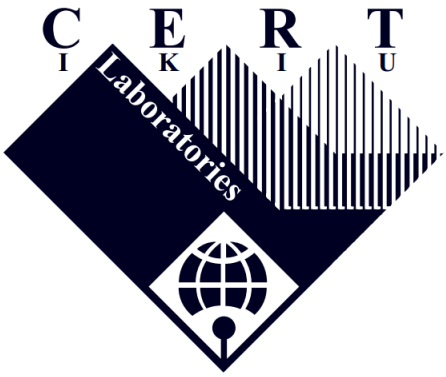

آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

پنجشنبه چهاردهم تیر ماه ۱۳۹۷

انتقال بدافزار از طریق افزونه تقلب بازی‌های رایانه‌ای

نسخه ۱,۰,۰

سردبیر: محمد پیشدار

مهاجمان از طریق افزونه‌های تقلب برای بازی‌های رایانه‌ای به انتشار بدافزارها می‌پردازند.

تاریخ: ۰۳ / جولای / ۲۰۱۸

بررسی اجمالی :

معمولا برای برخی بازی‌های رایانه‌ای افزونه‌های تقلب نظیر افزایش قدرت بازیکن در نبردها و یا سلامتی بی‌پایان ساخته می‌شود. امروزه بسیاری از مهاجمان فضای سایبری با سوءاستفاده از این امر به استقرار بدافزارهای مخرب در سیستم بازیکنان می‌پردازند. اخیرا در همین راستا مهاجمان فضای سایبری با ساخت و انتشار یک افزونه تقلب مخرب برای بازی رایانه‌ای فُرت‌نایت[1] توانسته‌اند بیش از ۷۸۰۰۰ بازیکن در سراسر جهان را آلوده نمایند. این افزونه با نصب یک بدافزار خاص مهاجمان را قادر به تغییر ارتباطات رایانه قربانی هنگام دسترسی به اینترنت از طریق پروتکل اِچ.تی.تی.پی.اِس می‌نماید [۱].

سیستم‌های آسیب‌پذیر [۱] :

- سیستم‌های دارای بازی فُرت‌نایت (و موارد مشابه)

[1]-Fortnite

شدت خطر :

در دولت

- سازمان‌های بزرگ و متوسط در دولت : **پایین**
- سازمان‌های کوچک دولتی : **پایین**

در تجارت

- سازمان های تجاری بزرگ و متوسط : **پایین**
- سازمان‌های کوچک تجاری : **پایین**
- کاربران خانگی : **بالا**

توضیحات فنی :

به تازگی یک پلتفرم بازی‌های رایانه‌ای وب گونه به نام راه بارانی[1] گزارشی در رابطه با این آسیب‌پذیری منتشر کرده است. بر اساس این گزارش یک نوع بدافزار خاص به سیستم تمام قربانیان اضافه شده است. بدافزاری که با سرقت ارتباطات رمزنگاری شده وب (پروتکل اِچ.تی.تی.پی.اِس[2]) در رایانه قربانیان پاسخ‌های بازگشت[3] از سرورهای درخواست شده را به صورت غیرمجاز تغییر می‌دهد. این تغییرات به گونه‌ای است که به نمایش متعدد تبلیغات هنگام مرور وب توسط قربانی خواهد انجامید [۱].

اندرو سامپسون[4]، مدیر عامل پلتفرم راه بارانی در این رابطه می‌گوید [۲]:

"در طول هفته گذشته صدها هزار گزارش خطا از سرورهای خود دریافت کرده‌ایم. خطاهایی که هنگام تلاش سیستم‌های قربانی به برقراری ارتباط غیرمجاز با پلتفرم‌های تبلیغاتی اتفاق افتاده‌اند (ارتباط با سرورهای نفر سوم مجاز نمی‌باشد). نمایش این خطاها به علت استفاده پلتفرم راه بارانی از مکانیسم امنیتی لیست سفید هنگام بارگیری محتویات مختلف است.

[1]-RainWay
[2]-HTTPS
[3]-Response
[4]- Andrew Sampson

لذا تمامی درخواست‌های ارتباط با وبگاه‌های خارج از این لیست از جمله پلتفرم‌های تبلیغاتی با پیام خطا مواجه خواهند گردید. حجم بالای این خطاها ما را به تکاپو واداشته و پس از بررسی‌های فراوان متوجه اشتراک تمام درخواست‌های تبلیغاتی در مبدا ارسال شدیم. تمام درخواست‌های تبلیغاتی از طرف بازی فُرت‌نایت به صورت غیرمجاز ارسال می‌گردید."

تحقیقات نشان می‌دهد که قربانیان این بدافزار تبلیغات از طریق نصب یک ابزار جعلی در بازی فُرت‌نایت آلوده شده‌اند. ابزاری که توسط مهاجمان برای امکان تقلب در این بازی ساخته شده است. مهاجمان با ساخت ویدیوهای تحریک‌کننده از منظر تقلب در بازی و انتشار آن توسط سیستم اشتراک ویدیوی یوتیوب[1] به فریب بازیکنان این بازی برای دریافت فایل مخرب می‌پرداختند. استفاده از کلمه رایگان نیز دلیل دیگری برای متقاعد کردن قربانیان برای دریافت این بدافزار بوده است. تیم راه بارانی پس از تشخیص این بدافزار پیگیری‌های لازم را برای حذف فایل‌های مربوطه در محل وبگاه‌های میزبان[2] انجام داده است. لازم به ذکر است که تا کنون تنها کاربران سیستم‌عامل ویندوز توسط بدافزار تبلیغاتی مربوطه تحت تاثیر قرار گرفته‌اند. بر این اساس می‌توان کاربران بازی فُرت‌نایت در سیستم‌عامل مک[3] و آی.او.اِس [4]را در برابر این بدافزار ایمن دانست. البته حتی با این وجود هم نمی‌توان نسبت به امنیت این نوع دستگاه‌ها در برابر بدافزارهای مذکور بی تفاوت بود. همانطور که مشاهده شد هشدار امنیتی پلتفرم راه بارانی پس از آلوده‌سازی بیش از ۷۸۰۰۰ بازیکن در سراسر جهان منتشر گردید. علاوه بر این نیز برخی وصله‌های مختلف نیز برای بازی فُرت‌نایت در فضای اینترنت دیده می‌شوند. این وصله‌ها پس از استقرار به نصب اجازه‌نامه‌های[5] سطح ریشه[6] در سیستم قربانی می‌پردازند. به این ترتیب مهاجمان می‌توانند با اجرای حملات مرد میانی[7] به ایجاد تغییرات در ترافیک ارسالی بپردازند. نکته جالب در مورد این حملات قابلیت اجرایی آن‌ها حتی با وجود ارتباطات ایمن است. به طور کلی مهاجمان معمولا بازی‌های رایانه‌ای پرطرفدار در جهان را برای ساخت افزونه‌های مخرب مورد هدف قرار می‌دهند. برخی محققان حوزه امینت اطلاعات در ماه گذشته ضمن تایید این موضوع، گوشی‌های هوشمند اندروید را به عنوان هدف جدید مهاجمان عنوان کرده بودند [۱].

[1]-Youtube
[2]-Host
[3]-Mac
[4]-IOS
[5]- Certificate
[6]-Root
[7]-Man in the Middle

پیشنهادات [۱] :

- دانلود بازی‌های رایانه‌ای و افزونه‌های آن تنها از منابع معتبر
- عدم اعتماد به فایل‌های بارگذاری شده کاربران در وبگاه‌های اشتراک محتوای (از جمله یوتیوب)

منابع :

1. The Hacker News Website (https://thehackernews.com/2018/07/fortnite-v-bucks-cheat.html)
2. Rainway Platform Blog (https://blog.rainway.io/how-we-discovered-a-virus-infecting-tens-of-thousands-of-fortnite-players-e5dd6fe1ff55)