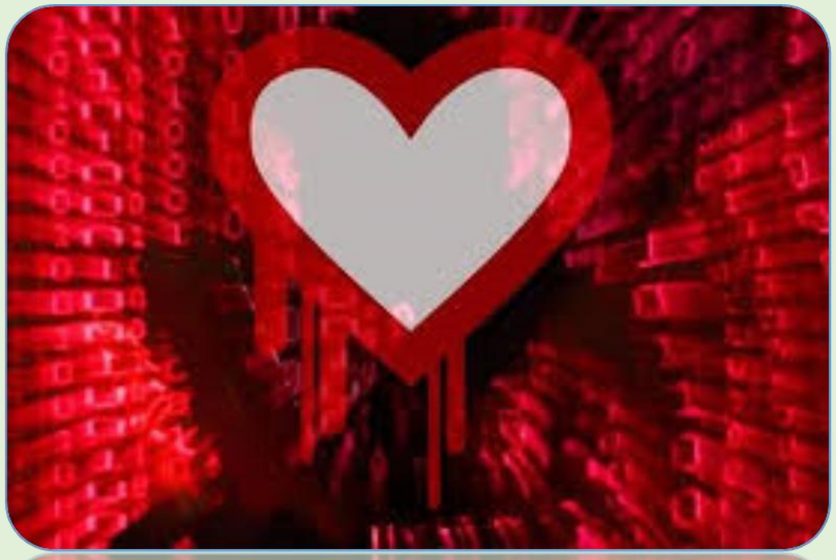


عامل نخستین هک "خونریزی قلبی "

پلیس جرایم سایبری کانادا یک نوجوان ۱۹ ساله اهل آنتاریو را به اتهام هک کردن سازمان مالیات این کشور با سوء استفاده از حفره امنیت اینترنتی خونریزی قلبی دستگیر کرده است .

اتهامات رسمی وارده به این نوجوان "استفاده بدون اجازه از یک رایانه" و "شیطنت در رابطه با داده " است.

این آسیب پذیری و رخنه فراگیر که از ۲۰ فروردین ماه اعلام جهانی شده مربوط به آسیب رسانی نرم‌افزارهای استفاده کننده از نسخه‌های بخصوصی از کتابخانه OpenSSL (یک مجموعه نرم‌افزار و کتابخانه از توابع رمزنگاری است که توسط سیستم‌عامل‌های مختلف مانند گنولینوکس، مایکروسافت ویندوز و مکینتاش مورد استفاده قرار گرفته و برای پیاده‌سازی پروتکل‌های SSL Secure Sockets Layer و TLS Transport Layer Security استفاده می‌شود .) است که امکان استخراج ناخواسته اطلاعات حساس را به حمله‌کننده می‌دهد.

SSL چیست؟

SSL یک پروتکل رمزنگاری است که برای برقراری یک ارتباطات امن بین یک سرویس دهنده و یک سرویس گیرنده طراحی شده است . در اینترنت بسیاری از وب سایت‌ها از این پروتکل و البته جایگزین آن یعنی پروتکل TLS برای دریافت داده‌های حساس کاربر مانند، کلمه عبور، اطلاعات بانکی کاربر استفاده می‌کنند. استفاده از این پروتکل‌ها تضمین دهنده‌ی این است که یک نفوذگر نباید بتواند اطلاعات رمز شده را در طول مسیر رمزگشایی کند . SSL یک پروتکل قدیمی می‌باشد نسخه‌ی سوم آن مربوط به ۱۵ سال پیش می‌باشد اما همچنان در مرورگرها از آن پشتیبانی می‌شود..

TLS چیست؟

مخفف واژه Transfer Layer Security می باشد که یک پروتکل برای برقراری و ایجاد یک ارتباط امن بین کلاینت و سرور می باشد . این پروتکل توانایی تشخیص هویت و برقراری یک ارتباط رمزنگاری شده بین کلاینت وسرور را دارد . منظور از تشخیص هویت هم کلاینت و هم سرور این است که هر دو آنها برای این که هویت یکدیگر را اثبات کنند بایستی به یکدیگر یک سری اطلاعات بدهند و این اطلاعات به صورت رمزنگاری شده منتقل می شوند تا در بین مسیر اگر شخصی شنود کرد قادر به استفاده از اطلاعات نباشد . این پروتکل را می توان جایگزین مناسبی برای SSL در آینده ای نه چندان دور دانست .

چرا سرقت اطلاعات،خونریزی قلبی نام گرفت؟

اینکه چرا این مشکل خونریزی قلبی یا Heartbeat نام گرفت، به این موضوع برمی گردد که این باگ یا رخنه امنیتی با استفاده از بارگذاری بر ضمائم SSL بسیاری از اطلاعات را تحت کنترل می گیرد .

فناوران فضای مجازی به این بخش نام ضربان قلب داده اند که از ابزارهای رمزگذاری شده اینترنت است و استفاده آن برای تمامی سایت ها جنبه عمومی دارد بنابراین میزان درگیری این مشکل در میان کاربران خصوصی و عمومی بسیار وسیع است.

خونریزی قلبی چیست و چگونه کار می‌کند؟

این مشکل بخشی از یک نرم‌افزار را با نام OpenSSL تحت تاثیر قرار می‌دهد که به‌عنوان راهکاری برای مسائل امنیتی در وب سرورها مورد استفاده قرار می‌گیرد. با استفاده از OpenSSL وب‌سایت‌ها می‌توانند اطلاعات خود را بصورت رمزنگاری شده در اختیار کاربران قرار دهند ، از این‌رو سایر افراد توانایی دسترسی و استفاده از داده‌های رد و بدل شده را که شامل نام‌های کاربری ، رمزهای عبور و کوکی‌ها است ، ندارند.

OpenSSL یک پروژه متن باز است ، یعنی این پروژه توسط مجموعه‌ای از افراد متخصص توسعه داده شده است که در قبال سرویس توسعه‌داده شده هزینه ای را دریافت نکرده‌اند . هدف این افراد کمک به توسعه‌ی وب و یاری جامعه‌ی اینترنت بوده است.

خونریزی قلبی یکی از ویژگی‌های داخلی OpenSSL را با نام Heartbeat یا ضربان قلب مورد استفاده قرار می‌دهد. زمانی که رایانه‌ی کاربر به یک وب‌سایت دسترسی پیدا می‌کند، وب‌سایت پاسخی را به مرورگر کاربر ارسال می‌کند تا رایانه‌ی کاربر را از فعالیت خود و همچنین قابلیت پاسخ‌گویی به درخواست‌های بعدی آگاه سازد، این رد و بدل شدن اطلاعات را ضربان قلب گویند. ارسال درخواست و پاسخ به آن با رد و بدل شدن داده‌ها همراه است. در حالت نرمال، زمانی که رایانه‌ی کاربر درخواستی را از سرور به عمل می‌آورد، ضربان قلب میزان داده‌ی مجاز درخواست شده از طرف کاربر را ارسال می‌کند، اما در مورد

سرورهایی که این باگ را در ساختار خود دارند، یک هکر قادر است تا درخواستی را مبنی بر گرفتن داده‌ها از حافظه‌ی سرور ارسال کرده و داده‌ای را با حداکثر اندازه‌ی ٦٥,٥٣٦ بایت دریافت کند.

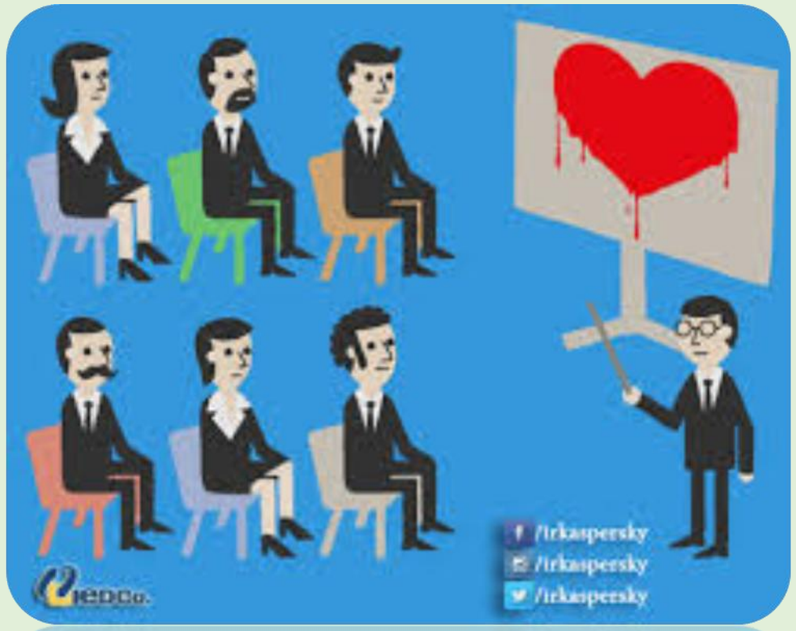
براساس اطلاعات ارائه شده توسط **CloudFlare** ، اطلاعات درخواست شده شاید دربردارنده‌ی اطلاعاتی از سایر بخش‌های **OpenSSL** نیز باشد. اطلاعات موجود در حافظه کاملا از پلتفرم مستقل هستند . با اتصال رایانه‌های بیشتر به سرور اطلاعات موجود در حافظه‌ی از بین رفته و اطلاعات جدید جایگزین می‌شود ، از این‌رو صدور درخواست‌های جدید توسط هکرها منجر به دریافت اطلاعات جدیدتری خواهد شد که شامل اطلاعات ورود، کوکی‌ها و داده‌هایی می‌شود که هکرها می‌توانند از آن‌ها بهره‌برداری نمایند.

حال سوال اصلی در مورد نگرانی یک کاربر معمولی اینترنت مطرح است. آیا کاربران اینترنت باید از وجود چنین مشکلی نگران باشند؟ متاسفانه پاسخ این پرسش بلی است. کاربران باید با استفاده از سرویس‌ه‌ایی چون Heartbleed Test ، LastPass Heartbleed Checker یا Qualys SSL Labs Test وب‌سایت‌های حساسی را که به آن‌ها مراجعه می‌کنند چک کرده و در صورت وجود مشکل، رمز عبور خود را تغییر دهند. این کار باید برای تمامی وب‌سایت‌هایی که دربردارنده‌ی این باگ بوده و پس از کشف آن رفع ایراد شده‌اند، انجام شود. از جمله‌ی چنین سرویس‌هایی می‌توان به یاهو و گوگل اشاره کرد. اما بصورت کلی باید کاربران از قانون تغییر رمز عبور بصورت متوالی و در فاصله‌های زمانی تبعیت کنند.

در صورتی که از سرنوشت اطلاعات خود نگران هستید، می‌توانید رمزهای عبور حساب‌های کاربری خود را تغییر دهید. یکی از اصلی‌ترین نکات برای انتخاب رمزعبور، عدم استفاده از الگویی مشابه برای تمامی حساب‌های کاربری است. همچنین باید در طول و کاراکترهای مورد استفاده در رمزعبور نیز دقت کرده و از ترکیب حروف با اعداد استفاده نمود. ضمنا طول رمزعبور بهتر است بیش از ۱۰ کاراکتر باشد.

انتشار کرم کامپیوتری جدیدی به نام "خونریزی قلبی" که امنیت خطوط ارتباطی در اینترنت را تهدید می‌کند، نگرانی کاربران و شرکت های بزرگ کامپیوتری در سراسر دنیا را برانگیخته است.

پژوهشگران می‌گویند این ویروس جدید، تهدیدی برای امنیتِ اطلاعات شخصی کاربران نظیر گذرواژه، اطلاعات حساب های بانکی و شماره بیمه تامین اجتماعی است. از سوی دیگر، تا زمانیکه وبگاه های در معرض خطر برای ارتقاء نرم افزارهای امنیتی خود اقدام نکنند، کاری از عهده کاربران شخصی ساخته نیست.



یک ضد ویروس برای پیشگیری از خونریزی قلبی

به گزارش اورژانس IT باشگاه خبرنگاران ، Trustlook Antivirus & Mobile Security یکی از قدرتمندترین برنامه های آنتی ویروس برای اندروید است که به صورت کاملا رایگان عرضه شده و تنها نرم افزاری است که خطر امنیتی "خونریزی قلبی" را تشخیص داده و آن را بلوکه می کند .

با استفاده از این آنتی ویروس برروی موبایل و تبلت خود می توانید به آسانی ویروس ها، تروجان ها و کدهای جاسوسی را تشخیص دهید و در عرض چند ثانیه اقدام به حذف آن ها نمایید .

تروجان ها بر خلاف ویروس ها، کرم ها و ... توانایی تکثیر خود را ندارند. آنها بسیار شبیه نرم افزارهای مفید و کاربردی رفتار می کنند، اما در درون خود کدهای مخفی دارند که باعث دسترسی هکر سازنده تروجان به کامپیوتر هدف (کامپیوتر آلوده شده) و به دست گرفتن کنترل آن می شوند. البته در مواردی که چند کاربر از یک کامپیوتر استفاده می کنند سطح دسترسی هکر بسته به سطح دسترسی کاربر آلوده و نوع تروجان تفاوت می کند.