عنوان مقاله:
بررسی حملات موسوم به BadTunnel

محل انتشار:
پنجمین کنفرانس بین المللی تحقیقات دانش بنیان در مهندسی کامپیوتر و فناوری اطلاعات (سال: 1396)

تعداد صفحات اصل مقاله: 8

نویسندگان:
غلامرضا احمدی - *مربی دانشگاه خلیج فارس، بوشهر، خیابان شهید ماهینی، دانشکده فنی مهندسی دانشگاه خلیج فارس*

مرتضی جهان تیغ - *دانشگاه زنجان، دانشکده مهندسی، زنجان، ایران*

خلاصه مقاله:
این مقاله روش جدیدی برای گذشتن از شبکه را معرفی می کند که با نام BadTunnel شناخته می شود. این روش نیازی ندارد که مهاجم روی همان شبکه باشد. حتی زمانی که دیوارآتشین و ابزارهای NAT در این میان وجود دارند این حمله می تواند موفقیت آمیز باشد. اگر مهاجم بتواند کاربر را متقاعد کند که یک صفحه را با استفاده از مرورگرهای Microsoft Edge یا internet explore مشاهده کند و یا یک سند office را باز کند، آنگاه می تواند : • خود را به عنوان یک پرینت یا فایل سرور معرفی کند (جا بزند). • sandbox اینترنت اکسپلورر را بدون EPM/AppContainer دور بزند.• ترافیک شبکه را سرقت کرده و نه تنها ترافیک http را بلکه ترافیک مربوط به اپدیت ویندوز و آ پ د ی ت List Certificate Revocation از طریق Microsoft Crypto Api را نیز می تواند سرقت کند. حملات BadTunnel برای تمامی نسخه های ویندوز کارا است. این حمله می تواند بر روی تمامی نسخه های internet explore و Microsoft edge اجرا شود. در حقیقت هرجایی که طرح URI یا مسیر UNC در فایل جاسازی شده باشد این حمله کارا است. برای مثال اگر مسیر URI و UNC یک فایل در یک لینک میانبر فایل جاسازی شده باشند (the Microsoft proprietary LNK / URL file) در لحظه ای که کاربر فایل را در مرورگر ویندوز مشاهده می کند حمله BadTunnel می تواند اتفاق می افتد. پس می تواند از طریق صفحات وب، ایمیل، فلش درایوها و دیگر مدیاها می تواند بکار گرفته شود.

کلمات کلیدی:
حمله Badtunnel، امنیت، مایکروسافت ویندوز، Netbios