بدافزار Flame (آتش)

این بدافزار که به عنوان sKyWIper نیز شناخته می‌شود قطعه پیچیده‌ای از یک بدافزار کامپیوتر است که رایانه‌های با سیستم‌عامل ویندوز را مورد حمله قرار می‌دهد. این بدافزار از سال ۲۰۰۶ شروع به فعالیت کرده‌است. و برای جاسوسی اینترنتی و تخریب اطلاعات مهم در کشورهای خاورمیانه و اروپای شرقی استفاده می‌شود .

این بدافزار در واقع پلتفرمی است که قابلیت دریافت و نصب ابزارهای گوناگون جهت فعالیت های مختلف را داراست. در صورتیکه هیچ کدام از اجزای پرشمار تشکیل دهنده این بدافزار توسط نرم افزار آنتی ویروس در دسترس شما مورد شناسایی قرار نگیرند. می توانید ابزار شناسایی و پاکسازی این بدافزار را که در مرکز ماهر تهیه شده را از کارشناسان شرکت سپکو تهیه نمایید.

این بد افزار مانند سلاح سایبری که قبلاً شناخته شده بود یعنی استاکس نت و دوکو، این بدافزار بصورت هدفمند ساخته شده و می‌تواند از طریق قابلیت روت کیت‌ها از نرم افزارهای امنیتی فعلی فرار کند. هنگامی که یک سیستم آلوده می‌شود، بدافزار فلیم می‌تواند بروی شبکه محلی یا از طریق فلش دیسک به سیستم های دیگر پخش شود و می‌تواند صدا، نماگرفت و یا فعالیت های کی‌برد و ترافیک شبکه را ضبط کند. برنامه همچنین مکالمات اسکایپ را ضبط می‌کند و می‌تواند سیستم آلوده را به Bluetooth beacons تبدیل کند که تلاش می‌کند اطلاعات تماس را از بلوتوث

اطراف جمع‌آوری کند. این داده‌ها همراه به اسناد محلی به سرور فرماندهی و کنترل ارسال می‌شود.

برخلاف استاکس نت که برای آسیب رساندن به یک فرایند صنعتی طراحی شده بود فلیم به نظر می‌رسد که صرفاً برای مقاصد جاسوسی نوشته شده است. به نظر نمی‌رسد که برای یک صنعت خاص را هدف قرار داده باشد بلکه یک ابزار حمله کامل است که برای اهداف سایبری و جاسوسی عمومی طراحی شده‌است.

فلیم هیچ تاریخ پایان عمر را بصورت توکار ندارد تا آن را غیرفعال کند، اما اپراتورها می‌توانند یک ماژول kill ارسال کنند که همه رده پاهای فایل‌ها فلیم را از سیستم پاک کند.