متخصصان کسپرسکی شناسایی کردند " رد پای شعله و گاس در بدافزار **MiniFlame** "

بنابر اعلام کارشناسان، یکی از سه بدافزاری که طی کاوش سرورهای کنترل و فرماندهی ویروس شعله شناسایی شد، به عنوان ابزار مراقبتی ثانویه علیه برخی اهداف خاص مورد استفاده قرار می‌گرفت.

به گزارش روابط عمومی شرکت پاد، در ابتدا گمان می‌شد بدافزار MiniFlame که به SPE هم شناخته می‌شود یکی از ماژول‌های ویروس شعله است، اما متخصصان مرکز تحقیقاتی کسپرسکی‌لب دریافتند که MiniFlame یک بدافزار مستقل است و در قالب plug-in دو ویروس شعله و گاس (Gauss) عمل می‌کند.

بر اساس این گزارش گاس یکی دیگر از حملات خرابکارانه‌ای است که از حمایت مالی دولتی برخوردار است و هدف آن سرقت اطلاعات بانکی آنلاین است.

الکساندر گوستف، متخصص امنیت ارشد کسپرسکی می گوید: «شعله بعد از جمع‌آوری و مرور داده‌ها قربانی مورد نظرش را تعریف و شناسایی می‌کند و سپس MiniFlame برای نظارت بیشتر روی هدف و اجرای عملیات خرابکاری سایبری نصب و اجرا می‌شود.»

به گفته گوستف، تیم تحقیقاتی او موفق به شناسایی نحوه عملکرد و ارتباط میان بدافزارهای استاکس نت، شعله، گاس و Duqu شده است.

«شعله کوچک» حدود 10 تا 20 حمله سایبری موفق داشته است. این درحالیست که شعله حدود 700 بار و گاس حدود 2 هزار و 500 بار کامپیوترها و شبکه های گوناگون را هدف قرار داده است. گفتنی است MiniFlame در مقایسه با دو بدافزار دیگر محدوده جغرافیایی متفاوتی را هدف اصلی خود قرار داده است. تاکنون 6 نسخه از MiniFlame شناسایی شده که بیشترین قربانیان این ویروس به لبنان بر می‌گردد. این درحالیست که ایران، سودان و سوریه اهداف اصلی شعله محسوب می‌شدند.

کسپرسکی همچنین در بیانیه‌ای در وبلاگ خود اعلام کرد: «نتایج تحقیقات نشان می‌دهد MiniFlame ابزاری برای حمله به هدف‌های خاص و درجه یک است و تاکنون علیه اهدافی به کار برده شده که بیشترین اهمیت و حساسیت را نزد مهاجمان دارا بوده‌اند.»

به گفته متخصصان کسپرسکی، هکرها از طریق MiniFlame می‌توانند به تمام فایل‌های سیستم‌های کامپیوتری آلوده دسترسی پیدا کنند و یا هنگام اجرای مرورگر اینترنتی، برنامه‌های آفیس، آدوبی ریدر، مسنجر یا کلاینت FTP روی کامپیوترهای قربانی، از صفحات و پوشه‌های مختلف اسکرین شات بگیرند. این بدافزار سپس اطلاعات مسروقه را به یکی از سرورهای کنترل و فرماندهی اختصاصی خود یا یکی از سرورهای شعله ارسال می‌کند. MiniFlame همچنین قادر است از طریق ماژول دیگری که درایوهای USB را هدف قرار می‌دهد به سیستم‌های کامپیوتری نفوذ کرده و اطلاعات سیستم آفلاین را به سرقت ببرد.

در قسمتی از بیانیه کسپرسکی آمده است: «اگر شعله و گاس را عملیات جاسوسی بزرگی بدانیم که سیستم هزاران را نفر را آلوده کرده است، شعله کوچک به ابزار تهاجمی ظریف و دقیقی شباهت دارد.»

ساختار MiniFlame مشابه شعله است. این بدافزار علاوه بر سرقت اطلاعات، دسترسی مستقیم به سیستم های آلوده را برای مهاجمان فراهم می‌کند. محققان بر این باورند که توسعه SPE سال 2007 آغاز شد و تا امسال ادامه داشته است. کسپرسکی تاکنون موفق شده است چند دامنه کنترل فرمان بدافزارهای شعله و MiniFlame را شناسایی کند. بر این اساس از ماه مه تا پایان سپتامبر گذشته متخصصان امنیت کسپرسکی

نزدیک به 14 هزار اتصال از 90 آدرس IP مختلف را به این دامنه‌ها ردیابی کردند که عمدتا به سرورهایی در لبنان ختم می‌شد، درحالی که رد پای MiniFlame در ایران، فرانسه و آمریکا هم دیده شده است.

متخصصان 10 فرمان قابل فهم برای این بدافزار را شناسایی کرده‌اند که ثبت و ارسال فایل ها از بدافزار به سرور کنترل و فرمان و بالعکس، تهیه اسکرین شات از مراحل نفوذ پیش فرض و غیر فعال شدن برای دوره‌های مشخص و از پیش برنامه‌ریزی شده از جمله آنهاست.

کاوش اولیه مرکز کنترل و فرمان ویروس شعله که به شناسایی MiniFlame منجر شد به سپتامبر گذشته بر می‌گردد. محققان کسپرسکی، سیمانتک، CERT-Bund/BSI و اتحادیه جهانی مخابرات علاوه بر شناسایی شعله، در کنار هم 3 بدافزار جدید و 4 پروتکل ارتباطی یعنی OldProtocol، OldProtocolE، SignupProtocol و RedProtocol را شناسایی کردند. MiniFlame از طریق این پروتکل‌ها به مرکز کنترل و فرماندهی متصل می‌شده است.

کشف ویروس SPE درحالیست که دو بدافزار دیگر با عنوان SP و IP هنوز ناشناخته مانده است. کارشناسان احتمال می‌دهند که SP به احتمال فراوان یک نسخه قدیمی از MiniFlame است، اما هویت بدافزار IP هنوز نامشخص است. بین سه بدافزار نامبرده IP از همه جدیدتر است. ارزیابی سرورهای کنترل و فرماندهی در ماه سپتامبر نشان داد که دست کم چهار برنامه نویس با سطوح مهارتی گوناگون پشت حملات این بدافزارها بوده‌اند. همچنین مشخص شد که در ارسال اطلاعات کامپیوترهای آلوده به سرورها شیوه‌های پیشرفته و پیچیده‌ای برای رمز نگاری داده‌ها به کار رفته است.

در گزارش کسپرسکی از شعله کوچک آمده است: «با شناسایی شعله، گاس و MiniFlame احتمالا فقط از سطح یک عملیات جاسوسی-سایبری بزرگ در خاورمیانه پرده برداشته‌ایم. اهداف اصلی این حملات همچنان نامعلوم است و از هویت قربانیان و مهاجمان اطلاعاتی در دست نیست.»