مصونیت از حمله‌های آتی در باج‌افزار اسپورا

باج‌افزار اسپورا به‌منظور مصونیت قربانی در حمله‌های آینده، گزینه پرداخت پول بیشتر را ارائه می‌دهد.

به گزارش واحد متخصصین سایبربان، محققان امنیتی باج‌افزار اسپورا (Spora) را شناسایی کردند که با دریافت پول از قربانی اطمینان می‌دهد که دوباره سامانه او را آلوده نسازد.

بر اساس گزارش محققان امنیتی، کدهای این باج‌افزار حرفه‌ای نوشته شده‌اند و یک وب‌گاه مخصوص پرداخت قربانی طراحی شده است. در این وب‌گاه گزینه‌های مختلفی به قربانی نمایش داده می‌شود که می‌توان به بازیابی فایل‌های رمزشده، پاک‌سازی باج‌افزار و پرداخت پول به‌منظور مصونیت از حمله‌های آینده، اشاره کرد. میزان پول پرداختی کاربران یکسان است و تفاوت هزینه وجود ندارد.

نحوه گسترش این بدافزار توسط ایمیل است که یک صورت‌حساب جعلی در قسمت وصله ایمیل قرار داده شده است. این وصله یک فایل فشرده با فرمت zipاست که در آن فایل HTA یا HTML App وجود دارد که در ظاهر شبیه فایل پی.دی.اف یا مایکروسافت آفیس است. هنگامی‌که این فایل اجرا شود، فایلJscript در فولدر ٪TEMP٪ قرار می‌گیرد. این فایل، اسکریپت رمز شده‌ای را نوشته و آن را اجرا می‌کند.

هنگامی‌که باج‌افزار اجرا می‌شود، فایل‌های موجود در سامانه قربانی و شبکه اشتراکی را رمز می‌کند؛ البته این باج‌افزار فایل‌های اصلی سامانه قربانی را رمز نمی‌کند تا سیستم‌عامل قربانی از کار نیفتد. اسپورا از CryptoAPI به‌منظور رمزنگاری استفاده می‌کند و با استانداردهای RSA و AES، فایل‌ها را رمز می‌کند. کلید رمزنگاری تقریبا قوی است که ابتدا کلید عمومی و خصوصی RSA با ۱۰۲۴ بیت طول، ایجاد می‌شود؛ سپس کلید خصوصی RSA توسط AES به طول ۲۵۶ بیت رمز می‌شود. هنگامی‌که کلید خصوصی رمز شد، کلید AES نیز توسط کلید عمومی RSA توسعه‌دهندگان باج‌افزار، رمز می‌شود. درنهایت این کلیدها در فایل KEY. ذخیره می‌شود.

یکی از ویژگی‌های اسپورا، عدم استفاده از سرور مدیریت مرکزی (C&C) به‌منظور رمزنگاری فایل‌ها است. با توجه به عدم وجود سرور مدیریت مرکزی، حتی با بررسی کامل یک کاربر و رمزگشایی اطلاعات وی، کاربر دیگر نیازمند شناسایی روش دیگری است.

اداره حراست آموزشکده شهید یزدانپناه سنندج