ویروس فلیم

1- فلیم چگونه کشف شد؟

ظاهرا شرکت نرم افزاری کسپراسکی در روسیه کاشف فلیم بوده است. ویتالی کاملیوک، کارشناس ارشد بدافزار در شرکت نرم افزارهای امنیتی کاسپرسکی کاشف فلیم است.

وی به عنوان عضوی در یک گروه کارشناسی به دنبال کد بدافزاری رایانه ای بود که گفته می شد اطلاعات رایانه های داخل ایران را از بین برده بود.

2- ویژگی های فلیم چیست؟

2-1- کد فلیم از ویروس استاکس نت خیلی بزرگتر است. کد فلیم 20 مگابایت حجم دارد در حالی که کد استاکس نت فقط 500 کیلو بایت بود. بنابراین، فلیم بزرگترین بدافزاری است که تا کنون مشاهده شده است.

2-2- زبان برنامه نویسی استفاده شده برای نوشتن این بدافزار لوا نام دارد که تا کنون در هیچ بدافزاری استفاده نشده بود. شرکت کسپراسکی می گوید از این زبان برنامه نویسی بیشتر در نوشتن بازی های رایانه ای استفاده می شود زیرا می توان دائما کدهای جدید به آن اضافه کرد و آن را ارتقا داد. استفاده از زبان برنامه نویسی لوا نشان می دهد طراح این ویروس در نظر دارد این ویروس را دائما رشد داده و تقویت کند.

2-3- فلیم از مارس 2010 فعال بوده است.

3- فلیم چگونه عمل می کند؟

3-1- بر خلاف استاکس نت فقط برای جاسوسی و جمع آوری اطلاعات طراحی شده است. این ویروس تواناییهایی بیش از این دارد. این ویروس از صفحه نمایشگر رایانه عکس می گیرد

و میکروفون رایانه را روشن می کند تا مکالمات محیط ضبط شود. بعدا اطلاعات گردآوری شده به منبع منتشر کننده ویروس منتقل می شود.

3-2- تیم مارر و دیوید وینستاین، روز 10 خرداد در فارین پالیسی نوشتند: «بنا بر اعلام کاسپرسکی بدافزارهای دیگری هم وجود دارند که می توانند صدا را ضبط کنند اما نکته اصلی در مورد فلیم کامل بودن آن است، یعنی توانایی آن برای به سرقت بردن اطلاعات از شیوه های بسیار متنوع».

3-3- مارک کلایتون روز 10 خرداد درباره شیوه عمل فلیم در کریستین ساینس مانیتور نوشته است: «کارشناسان می گویند به علت بزرگی و پیچیدگی ویروس فلیم کشف کامل برنامه آن و این که چه کارهایی انجام داده است سال ها زمان می برد. با این حال، از یافته هایی که تاکنون بدست آمده مشخص شده است که ویروس فلیم می تواند از طریق یو اس بی، بلوتوث یا دیگر ابزارها در یک شبکه گسترش پیدا کند. در دستگاه های آلوده، این ویروس می تواند برای اجرا شدن منتظر نرم افزارهای خاصی شود و سپس به تصاویر دست یابد، میکروفون های داخلی را برای ضبط مکالمات روشن کرده و ئی میل ها و چت ها را رهگیری کند. این ویروس می تواند اطلاعات بدست آمده را بسته بندی و رمزگذاری کرده و آنها را برای رایانه های مشخصی در سراسر جهان بفرستد».

3-4- به زبان فنی می توان گفت ویروس فلیم مانند یک «کرم» عمل می کند به این صورت که بدون نیاز به دخالت انسان گسترش می یابد و برای رساندن اطلاعات ربوده شده به دست گردانندگانش کانال هایی را برای خود باز می کند.

4- چه کسی فلیم را ساخته است؟

4-1- شرکت کاسپرسکی عقیده دارد این ویروس با توجه به پیچیدگی و مکان جغرافیایی رایانه های آلوده احتمال ساخته یک ملت-دولت است و نه یک شرکت و موسسه خصوصی یا گروهی از هکرها.

4-2- موشه یعلون، معاون رئیس کابینه اسرائیل و وزیر امور راهبردی اسرائیل روز سه شنبه 8 خرداد تقریبا به صراحت تایید می کند که اسراییل این ویروس را ساخته است. وی به رادیو نظامی اسرائیل گفته است: «به نظر منطقی می آید که فرض کنیم هرکس که تهدید ایران را

تهدیدی جدی تلقی می‌کند، تدابیر مختلف، که شامل اینها (حملات سایبری با ویروس فلیم) می‌شود را برای صدمه زدن به آن (ایران) اتخاذ خواهد کرد. اسرائیل از این نعمت برخوردار بوده که دارای فناوری پیشرفته (رایانه ای) بوده است. این ابزار (فناوری پیشرفته) که ما (اسرائیل) به آن افتخار می کنیم باب انواع فرصت ها را بر روی ما می گشاید.

3-4- مارک کلایتون روز 10 خرداد در کریستین ساینس مانیتور می نویسد: «کارشناسان شرکت کاسپراسکای معتقدند به احتمال زیاد یک کشور این ویروس را ساخته است. آنها معتقدند این ویروس نه نتها بسیار پیچیده است بلکه کار اصلی آن جاسوسی اطلاعات است. یکی از شرکای اتحادیه بین المللی مخابرات نیز که در این تحقیقات همکاری می کند با این ارزیابی موافق است. شرکت کرایسیس لب CrySyS Lab))مستقر در دانشگاه فن آوری و اقتصاد در بوداپست مجارستان گزارشی از بررسی های خود از ویروس فلیم منتشر کرد. در گزارش این شرکت آمده است: «نتایج بررسی های فنی ما این فرضیه را تایید می کند که سرویس دولتی یک کشور با بودجه و تلاش قابل توجهی این ویروس را ساخته است».