختلف را داراست. در حال حاضر هیچ کدام از اجزای پرشمار تشکیل دهنده این بدافزار توسط بیش از ۴۳ نرم افزار آنتی ویروس در دسترس مورد شناسایی قرار نمی‌گیرند. با این وجود ابزار شناسایی و پاکسازی این بدافزار در مرکز ماهر تهیه شده و از امروز در اختیار سازمان‌ها و شرکت‌های متقاضی قرار خواهد گرفت.

شماری از قابلیت‌های مهم این بدافزار عبارتنداز:

- انتشار از طریق حافظه‌های فلش
- انتشار در سطح شبکه
- پویش شبکه و جمع آوری و ثبت اطلاعات منابع شبکه و رمز عبور سیستم‌های مختلف
- پویش دیسک کامپیوتر آلوده و جستجو برای فایل‌هایی با پسوندها و محتوای مشخص
- تهیه تصویر از فعالیت‌های خاص کاربر سیستم آلوده با ذخیره‌سازی تصاویر نمایش داده شده بر روی مانیتور کاربر
- ذخیره‌سازی صوت دریافتی از طریق میکروفن سیستم در صورت وجود
- ارسال اطلاعات ذخیره شده به سرورهای کنترل خارج از کشور
- دارا بودن بیش از ۱۰ دامنه مورد استفاده به عنوان سرور C&C
- برقراری ارتباط امن با سرورهای C&C از طریق پروتکل های SSH و HTTPS
- شناسایی و از کار انداختن بیش از ۱۰۰ نرم‌افزار آنتی‌ویروس، ضد بدافزار، فایروال و ...
- قابلیت آلوده سازی سیستم‌های ویندوز XP، ویستا و ویندوز ۷
- قابلیت آلوده‌سازی سیستم‌های یک شبکه در مقیاس بالا

به احتمال قریب به یقین و با در نظر گرفتن پیچیدگی و کیفیت بالای عملکرد و همچنین اهداف مشابه این بدافزار، میتوان آن را محصولی از خانواده استاکس نت و دیوکیودانست.

نشانه‌های یافت شده حاکی از آن است که رویدادهای رخ داده اخیر درخصوص از بین رفتن همزمان اطلاعات سیستم‌های کامپیوتری نتیجه فعالیت یکی از اجزای این بدافزارمیباشد.

با تحلیل انجام شده فهرستی از اجزای تشکیل دهنده این بدافزار شناسایی شده و در جدول زیر ارائه میگردد. این اطلاعات قابل ارائه به تولیدکنندگان عمده آنتی‌ویروس می‌باشد و از این پس اجزای این بدافزار میتـواند مورد شناسایی آنتی‌ویروس‌ها قرار گیرد.

علائم آلودگی و جزئیات اجزای تشکیل دهنده‌بدافزار

وجود هریک از این نشانه‌ها بیانگر آلودگی سیستم به بدافزار Flame است:

ردیف	نوع علائم	آدرس
1	وجود کلید رجیستری	HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa\Authentication Packages -> mssecmgr.ocx
2	فایلهای اجرایی و تنظیمات آلودگی	windows\system32\mssecmgr.ocx Windows\System32\ccalc32.sys Windows\System32\msglu32.ocx Windows\System32\boot32drv.sys Windows\System32\nteps32.ocx Windows\System32\advnetcfg.ocx Windows\System32\soapr32.ocx Windows\System32\to961.tmp Windows\ EF_trace.log

سازمان ملل درباره خطر ویروس "فلیم" هشدار می‌دهد

این جدی‌ترین هشدار سایبری است که ما تا به حال اعلام کرده‌ایم

یک آژانس سازمان ملل که متعهد به کمک به کشورهای عضو در ایمن کردن طرح‌های زیربنایی ملی‌شان است، درباره خطرات ویروس «فلیم» (Flame) که اخیرا در ایران و بخش‌های دیگر خاورمیانه کشف شده است، هشدار صریحی داد.

به گزارش افتانا (پایگاه خبری امنیت فناوری اطلاعات)، مارکو اوبیسو، هماهنگ کننده امنیت سایبری در اتحادیه بین‌المللی ارتباطات دوربرد (ITU) وابسته به سازمان ملل مستقر در ژنو در این باره گفت: «این جدی‌ترین هشدار سایبری است که ما تا به حال اعلام کرده‌ایم.»

او در مصاحبه‌ای گفت این هشدار محرمانه برای کشورهای عضو روشن خواهد کرد که ویروس «فلیم» یک ابزار خرابکاری خطرناک است که بالقوه می‌تواند برای حمله به زیربنای حیاتی کشورها مورد استفاده قرار گیرد. او می‌گوید: «کشورهای عضو باید در این باره هشیار باشند.»

بر اساس گزارش شرکت کسپرسکی لب، سازنده روسی نرم‌افزارهای امنیت سایبری که به خاطر کشف ویروس‌های کامپیوتری شهرت دارد، شواهد بیانگر آن است که این ویروس که «فلیم» نامیده شده است بوسیله همان کشور یا کشورهای سازنده کرم «استاکس‌نت» که در سال ۲۰۱۰ به برنامه هسته‌ای ایران حمله کرد، ساخته شده است.

اوبیسو گفت که «به نظر من این ویروس جدید تهدیدی بسیار جدی‌تر از استاکس‌نت است.»

او گفت ITU برنامه‌ای برای جمع‌آوری داده‌ها، شامل نمونه‌های ویروسی، را ترتیب داده است تا انتشار «فلیم» در سراسر جهان و تغییرات ترکیب آن را ردیابی کند.

کسپرسکی لب می‌گوید عفونت با ویروس» فلیم» را پس از آن یافت که ITU از این شرکت خواست گزارش‌های اخیر از تهران درباره یک ویروس اسرارآمیز که باعث دست رفتن گسترده داده‌ها در برخی از سیستم‌های کامپیوتری شده است، را مورد بررسی قرار دهد.

به گفته اوبیسو گروه کسپرسکی لب هنوز نسخه اصلی این ویروس پاک کننده داده‌ها را در اختیار ندارد و دولت ایران نمونه‌ای از این نرم‌افزار را به کسپرسکی نداده است.

وزیر آی‌سی‌تی:

تا حدود زیادی ویروس‌ها شناسایی و پاک‌سازی شدند

تقی‌پور: ما اولین کشوری بودیم که توانستیم ویروس فلیم را شناسایی و آن را به دنیا اعلام کنیم؛ پس از این مرحله بلافاصله ضدبدافزارهای آن نوشته شد به نحوی که تا حدود زیادی ویروس‌ها شناسایی و پاک سازی شدند.

وزیر ارتباطات و فناوری اطلاعات تاکید کرد: به هیچ عنوان به دلیل حملات سایبری فلیم آسیب قابل ذکری به کشور وارد نیامده است.

به گزارش افتانا (پایگاه خبری امنیت فناوری اطلاعات)، رضا تقی‌پور اظهار کرد: باید درباره حملات اینترنتی بگوییم که برخلاف اغلب حملات معمول که از طریق هکرها و یا افراد طراحی می‌شد، این بار حملات با اهداف خاص و از سوی دولت‌ها برنامه‌ریزی شده بود.

وی ادامه داد: ما درباره این مطلب در مجامع بین‌المللی طرح موضوع کرده و از این مجامع خواستیم که هشدارهای لازم را به کشورهای حمله کننده بدهند. البته خود ما هم تلاش‌های متعددی داشته‌ایم و سعی داریم از وقوع این حملات جلوگیری کنیم.

تقی‌پور ادامه داد: البته توانمندی‌های داخلی و فناوری‌های بومی ما آنچنان بالاست که به هیچ عنوان از این حملات آسیب قابل ذکری به کشور نرسیده است و تمام سازمان‌های ما توانسته‌اند با این حملات مقابله و برخورد کنند و در این زمینه هیچ کم و کسری وجود ندارد.

اما وزیر ارتباطات و فناوری اطلاعات در پاسخ به سوال خبرنگاران مبنی بر این که آیا آنتی‌ویروس‌های لازم به بخش‌های کشور تحویل داده شده است اظهار کرد: ما اولین کشوری بودیم که توانستیم ویروس فلیم را شناسایی و آن را به دنیا اعلام کنیم؛ پس از این مرحله بلافاصله ضدبدافزارهای آن نوشته شد به نحوی که تا حدود زیادی ویروس‌ها شناسایی و پاک سازی شدند.

وی در ادامه در پاسخ به سوال دیگری مبنی بر این که آیا ممکن است تلاش ایران برای راه‌اندازی شبکه ملی اطلاعات موجب گسترش چنین حملاتی شده باشد گفت: قطعا یکی از بحث‌هایی که موجب این حملات می‌شود آن است که دشمنان می‌خواهند از این پیشرفت‌ها جلوگیری کنند و اجازه ندهند ما در زمینه‌های کلی و بنیادی پیشرفت‌های متعدد داشته باشیم. اما خوشبختانه ما این حملات را مهار کرده‌ایم و حملات سایبری یکی از ملاحظاتی است که در طراحی مباحث مربوط به شبکه ملی اطلاعات کاملا مورد توجه قرار گرفته است.

افتا
پایگاه خبری افتا
ویژه‌نامه افتا/فلیم
تیرماه ۱۳۹۱ ۷
www.aftana.ir

آیا برای فلیم بعدی آماده‌ایم؟

میزگرد بررسی تأثیرات حمله سایبری فلیم بر فضای امنیت اطلاعات ایران

مقدمه:

حمله سایبری فلیم (شعله‌آتش) که پس از حمله استاکس‌نت در سال ۲۰۱۰ دومین حمله هدفمند به زیرساخت‌های سایبری کشورمان بود، بار دیگر زنگ خطر در مورد لزوم توجه جدی به امنیت فضای تبادل‌اطلاعات را به صدا درآورد. اما این بار و برخلاف حمله استاکس‌نت آمادگی بیشتری در میان سازمان‌های دولتی در بین خصوصی دیده‌شد. هر چند که کماکان ضعف‌های عمده‌ای در این میان دیده‌شود. عملکرد خوب مرکز ماهر در شناسایی و ارائه برنامه پاکسازی شعله‌آتش از نقاط قوت فعالیت ماهر بود که متاسفانه مکان گفتگو و حضور ایشان در میزگرد برگزار گردید. نمایندگان شرکت‌های بخش خصوصی و ارائه‌کنندگان ضد ویروس‌های خارجی به تحلیل این ماجرا پرداختند. در این میزگرد آقایان رستمی (مدیر دپارتمان بیت‌دیفندر در شرکت بدرالکتریک)، اخلاقی (مدیرعامل شرکت دمسان رایانه)، بقایی (مدیرعامل شرکت ایدکو) و رمضانی‌نیا (کارشناس فنی شرکت آرکا سامانه) حضور داشتند و به بیان دیدگاه‌های خود پرداختند.

کسپرسکی
نسخه فارسی
www.irkaspersky.com

صالحی: اجازه دهید بحث را با بررسی تاثیرات فلیم بر فضای سایبر آغاز کنیم و اقدامات شرکت‌های ارائه‌کننده ضد بدافزار که در مقابله با این بدافزار فعالیت‌کردند را بررسی‌نماییم. از آنجاییکه سیمانتک و کسپرسکی بازخورد سریعتری را نسبت به این موضوع داشتند، ابتدا از ایشان می‌خواهم که صحبت را آغاز کنند.

بقـایی: باید گفت که فلیم یکی از قویترین سلاح‌های سایبری است که تا به حال در مجموعه جنگ‌های سایبری مورد استفاده قرار گرفته که برای ایران طراحی شده بود. این سلاح سایبری از سال ۲۰۱۰ مشغول فعالیت بود و یکسری از اطلاعات را سرقت کرده و به منابع مورد نظر خودش انتقال داده است.

صـالحی: موضوع فلیم از کجا آغاز شد؟ ظاهرا جرقه اولیه وجود آن بعد از حمله سایبری به وزارت نفت زده شد. اما ظاهراً پیشینه دیگری هم داشته است.

اخـلاقی: اولین موضوعی که مطرح شد و شاید بتوان آن را به فلیم هم مرتبط کرد اتفاقی بود که در اسفند سال ۹۰ رخ داد که برای یکی از شرکت‌های شهرستانی بوقوع پیوست. در آن زمان گزارش شد که همه اطلاعات آن ها پاک شده است و بعد از آن بود که زمزمه وجود نوعی بدافزار که اقدام به پاک کردن اطلاعات رایانه‌ها می‌کند شنیده شد. اما اتفاق جدی که ذهن‌ها را متوجه خود کرد اتفاقی بود که در دوم اردیبهشت‌ماه حوالی ساعت۱۲ روی‌داد و طی آن همه رایانه‌ها restart شده بودند و همه اطلاعات آن پاک شده بود. ابتدا گمان بر این می‌رفت که حمله هکری شده باشد اما بعدا معلوم‌شد که دستور خودکشی به آن بدافزار ابلاغ شده است که خود را پاک کند. من فلیم را به عنوان یک ابزار چند وجهی مد نظر دارم چرا که یک جاسوس افزار حرفه‌ای است که اقدام به سرقت اطلاعات می‌کند و هم اینکه می‌توان از آن برای خرابکاری استفاده کرد و نوع خرابکاری آن هم بسیار منحصر به فرد است چرا که تا الان وسعت خرابی‌هایی که این بدافزار به‌وجود آورده است سابقه نداشته است و به نوعی طراحی این نوع سلاح سایبری در واقع زنگ هشدار برای آغاز یک جنگ سایبری می‌باشد.

رستمـی: تمام مسائلی که دوستان فرمودند به نوعی صحیح است، اما طبق گزارش‌هایی که ما از بیت دیفندر دریافت کردیم، فلیم توسعه یافته بدافزاری است که در سال ۲۰۰۵ تولید شده بود و البته بدافزار سال ۲۰۰۵ صرفا با مقاصد جاسوسی طراحی شده بود که مسئله انجام فعالیت‌های تخریبی در فلیم گنجانده شده است و به نوعی ابزار جدیدی را با خود به همراه داشت.

صـالحی: آنطوریکه در رسانه ها منتشر شد، بیشترین هجوم مربوط به رایانه‌های شرکت نفت بوده است، چه اتفاقاتی بعد از این حمله صورت گرفت؟

رستمـی: تا آنجـاییکه که ما می‌دانیم بعد از این حمله کلیه شبکه و سیستم‌های رایانه‌ای قطع شدند و دستورالعملـی برای راه اندازی شبکه اینترنت خارج از شبکه سازمانی به واحدهای زیر مجموعه ابلاغ شده‌است که به این ترتیب هر سازمانی باید دو شبکه مستقل برای خود داشته باشد که یکی مربوط به امور داخلی سازمان است و دومی مربوط به استفاده از اینترنت و این دو شبکه به هیچ عنوان نباید به یکدیگر ارتباط داشته باشند. البته با ذکر این نکته که انجام این پروژه طرح جدیدی نیست و سال ۸۴ و ۸۵ نیز دستورالعمل مشابهی نه تنهـا در وزارت نفت بلکه در سایر نهادها نیز ابلاغ شد. اما از همان زمان هم کارشناسان و مشاورین انجام چنین را تائید نکردند. چرا که به زعم آن ها انجام چنین پروژه‌ای راه حل منـاسبی برای حل مشکلات ایجاد شده نیست. چرا که برای ارتقا امنیت در سازمان می‌بایست که ابتدا تعریف امنیت پیاده‌سـازی شود و اگـر تعریف امنیت در سازمـان به درستی صورت نپذیرد قطعا در بخشی از سازمـان این دو شبکه به هم متصـل خواهنـد شد که همیـن اتصـال کوتـاه و یا کوچک کل فرآیند را به محل اولیه خود باز می‌گرداند. اما این دستورالعمل مجددا به صورت جدی‌تری ابلاغ شده و در حال پیگیری برای پیاده‌سازی آن است. حتی تا جائیکه بنده می‌دانم ورود حافظه فلش نیز به سازمان‌های تابعه وزارت نفت تنها بعد از بررسی آن از لحاظ وجود ویروس و پاکسازی آن میسر می‌باشد.

بقـایی: اگر بخواهیم واکنش‌ها را از نگاهی دیگر بررسی کنیم میبینیم که در همان ایام بروز بحران، رفت و آمد به مراکز و بخش های رایانه‌ای بسیار محدود شد تا جائیکه حتی افراد کمی بودند که توانستند از نزدیک مشکل به وجود آمده را ببینند و این مسئله، مسئله مهمی بود. به نظرم چرا که تا مدت زمان زیادی حتی نمونه‌ای از سیستم آلوده نیز در اختیار کسی قرار نگرفت. چرا که بالاخره هر یک از سازمان‌های تابعه وزارت نفت مدت‌های زیادی بود که با شرکت‌های ارائه دهنده خدمات

ما بایـد امنیت را به عنوان یک فرایند ببینیم و نگـاه سیستمی بـه مسئـله امنیت داشته باشیـم.

و محصولات امنیت در حال همکاری بودند. در نتیجه بهتر بود که نمونه فایل‌های آلوده در اختیار شرکت‌ها قرار می گرفت.
در همان زمان اسفند ماه ۹۰ که اولین اتفاقات رخ داد نیز ما با تمام مشتریان خود تماس گرفتیم و از آن‌ها خواستیم که از اطلاعات خود نسخه پشتیبان تهیه کنند تا در صورت آلوده بودن به بدافزار اتفاق جدی برای آن‌ها نیفتد. حتی در فاصله اسفند تا اردیبهشت هم به بسیاری از مشتریان خود گفتیم که می‌توانیم از کسپرسکی متخصصانی را به ایران بیاوریم تا به بررسی مسئله بپردازند، حتی قرار شد که هماهنگی‌هایی با وزارت خارجه نیز صورت بگیرد اما متاسفانه هیچ پیگیری بعدی صورت نگرفت. چه خوب بود که در همان اسفند ۹۰ مسئله جدی گرفته می‌شد تا شاهد این اتفاق در اردیبهشت ماه نباشیم.

اخلاقی: در تکمیل این حرف‌ها باید اضافه کنم که حتی تا اوایل خردادماه هم هیچ گونه اطلاعات مناسبی و درخوری منتشر نشد.

بقایی: فلیم به نظر من باعث شد که مرکز ماهر از یک توانایی بالقوه به یک توانایی بالفعل برسد.

رستمی: اگر بخواهیم از نگاه کلان‌تری به مسئله نگاه کنیم باید بگوییم که ما در مملکت یک بیماری داریم به نام بیماری امنیت. فارغ از اینکه بدافزاری وجود دارد یا خیر و اینکه چه کسی می‌خواهد در مقابل این بدافزارها از خود دفاع کند یا خیر به نظر من باید مشکل را در ابعادی بزرگ‌تر بررسی کرد و آن مشکل فرایند امنیت است و اینکه متولی صاحب صلاحیتی در این زمینه نداریم. البته تشکیل مرکز ماهر برای رسیدگی به این فرآیند حرکت خوبی است اما به راستی ماهر برای پیاده سازی این مسئله تا به حال چه حرکت جدی کرده است؟ به نظر اگر این اتفاق در سازمان‌های ما بیفتد بسیاری از مسائل حل می شود و متوجه می‌شوند که زمانی که مجددا چنین اتفاقاتی رخ داد باید به شرکت‌هایی که در این حوزه فعالیت می‌کنند اعتماد کرد، به آن‌ها فضا داد و از کمک آن‌ها استفاده کرد.

اخلاقی: من هم با این مسئله موافقم، اعتماد به شرکت‌های فعال در حوزه امنیت سایبر بسیار مهم است.

رستمی: ما حتی برای دریافت نمونه‌های آلوده بسیار تلاش کردیم. به هر صورت باید این نمونه‌ها توسط افراد متخصصی تست می شدند. کما اینکه شاید همین نمونه‌های آلوده هم دارای نسخه‌های متفاوتی باشند.

بقایی: اما به این موضوع می‌توان نگاه دیگری هم داشت و آن اینکه ماجرای فلیم به نظر من باعث شد که مرکز ماهر از یک توانایی بالقوه به یک توانایی بالفعل برسد. به طور مثال تا قبل از این ماجرا چیزی که از ماهر دریافت می‌کردیم تنها گزارش‌هایی مبنی بر وجود آلودگی‌هایی بود و انصافا هم وب سایت ماهر تا به حال مقالات و گزارش‌های خوبی را منتشر کرده است. اما موضوع فلیم به طور خاص باعث شد که ماهر به صورت عملیاتی وارد شود و اتفاقا دولت و وزارت نفت هم به این مرکز اطمینان کردند .

صالحی: در بین مشتریانی که شما دارید به خصوص بعد از ماجرای فلیم آیا باعث شد که هیچ کدام از سازمان ها فردی را به عنوان مدیر امنیت اطلاعات به کارگیرند یا بخشی را با این عنوان ایجاد کنند؟

رستمی: معمولا در سازمان هایی که مشتری ما هستند یک فردی هست که متولی امنیت است و بعد از این ماجرای نیز کماکان همان افراد هستند اما در سازمان‌های زیادی می‌بینیم که وظایف امنیت سایبری به خوبی تفکیک نشده‌اند وبا وظایف حراست سازمان‌ها تداخل دارد. متاسفانه بعد از ماجرای فلیم، این تداخل بیشتر هم شده است.

صالحی: اگر بخواهیم تا اینجا یک جمع‌بندی انجام دهیم باید بگوییم که یک نظام مدیریت امنیت اطلاعات و پیاده‌سازی استاندارد ISMS می‌توانست در تدوین سناریوی بحران به سازمان‌ها کمک کند تا بتوانند در چنین مواقعی باید چه بکنند.؟

اخلاقی: در تایید این سخنان باید بگویم که در واقع ما نه در بخش پیشگیری و نه در بخش مدیریت بحران هیچ نظام تعریف شده‌ای نداریم و غالبا در موقع برخورد با مشکلات به صورت بداهه آن‌را مدیریت می‌کنیم. اما نکته مهمی که باید بیشتر به آن پرداخت مسئله تفکیک اینترنت از شبکه داخلی است که به نظر من تنها نکته‌ای که دارد این است که حمله سایبری بعدی به کشور به مراتب مخرب‌تر خواهد بود، چرا که یک اعتماد کاذبی به وجود می‌آورد. و دیگر اینکه که بدافزاری که در آن صورت به شبکه حمله خواهد کرد قطعا هدف تخریبی دنبال خواهد کرد و به جمع آوری اطلاعات بسنده نخواهد کرد.

حمله سایبری بعدی به کشور به مراتب مخرب‌تر خواهد بود

اشکال به صورت کلی اینجاست که زمانی که ما راهکاری را پیشنهاد می‌کنیم راهکاری بدون توجه به نتیجه است.

صـالحی: البته تفکیک شبکه‌ها از اوائل دهه هشتاد در برخی وزارت خانه‌ها صورت گرفته است.

رستمـی: البته ضمن تایید صحبت‌های آقای اخلاقی اضافه کنم که بنده هم تا به حال هیچ سند و گزارشی ندیدیم که حتی در مکان‌هایی با درجه اهمیت امنیتی بالا نیز چنین پروژه‌های پیاده شده باشد.

اخـلاقی: البته باید اضافه کنم در خارج از ایران تفکیک شبکه وجود دارد اما در مراکز بسیار خاص این امر اتفاق افتاده است.

رستمـی: ولی همانطور که شما اشاره کردید در مراکزی با ویژگی‌های بسیار خاص چنین اتفاقی افتاده است نه اینکه یک نسخه ثابت برای کلیه سازمان‌ها و نهادها بپیچیم که همه باید شبکه خود را تفکیک کنند.

اخـلاقی: نکته جالب اینکه در مکان‌هایی هم که این تفکیک شبکه صورت گرفته است دستورالعمل دسترسی و کار با شبکه‌ای که به اینترنت متصل نیست بسیار مفصل‌تر و جدی‌تر از شبکه ای است که به اینترنت متصل است.

صـالحی: در تکمیل این گفته‌ها هم به یک مثال نقض خیلی مناسب می‌توان اشاره کرد و آن هم استاکس نت است. استاکس نت بدافزاری بود که اتفاقا از طریق اینترنت منتقل نشد و همین مساله ثابت می‌کند که انتقال بدافزارها به هر صورت از طریق شبکه انجام می‌گیرد چه این شبکه به اینترنت متصل باشد و چه اینکه متصل نباشد. حالا آیا درست است که همه ما مسئولیت چنین اتفاقی را به حساب نرم‌افزارهای ضد بدافزار بگذاریم و فعالیت‌های آنان را زیر سئوال ببریم؟

بقـایی: در قدم اول باید بگویم که تمامی شرکت‌های ضد بدافزار اولین کاری که انجام می‌دهند این است در توافقنامه اولیه استفاده از نرم افزار که معمولا هم کمتر کسی آن را می‌خواند اعلام کنند که اگر اتفاقی بیفتد و به موجب آن اطلاعات شما سرقت شود یا اینکه تخریب شود، با اینکه ما تا حد ممکن سعی می‌کنیم جلوی بروز آن را بگیریم ولی در عین حال تعهدی متوجه ما نیست

لذا ضد بدافزار به هیچ عنوان ضمانتی نمی‌دهد که شما هیچ‌گاه دچار مشکلی نمی‌شوید بلکه ابزاری است برای اینکه میزان آلودگی‌های شما را به حداقل برساند. لذا ضدبدافزار همه چیز نیست به طور مثال هیچ ضدبدافزاری نسبت به حفره‌های امنیتی سیستم عامل هم تعهدی ندارد.

اخـلاقی: باید گفت که ضدبدافزار یک سامانه ری‌اکتیو(واکنشی)است.به عبارتی حتما باید چیزی پیدا شود و بعد شرکت صاحب برند ضد ویروس آن را تحلیل کند وابزار پاک‌سازی وجلوگیری از گسترش آن را بسازد و در نهایت در قالب به روزرسانی این ابزار به نرم‌افزار ضد بدافزار افزوده می‌شود.

لذا برای ارتقاء امنیت باید به مسئله پرواکتیو (پیشگیرانه) توجه کرد. حال ممکن است صاحب برند ضد بدافزار همراه نرم افزار یا در خود نرم افزار چنین ابزارهایی را هم به شما ارائه کند. البته هیچ کدام از این‌ها نمی‌تواند جایگزین نظام مدیریت امنیت اطلاعات شود. چرا که هر کدام از اینها بخشی از این نظام هستند.

رمضانی‌نیـا: یکی از مسـائلی که بایـد به آن توجه کرد کمبـود دانـش فنـی افـراد و کارکنـان سازمـان‌هـاوحتـی‌بخـش‌هـای حراستـی است.

رستمـی: باید به این نکته توجه کرد که در واقع ضدبدافزار جزئی از همین نظام فراگیر مدیریت امنیت اطلاعات است وهمه این نظام نیست. به عنوان یکی از این اجزاء در محل خودش وظیفه مربوطه را انجام می‌دهد و باید گفت که اگر هر جزء از این نظام ناقص باشد طبیعتا سامانه دچار مشکل خواهد شد.

اخـلاقی: نگاه در واقع به این ترتیب است که چون یک بدافزاری موجب مشکل شده است پس ضدبدافزار مقصر اصلی ماجرا است.

رستمـی: در واقع باید گفت که زمانی که ما هنوز در بسیاری از سازمان‌ها تعریف رفتار سازمانی به درستی لحاظ نشده است لذا نمی توان از ضدبد افزار انتظار معجزه داشت و باز هم اشاره می‌کنم که باید به فرایند پیاده‌سازی نظام مدیریت امنیت اطلاعات بصورت کلی توجه کرد.

باید به شرکت‌هـایی که در این حـوزه فعـالیت می‌کنند اعتمـاد کرد

افتا
پایگاه خبری افتا
ویژه‌نامه افتا/فلیم
تیـرمـاه ۱۳۹۱
۱۰
www.aftana.ir

رمضانی‌نیا: یکی از مسائلی که باید به آن توجه کرد کمبود دانش فنی افراد و کارکنان سازمان‌ها و حتی بخش‌های حراستی است به طور مثال حتی در یکی از سازمان‌های کشور که بحث تفکیک شبکه داخلی از شبکه اینترنت نیز در آن صورت گرفته و نرم‌افزار ضد بدافزار نیز مورد استفاده قرار می‌گیرد بسیاری از موارد امنیتی رعایت نمی‌شود. در نتیجه با وجود نرم‌افزار و سخت‌افزار امنیتی مناسب، همچنان مشکلات امنیتی پابرجاست.
در یک جمله داشتن انواع ابزارها بدون داشتن دانش فنی نمی‌تواند کمک مهمی به ارتقاء سطح امنیت سازمان کند.

اخلاقی: البته یک مخالفت کوچکی با این نتیجه گیری داشته باشیم که با افزایش ابزارها می‌توانیم امنیت را افزایش دهیم ولی مسئله مهم اینکه نباید این مسئله باعث شود که خیالمان راحت باشد و به عبارتی نباید باعث بی‌تفاوتی ما شود.

رمضانی‌نیا: در واقع اینگونه بیان می‌کنم که اگر ما رانندگی بلد باشیم تفاوتی نمی‌کند که چه ماشینی داریم، این ماشین قدیمی است یا یک ماشین لوکس و مهم سواد ما در خصوص چگونگی رانندگی و تجربه و مهارت رانندگی است و امکانات ماشین در اولویت بعدی رانندگی است.

صالحی: یک سؤال مهم هنوز باقی است. استاکس نت آمد و موجی از لزوم توجه به امنیت در سازمان ایجاد کرده. هم اکنون موج دومی به نام فلیم ایجاد شده است که باز هم ممکن است به بالا رفتن سطح امنیت کمک کند. اما آیا به نظر شما ما برای فلیم بعدی آماده‌ایم؟

بقایی: باید گفت که حتی گفتن اینکه آماده هستیم یا نه زمانبر است، و باز هم تاکید می کنم که مسئله مهم این است که ما باید امنیت را به عنوان یک فرایند ببینیم و نگاه سیستمی به مسئله امنیت داشته باشیم. ما اگر بتوانیم استانداردهای مدیریت امنیت را اجرایی کنیم عملا آمادگی لازم را کسب خواهیم کرد. به نظر می‌رسد که اقداماتی هم در این راستا انجام شده است و حداقل اینکه گام‌هایی در خصوص پیاده‌سازی ISMS برداشته شده است. اما متاسفانه ما معمولاً دچار فراموشی می‌شویم و تا بروز حادثه بعدی اقدام خاصی را انجام نمی‌دهیم.

اخلاقی: از این بابت که در خصوص فلیم بعدی آمادگی چندانی وجود ندارد و باید گفت بله واقعا آمادگی وجود ندارد و همچنین باید تاکید کنم که فلیم بعدی به مراتب مخرب تر است.

صالحی: چرا فکر می‌کنید فلیم بعدی مخرب‌تر است؟

اخلاقی: چرا که الآن به فلیم می‌گوییم سلاح سایبری، چرا اسم سلاح را روی آن گذاشتیم؟ چون یک دولت آن راتهیه کرده است و طبیعتا دولت متخاصم تمام تلاش خود را برای اینکه این سلاح بتواند ضربه قوی‌تری به مقاصد مورد نظر وارد کند خواهد کرد و حتی این پروژه تفکیک‌سازی اینترنت از اینترنت تسریع کننده این جریان خواهد بود به نحوی که حتی حمله بعدی آن چنان صدماتی به بار آورد که دیگر هیچ چیز قابل جبران نخواهد بود.

رمضانی‌نیا: حداقل اینکه در حال حاضر الان فرهنگ خرید ضد بدافزار تقریبا جا افتاده است باز هم جای خوشحالی است اما اینکه باز هم استفاده از ابزارهای نامناسب و استفاده از سیستم عامل‌های کرک شده هنوز باب است قطعا موجب نگرانی می‌شود.

اخلاقی: مسئله‌مهمی که به نظرم باید به‌آن پرداخت ایجاد یک مرکز CERT با حضور نمایندگان بخش خصوصی است.

بقایی: می‌خواهم تأکید کنم که اگر همین فلیم منجر به اخذ تصمیمات امنیتی جدی تری شود هم خوب خواهد بود.

اخلاقی: اما چون هنوز مشکلات زیرساختی داریم بهتر است به آن توجه کنیم که در صورت بروز حمله مجدد بتوانیم جلوی آنرا بگیریم.

رمضانی‌نیا: اگر شرکت‌ها به سمت تخصصی‌تر شدن بروند و راهکار محورتر بشوند، می‌توانند بسیاری از این قبیل مشکلات را حل کنند.

اخلاقی: مسئله مهمی که به نظرم باید به آن پرداخت ایجاد یک مرکز CERT با حضور نمایندگان بخش خصوصی است به عبارتی ایجاد نهادی با حضور نمایندگان همه شرکت‌های فعال در بخش خصوصی است منجر به هماهنگی‌های بیشتری دست‌یابند و راهکارهای جامع‌تری را برای مدیریت صحیح بحران‌ها و پیاده‌سازی نظام مدیریت امنیت اطلاعات ارائه کنند.

توفیق رمضان نیا
در حال حاضر الان فرهنگ خرید ضد بدافزار تقریبا جا افتاده است

اینفوگرافی فعالیت بدافزار Flame (شعله آتش)

میزگرد بررسی تاثیرات حمله سایبری فلیم بر فضای امنیت اطلاعات ایران

در «شعله» بعدی می‌سوزیم یا از روی آن می‌پریم

حمله سایبری فلیم (شعله آتش) که پس از حمله استاکس نت در سال ۲۰۱۰ دومین حمله هدفمند به زیرساخت‌های سایبری کشورمان بود، بار دیگر زنگ خطر لزوم توجه جدی به امنیت فضای تبادل اطلاعات را به صدا درآورد. البته این بار بر خلاف حمله استاکس نت آمادگی بیشتری در میان سازمان‌های دولتی و خصوصی دیده شد. در میزگردی برای بررسی عملکرد سازمان‌ها به ویژه مرکز ماهر آقایان رستمی (مدیر دپارتمان بیت دیفندر در شرکت بدرالکتریک)، اخلاقی (مدیر عامل شرکت دمسان رایانه)، بقایی (مدیر عامل شرکت ایدکو) و رمضانی نیا (کارشناس فنی شرکت آرکا سامانه) به بیان دیدگاه‌های خود پرداخته اند.

اجازه دهید بحث را با بررسی تاثیرات فلیم بر فضای سایبر آغاز کنیم و اقدامات شرکت‌های ارایه کننده ضد بدافزار که در مقابله با این بدافزار فعالیت کردند را بررسی کنیم. از آنجاکه سیمانتک و کسپرسکی باز خود سریع تری به این موضوع داشتند، ابتدا از ایشان می خواهم که صحبت را آغاز کنند.

بقایی: باید گفت که فلیم یکی از قوی ترین سلاح‌های سایبری است که تابه حال در مجموعه جنگ‌های سایبری مورد استفاده قرار گرفته که برای ایران طراحی شده بود. این سلاح سایبری از سال ۲۰۱۰ مشغول فعالیت بود و یکسری از اطلاعات را سرقت کرده و به منابع مورد نظر خودش انتقال داده است.

موضوع فلیم از کجا آغاز شد؟ ظاهرا جرقه اولیه وجود آن بعد از حمله سایبری به وزارت نفت زده شد. اما ظاهرا پیشینه دیگری هم داشته است.

اخلاقی: نخستین موضوعی که مطرح شد و شاید بتوان آن را به فلیم هم مرتبط کرد اتفاقی بود که در اسفند ماه سال ۹۰ برای یکی از شرکت‌های شهرستانی به وقوع پیوست. در آن زمان گزارش شد که همه اطلاعات آنها پاک شده است. بعد از آن بود که زمزمه وجود نوعی بدافزار که اقدام به پاک کردن اطلاعات رایانه‌ها می کند شنیده شد اما اتفاق جدی که ذهن‌ها را متوجه خود کرد اتفاقی بود که در دوم اردیبهشت ماه حوالی ساعت ۱۲ روی داد و طی آن همه رایانه‌ها restart شده بودند و همه اطلاعات آنها پاک شده بود. ابتدا گمان بر این می‌رفت که حمله هکری شده باشد. اما بعدا معلوم شد دستور خودکشی به آن بدافزار ابلاغ شده است که خود

رمضانی نیا: داشتن انواع ابزارها بدون دانش فنی نمی تواند به ارتقای سطح امنیت سازمان کمک کند

را پاک کند. من فلیم را به عنوان یک ابزار چند وجهی مدنظر دارم. چرا که یک جاسوس افزار حرفه‌ای است که اقدام به سرقت اطلاعات می کند و هم اینکه می توان از آن برای خرابکاری استفاده کرد و نوع خرابکاری آن هم بسیار متحصر به فرد است چرا که تا الان وسعت خرابی‌هایی که این بدافزار به وجود آورده است سابقه نداشته است و به نوعی طراحی این نوع سلاح سایبری در واقع زنگ هشدار برای آغاز یک جنگ سایبری است.

رستمی: تمام مسایلی که دوستان گفتند به نوعی صحیح است، اما طبق گزارش‌هایی که ما از بیت دیفندر دریافت کردیم، فلیم توسعه یافته بدافزاری است که در سال ۲۰۰۵ تولید شده بود و البته بدافزار سال ۲۰۰۵ صرفا با مقاصد جاسوسی طراحی شده بود که مساله انجام فعالیت‌های تخریبی در فلیم گنجانده شده است و به نوعی ابزار جدیدی را با خود به همراه داشت.

طوری که در رسانه‌ها منتشر شد، بیشترین هجوم مربوط به رایانه‌های شرکت نفت بوده است، چه اتفاقاتی بعد از این حمله صورت گرفت؟

رستمی: تا آنجایی که ما می دانیم، بعد از این حمله تمامی شبکه و سیستم‌های رایانه‌ای قطع شدند و دستورالعملی برای راه‌اندازی شبکه اینترنت خارج از شبکه سازمانی به واحدهای زیر مجموعه ابلاغ شده است که به این ترتیب هر سازمانی باید دو شبکه مستقل برای خود داشته باشد که یکی مربوط به امور داخلی سازمان است و دومی مربوط به استفاده از اینترنت و این دو شبکه به هیچ عنوان نباید به یکدیگر ارتباط داشته باشند. البته با ذکر این نکته که انجام این پروژه طرح جدیدی نیست و سال ۸۴ و ۸۵ نیز دستورالعمل مشابهی نه تنها در وزارت نفت بلکه در سایر نهادها نیز ابلاغ شد اما از همان زمان هم کارشناسان و مشاوران انجام چنین را تایید نکردند. چرا که به زعم آنها انجام چنین پروژه‌ای راه حل مناسبی برای حل مشکلات ایجاد شده نیست. چرا که برای ارتقای امنیت در سازمان باید که ابتدا تعریف امنیت پیاده سازی شود و اگر تعریف امنیت در سازمان به درستی صورت نپذیرد قطعا در بخشی از سازمان این دو شبکه به هم متصل خواهند شد که همین اتصال کوتاه و یا کوچک کل فرآیند را به محل اولیه خود باز می گرداند. اما این دستورالعمل مجددا به صورت جدی‌تری ابلاغ شده و در حال پیگیری برای پیاده‌سازی آن است. حتی تا جایی که بنده می دانم ورود حافظه فلش نیز به سازمان‌های تابعه وزارت نفت تنها بعد از بررسی آن از لحاظ وجود ویروس و پاکسازی آن میسر است.

بقایی: اگر بخواهیم واکنش‌ها را از نگاهی دیگر بررسی کنیم می‌بینیم که در همان ایام بروز بحران رفت و آمد به مراکز و بخش‌های رایانه‌ای بسیار محدود شد تا جایی که حتی افراد کمی بودند که توانستند از نزدیک مشکل به وجود آمده را ببینند و این مساله مهم بود. به نظرم چرا که تا مدت زمان زیادی حتی نمونه‌ای از سیستم آلوده نیز در اختیار کسی قرار نگرفت. چرا که بالاخره هر یک از سازمان‌های تابعه وزارت نفت مدت‌های زیادی بود که با شرکت‌های ارایه دهنده خدمات و محصولات امنیت در حال همکاری بودند. در نتیجه بهتر بود که نمونه فایل‌های آلوده در اختیار شرکت‌ها قرار می گرفت. در همان زمان اسفند ماه ۹۰ که نخستین اتفاقات رخ داد نیز ما با تمام مشتریان خود تماس گرفتیم و از آنها خواستیم که از اطلاعات خود نسخه پشتیبان تهیه کنند تا در صورت آلوده بودن به بدافزار اتفاق جدی برای آنها نیفتد. حتی در فاصله اسفند ماه تا اردیبهشت ماه هم به بسیاری از مشتریان خود گفتیم که می توانیم از کسپرسکی متخصصانی را به ایران بیاوریم تا به بررسی مساله بپردازند، حتی قرار شد که هماهنگی‌هایی با وزارت خارجه نیز صورت بگیرد اما متاسفانه هیچ پیگیری بعدی صورت نگرفت. چه خوب بود که در همان اسفند ماه ۹۰ مساله جدی گرفته می شد تا شاهد این اتفاق در اردیبهشت ماه نباشیم.

اخلاقی: در تکمیل این حرف‌ها باید اضافه کنم که حتی تا اوایل خردادماه هم هیچ گونه اطلاعات مناسبی در خوری منتشر نشد.

رستمی: اگر بخواهیم از نگاه کلان‌تری به مساله نگاه کنیم باید بگوییم که ما در مملکت یک بیماری داریم به نام بیماری امنیت. فارغ از اینکه بدافزاری وجود دارد یا خیر و اینکه چه کسی می خواهد در مقابل این بدافزار از خود دفاع کند یا خیر به نظر من باید مشکل را در ابعادی بزرگ‌تر بررسی کرد و آن مشکل فرآیند امنیت است و اینکه متولی صاحب صلاحیتی در این زمینه نداریم. البته تشکیل مرکز ماهر برای رسیدگی به این فرآیند حرکت خوبی است اما به راستی ماهر برای پیاده‌سازی این مساله تابه حال چه حرکت جدی کرده است؟ به نظر اگر این اتفاق در سازمان‌های ما بیفتد بسیاری از مسایل حل می‌شود و متوجه می‌شوند زمانی که مجددا چنین اتفاقاتی رخ داد باید به شرکت‌هایی که در این حوزه فعالیت می کنند اعتماد کرد، به آنها فضا داد و از کمک آنها استفاده کرد.

اخلاقی: من هم با این مساله موافقم، اعتماد به شرکت‌های فعال در حوزه امنیت سایبر بسیار مهم است.

رستمی: ما حتی برای دریافت نمونه‌های آلوده بسیار تلاش کردیم، به هر صورت باید این نمونه‌ها توسط افراد متخصصی تست می‌شدند. کما اینکه شاید همین نمونه‌های آلوده هم دارای نسخه‌های متفاوتی باشند.

بقایی: اما به این موضوع می توان نگاه دیگری هم داشت و آن اینکه ماجرای فلیم به نظر من باعث شد که مرکز ماهر از یک توانایی بالقوه به یک توانایی بالفعل برسد. به طور مثال تا قبل از این ماجرا چیزی که از ماهر دریافت می کردیم تنها گزارش‌هایی مبنی بر وجود آلودگی‌هایی بود و انصافا هم وب سایت ماهر تابه حال مقالات و گزارش‌های خوبی را منتشر کرده است. اما موضوع فلیم به طور خاص باعث شد که ماهر به صورت عملیاتی وارد شود و اتفاقا دولت و وزارت نفت هم به این مرکز اطمینان کردند.

در بین مشتریانی که شما دارید به خصوص بعد از ماجرای

رستمی: در سازمان‌های زیادی می بینیم که وظایف امنیت سایبری با وظایف حراست تداخل دارد

فلیم آیا باعث شد که هیچ کدام از سازمان‌ها فردی را به عنوان مدیر امنیت اطلاعات به کار گیرند یا بخشی را با این عنوان ایجاد کنند؟

رستمی: معمولا در سازمان‌هایی که مشتری ما هستند یک فردی هست که متولی امنیت است و بعد از این ماجرا نیز کماکان همان افراد هستند اما در سازمان‌های زیادی می بینیم که وظایف امنیت سایبری به خوبی تفکیک نشده‌اند و با وظایف حراست سازمان‌ها تداخل دارد. متاسفانه بعد از ماجرای فلیم، این تداخل بیشتر هم شده است.

اگر بخواهیم تا اینجا یک جمع بندی انجام دهیم باید بگوییم که یک نظام مدیریت امنیت اطلاعات و پیاده سازی استاندارد ISMS می توانست در تدوین سناریوی بحران به سازمان‌ها کمک کند تا بتوانند در چنین مواقعی باید چه بکنند؟

اخلاقی: در تایید این سخنان باید بگویم که در واقع ما نه در بخش پیشگیری و نه در بخش مدیریت بحران هیچ نظام تعریف شده‌ای نداریم و غالبا در موقع برخورد با مشکلات به صورت بداهه آن را مدیریت می کنیم. اما نکته مهمی که باید بیشتر به آن پرداخت مساله تفکیک اینترنت از شبکه داخلی است که به نظر من تنها نکته‌ای که دارد این است که حمله سایبری بعدی به کشور به مراتب مخرب‌تر خواهد بود. چرا که یک اعتماد کاذبی به وجود می آورد و دیگر اینکه بدافزاری که در آن صورت به شبکه حمله خواهد کرد قطعا هدف تخریبی دنبال خواهد کرد و به جمع آوری اطلاعات بسنده نخواهد کرد.

اشکال به صورت کلی اینجاست که زمانی که ما راهکاری را پیشنهاد می کنیم راهکاری بدون توجه به نتیجه است.

البته تفکیک شبکه‌ها از اوایل دهه ۸۰ در برخی وزارتخانه‌ها صورت گرفته است.

رستمی: البته ضمن تایید صحبت‌های آقای اخلاقی اضافه کنم که بنده هم تابه حال هیچ سند و گزارشی ندیدم که حتی در مکان‌هایی با درجه اهمیت امنیتی بالا نیز چنین پروژه‌هایی پیاده شده باشد.

اخلاقی: اما باید اضافه کنم در خارج از ایران تفکیک شبکه وجود دارد ولی در مراکز بسیار خاص این امر اتفاق افتاده است.

رستمی: اگر چه همان طور که شما اشاره کردید در مراکزی با ویژگی‌های بسیار خاص چنین اتفاقی افتاده است نه اینکه یک نسخه ثابت برای تمامی سازمان‌ها و نهادها بپیچیم که همه باید شبکه خود را تفکیک کنند.

اخلاقی: نکته جالب اینکه در مکان‌هایی هم که این تفکیک شبکه صورت گرفته است دستورالعمل دسترسی و کار با شبکه‌ای که به اینترنت متصل نیست بسیار مفصل تر و جدی تر از شبکه‌ای است که به اینترنت متصل است.

در تکمیل این گفته‌ها هم به یک مثال نقض خیلی مناسب می توان اشاره کرد و آن هم استاکس نت است. استاکس نت بدافزاری بود که انتقال از طریق اینترنت منتقل نشد و همین مساله ثابت می کند که انتقال بدافزار ها به هر صورت از طریق شبکه انجام می گیرد چه این شبکه به اینترنت متصل باشد و چه اینکه متصل نباشد. حالا آیا درست است که همه ما مسولیت چنین اتفاقی را به حساب نرم‌افزارهای ضد بدافزار بگذاریم و فعالیت‌های آنان را زیر سوال ببریم؟ بقایی: در قدم اول باید بگویم که تمامی شرکت‌های ضد بدافزار نخستین کاری که انجام می دهند این است در توافق نامه اولیه استفاده از نرم افزار که معمولا هم کمتر کسی آن را می خواند اعلام کنند که اگر اتفاقی بیفتد و به موجب آن اطلاعات شما سرقت شود یا اینکه تخریب شود، با اینکه ما تا حد ممکن سعی می کنیم جلوی بروز آن را بگیریم ولی در عین حال تعهدی متوجه ما نیست. لذا ضد بدافزار به هیچ عنوان ضمانتی نمی دهد که شما هیچ گاه دچار مشکلی نمی شوید بلکه ابزاری است برای اینکه میزان آلودگی‌های شما را به حداقل برساند. لذا ضد بدافزار هم همه چیز نیست به طور مثال هیچ ضد بدافزاری نسبت به حفره‌های امنیتی سیستم عامل هم تعهدی ندارد.

اخلاقی: باید گفت که ضد بدافزار یک سامانه ری

اخلاقی: ما نه در بخش پیشگیری و نه در بخش مدیریت بحران هیچ نظام تعریف شده‌ای نداریم و غالبا بداهه رفتار می کنیم

اکتیو (واکنشی) است به عبارتی حتما باید چیزی پیدا شود و بعد شرکت صاحب برند ضد ویروس آن را تحلیل کند و ابزار پاک سازی و جلوگیری از گسترش آن را بسازد و در نهایت در قالب به روزرسانی این ابزار به نرم افزار ضد بدافزار افزوده می شود.

لذا برای ارتقای امنیت باید به مساله پروآکتیو (پیشگیرانه) توجه کرد. حال ممکن است صاحب برند ضد بدافزار همراه نرم افزار یا در خود نرم افزار چنین ابزارهایی را هم به شما ارایه کند. البته هیچ کدام از اینها نمی تواند جایگزین نظام مدیریت امنیت اطلاعات شود. چرا که هر کدام از اینها بخشی از این نظام هستند.

رستمی: باید به این نکته توجه کرد که در واقع ضد بدافزار جزیی از همین نظام فراگیر مدیریت امنیت اطلاعات است و همه این نظام نیست. به عنوان یکی از این اجزا در محل خودش وظیفه مربوطه را انجام می دهد و باید گفت که اگر هر جز از این نظام ناقص باشد طبیعتا سامانه دچار مشکل خواهد شد.

اخلاقی: نگاه در واقع به این ترتیب است که چون یک بدافزاری موجب مشکل شده است پس ضد بدافزار مقصر اصلی ماجراست.

رستمی: در واقع باید گفت که زمانی که ما هنوز در بسیاری از سازمان‌ها تعریف رفتار سازمانی به درستی لحاظ نشده است لذا نمی توان از ضد بدافزار انتظار معجزه داشت و باز هم اشاره می کنم که باید به فرآیند پیاده‌سازی نظام مدیریت امنیت اطلاعات به صورت کلی توجه کرد.

بقایی: اگر بتوانیم استانداردهای ISMS اجرایی کنیم آمادگی لازم را کسب خواهیم کرد. اما متاسفانه تا حادثه بعدی دچار فراموشی می شویم

رمضانی نیا: یکی از مسایلی که باید به آن توجه کرد کمبود دانش فنی افراد و کارکنان سازمان‌ها و حتی بخش‌های حراستی است به طور مثال حتی در یکی از سازمان‌های کشور که بحث تفکیک شبکه داخلی از شبکه اینترنت نیز در آن صورت گرفته و نرم افزار ضد بدافزار نیز مورد استفاده قرار می گیرد بسیاری از موارد امنیتی رعایت نمی شود. در نتیجه با وجود نرم افزار و سخت افزار امنیتی مناسب، همچنان مشکلات امنیتی با بر جاست.

در یک جمله داشتن انواع ابزارها بدون داشتن دانش فنی نمی تواند کمک مهمی به ارتقای سطح امنیت سازمان کند.

اخلاقی: البته یک مخالفت کوچکی با این نتیجه گیری داشته باشیم که با افزایش ابزارها می توانیم امنیت را افزایش دهیم ولی مساله مهم اینکه نباید این مورد باعث شود که خیال مان راحت باشد و به عبارتی نباید باعث بی تفاوتی ما شود.

رمضانی نیا: در واقع اینگونه بیان می کنم که اگر ماراندگی بلد باشیم تفاوتی نمی کند که چه ماشینی داریم، این ماشین قدیمی است یا یک ماشین لوکس و مهم سواد ما در خصوص چگونگی رانندگی و تجربه و مهارت رانندگی است و امکانات ماشین در اولویت بعدی رانندگی است.

یک سوال مهم هنوز باقی است. استاکس نت آمد و موجی از لزوم توجه به امنیت در سازمان ایجاد کرد. هم اکنون موج دومی به نام فلیم ایجاد شده است که باز هم ممکن است به بالا رفتن سطح امنیت کمک کند. اما آیا به نظر شما ما برای فلیم بعدی آماده ایم؟

بقایی: باید گفت که حتی گفتن اینکه آماده هستیم یا نه زمانبر است، و باز هم تاکید می کنم که مساله مهم این است که ما باید امنیت را به عنوان یک فرآیند ببینیم و نگاه سیستمی به مساله امنیت داشته باشیم. ما اگر بتوانیم استانداردهای مدیریت امنیت را اجرایی کنیم عملا آمادگی لازم را کسب خواهیم کرد. به نظر می رسد که اقداماتی هم در این راستا انجام شده است و حداقل اینکه گام‌هایی در خصوص پیاده سازی ISMS برداشته شده است. اما متاسفانه ما معمولا دچار فراموشی می شویم و تا بروز حادثه بعدی اقدام خاصی را انجام نمی دهیم.

اخلاقی: از این بابت که در خصوص فلیم بعدی آمادگی چندانی وجود ندارد و باید گفت بله واقعا آمادگی وجود ندارد و همچنین باید تاکید کنم که فلیم بعدی به مراتب مخرب تر است.

چرا فکر می کنید فلیم بعدی مخرب تر است؟

اخلاقی: چرا که الآن به فلیم می گوییم سلاح سایبری، چرا اسم سلاح را روی آن گذاشتیم؟ چون یک دولت آن را تهیه کرده است و طبیعتا دولت متخاصم تمام تلاش خود را برای اینکه این سلاح بتواند ضربه قوی تری به مقاصد مورد نظر وارد کند خواهد کرد و حتی این پروژه تفکیک سازی اینترنت از اینترانت تسریع کننده این جریان خواهد بود به نحوی که حتی حمله بعدی آن چنان صدماتی به بار آورد که دیگر هیچ چیز قابل جبران نخواهد بود.

رمضانی نیا: حداقل اینکه در حال حاضر الان فرهنگ خرید ضد بدافزار تقریبا جا افتاده است باز هم جای خوشحالی است اما اینکه باز هم استفاده از ابزارهای نامناسب و استفاده از سیستم عامل‌های کرک شده هنوز باب است قطعا موجب نگرانی می شود.

بقایی: می خواهم تاکید کنم که اگر همین فلیم منجر به اخذ تصمیمات امنیتی جدی تری شود هم خوب خواهد بود.

اخلاقی: اما چون هنوز مشکلات زیرساختی داریم بهتر است به آن توجه کنیم که در صورت بروز حمله مجدد بتوانیم جلوی آنرا بگیریم.

رمضانی نیا: اگر شرکت‌ها به سمت تخصصی تر شدن بروند و راهکار محورتر بشوند، می توانند بسیاری از این قبیل مشکلات را حل کنند.

اخلاقی: مساله مهمی که به نظرم باید به آن پرداخت ایجاد یک مرکز CERT با حضور نمایندگان بخش خصوصی است به عبارتی ایجاد نهادی با حضور نمایندگان همه شرکت‌های فعال در بخش خصوصی است منجر به هماهنگی‌های بیشتری دست یابند و راهکارهای جامع‌تری را برای مدیریت صحیح بحران‌ها و پیاده سازی نظام مدیریت امنیت اطلاعات ارایه کنند.