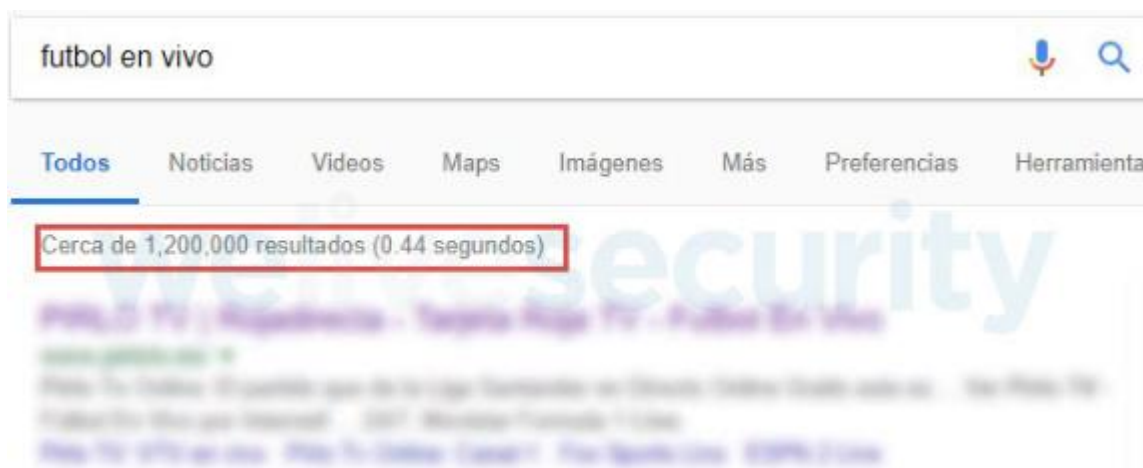


تهدیدات رایج هنگام استفاده از سایت‌های استریم برای تماشای مسابقات جام جهانی

با شروع جام جهانی FIFA، طرفداران فوتبال به دنبال تماشای این مسابقات از طریق سایت‌های استریمینگ (streaming) هستند. اگر در استفاده از این سایت‌ها احتیاط کافی نداشته باشید در معرض خطرات امنیتی سایبری قرار خواهید گرفت. چون تعدادی از این سایت‌ها غیرقانونی هستند و بسیاری از آنها توسط مجرمان سایبری اداره می‌گردند تا از طریق ایمیل گسترش پیدا کنند و دستگاه‌های کاربران را تحت تاثیر قرار دهند.

در اینجا بحث فقط در مورد تبلیغات تهاجمی نیست. کمپین‌های مخربی ایجاد شده‌اند که از اشتیاق طرفداران فوتبال که به دنبال راهی برای تماشای مسابقات هستند، سواستفاده می‌کنند.

برای نشان دادن بعضی از این نمونه سایت‌های مخرب، یک جستجوی ساده در Google انجام شده درست مثل طرفداران فوتبال که این کار را انجام می‌دهند. این جستجوی ساده بیش از یک میلیون نتیجه داشت. با بررسی چندین سایت که موتور جستجو ارائه کرده‌است تهدیدات زیادی کشف شد. در ادامه برخی از رایج‌ترین تهدیدات برای هشدار به طرفداران فوتبال ارائه شده‌است (این تحقیقات در بوبین آیرس انجام شده و در نتیجه برخی تصاویر اسپانیایی هستند).



شکل ۱ نمونه‌ای از جستجوی گوگل

لازم به ذکر است که همه این سایت‌ها مخرب نیستند. با این حال تعداد نمونه‌های مخرب در ۱۰ صفحه اول نتایج جستجو بیشتر بوده‌اند.

کمپین مهندسی اجتماعی برای سرقت اطلاعات

در برخی از صفحات ورزشی استریمینگ (streaming) هنگامی که کاربر در ابتدا وارد می‌شود به صورت اتوماتیک به سایت‌های دیگری با کمپین مهندسی اجتماعی هدایت می‌شوند. این سایت‌ها به دنبال جلب نظر کاربران برای سرقت اطلاعات شخصی آنها هستند. در برخی از سایت‌ها، فقط با ورود به مرورگر به طور خودکار ما را به دو کمپین مهندسی اجتماعی هدایت می‌کند. اولین مورد شامل نظرسنجی و احتمالاً امکان برنده شدن جایزه می‌باشد. این تنها با هدف سرقت اطلاعاتی که مرورگر کاربر استفاده می‌کند انجام می‌شود.

https://...arket.net/index.php#

Junio 11, 2018 11:07:51
Encuesta de opinión de Firefox

¡ENHORABUENA!

¡Has sido seleccionado personalmente para tomar parte en nuestra encuesta de opinión de Junio! Cuéntanos qué piensas sobre Firefox y tendrás la oportunidad de conseguir (1) de los siguientes premios:

APPLE IPHONE X
APPLE MACBOOK

02:20:32

Pregunta 1 de 4:
¿Con qué frecuencia usas Firefox?

Todo el tiempo A veces
Nunca

Copyright 2018 - Todos los derechos reservados.
Esta encuesta es un anuncio. La privacidad es importante para nosotros. No recopilamos tu información personal en este cuestionario. Todos los nombres de productos o marcas son marcas comerciales de sus propietarios respectivos. Ningún navegador o proveedor de servicios de Internet ha creado, participado en, o de cualquier modo revisado este anuncio o lo ha autorizado. Este sitio web recibe una compensación por la compra de los productos presentados. Los productos tienen términos y condiciones importantes, por favor, lee todos los términos y condiciones de los productos antes de pedir alguno de ellos.

شکل ۲ مثالی از یک صفحه که هدف آن یافتن نوع مرورگر مورد استفاده کاربر است.

هنگامی که کاربر نظرسنجی را تکمیل کرد، احتمال برنده شدن آخرین دستگاه موجود در قرعه‌کشی روز به عنوان یک جایزه ارائه می‌شود.

https://opinion.b.promo-market.net/index.php#

Junio 11, 2018 11:08:13
Encuesta de opinión de Firefox

01:45:43

¡Gracias por tu participación!

Tienes una oportunidad de ganar (1) productos de la lista de abajo. Debido a la alta participación de hoy, los premios para los clientes solo se pueden reservar durante 2 minutos.



Apple iPhone X
Precio normal: ~~849\$~~
Tiempo limitado: 0 \$
Cantidad restante: 1
SELECCIONA (1)



Apple Macbook
Precio normal: ~~1999\$~~
Tiempo limitado: Reward
Cantidad restante: 0
INDISPONIBLE

شکل ۳ مثالی از پیشنهاد یک جایزه


در نهایت مبلغی اندک برای ارسال جایزه، از کاربر درخواست می‌گردد. مهم نیست که قربانی چندبار تلاش می‌کند تا شماره کارت خود را وارد کند، پیامی نشان داده می‌شود که پرداخت مجاز نیست. با اینکار مجرمین پشت این کمپین اطلاعات کارت کاربر را به سرقت می‌برند.

Completa el formulario


https://...landing/payment_control/ua_3275b1e825893...

Pago seguro


Producto	Cantidad
Iphone 8 + Trial gratis backh...	1\$
Total	1\$



Nombre del titular

Número de la tarjeta 

Número de la tarjeta

CVV 

Transação não autorizada. Código de segurança inválido.

☒ [Acepto los términos y condiciones](#)

Hacer el pago

Deducción:

1 \$


Tu numero de pedido es:

شکل ۴ پیغام خطای پرداخت غیرمجاز نشان داده شده به کاربر

کمپین دوم که از قالب مهندسی اجتماعی استفاده می کند، قربانی را قانع می کند تا شماره تلفن و شماره شناسایی خود را (همراه با سایر اطلاعات شخصی) وارد کند.

← → ↻ 🏠 ⓘ com/wingames/iphone/es-ar/step1 ... 📧 ☆ ⬇

Participa ahora y llévate este iPhone X GRATIS



Por favor, introduzca los datos para entregarle el premio.

Sr/Sra	E-mail
Sr.	camilo.otros@gmail.com
Nombre	Apellido
Juan	Perez
Zona	Localidad
GBA NORTE	Garín
Celular	
+54 11	1534589955

Todos los campos son obligatorios para validar sus datos.
Los usuarios que se registren con datos falsos o erróneos no entrarán en nuestra base de datos y no recibirán la oferta.

☒ Declaro ser mayor de 18 años

Nacimiento :

13 Mayo 1990

☒ He leído y acepto las [condiciones](#), la [Política de protección de datos](#)

☒ Participá

شکل ۵ مثال از ترفند مورد استفاده برای متقاعد کردن کاربر برای وارد کردن شماره تلفن همراه و شماره شناسایی

کدهای مخرب در حال اجرا در صفحات مربوط به تماشای ورزش آنلاین

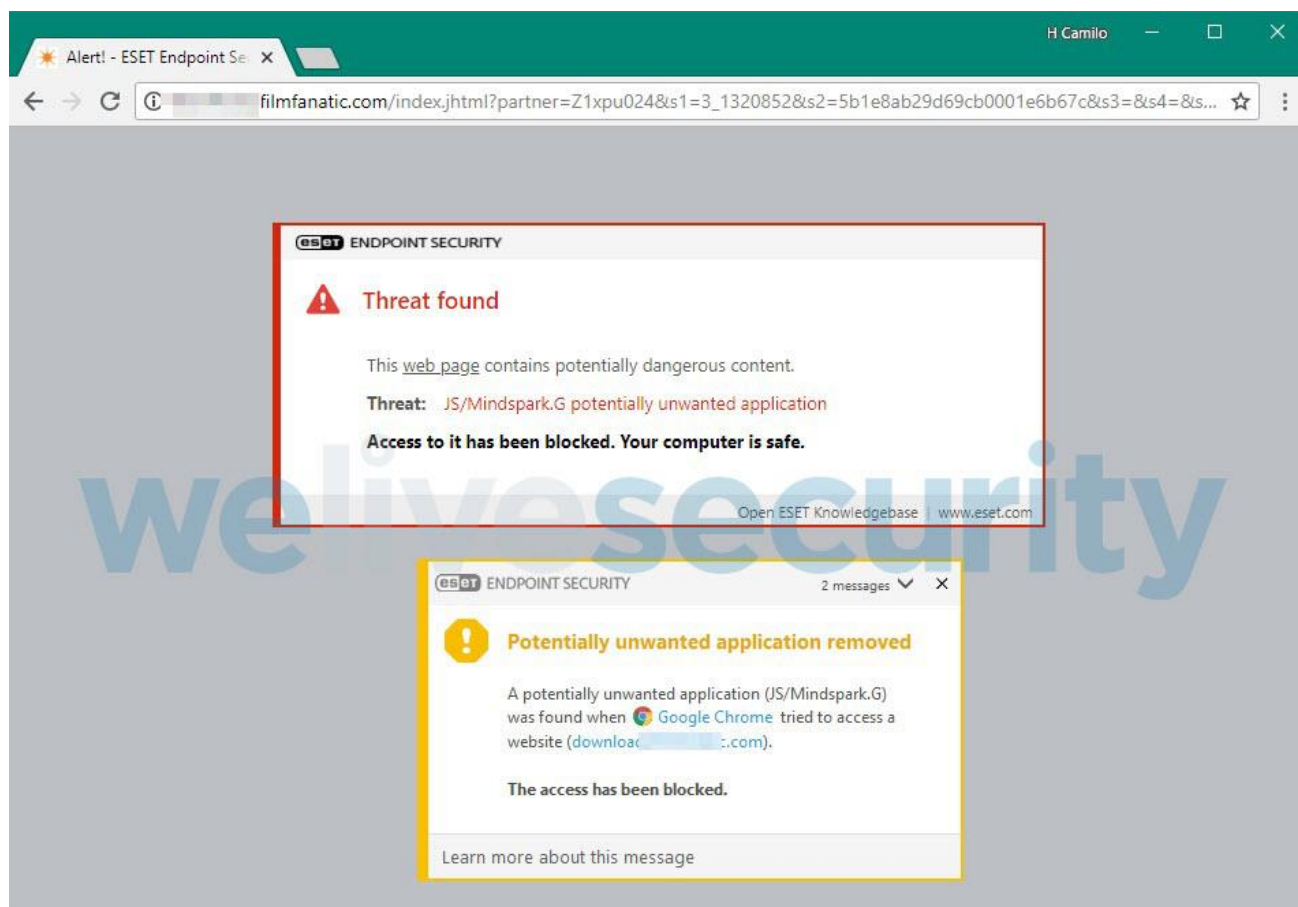
این کدهای مخرب در پخش کننده‌های ویدیویی افزونه‌ها یا add-on‌هایی را پنهان می‌کنند که به منظور دستیابی به اطلاعات شخصی بر روی دستگاه کاربر نصب می‌شوند.



شکل ۶ مثالی از تروجان پنهان شده

ابزارهای تبلیغاتی مزاحم و آزار دهنده

PUA ها برنامه‌های بالقوه خطرناکی هستند که بالاترین میزان تشخیص در کشورهای آمریکای لاتین را داشته‌اند. خوشبختانه، در وبسایت‌هایی که بررسی شدند، محصولات ESET این نوع تهدیدات را شناسایی و مسدود کرده است.

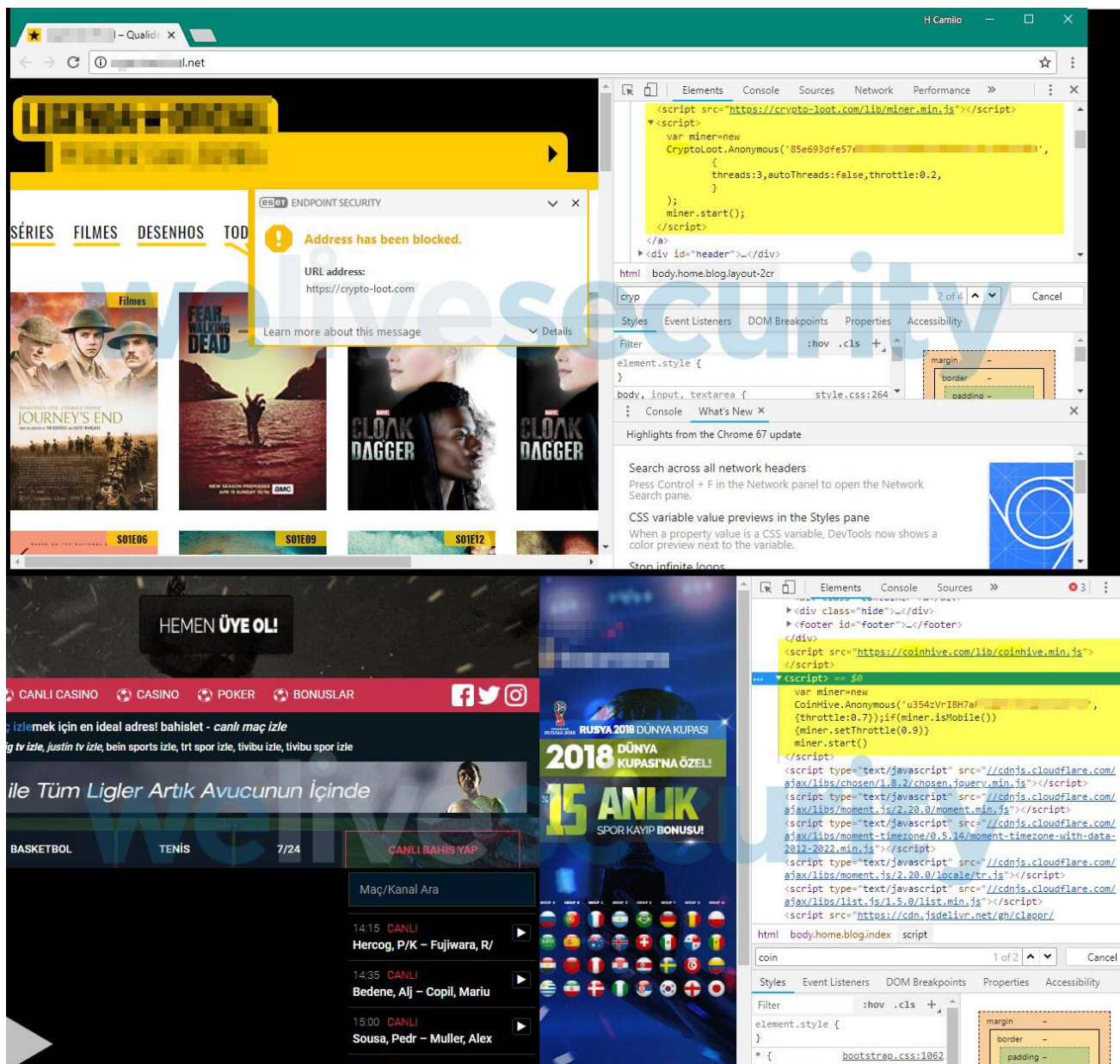


شکل ۷ مسدود سازی آنتی ویروس ESET

هرچند که این برنامه‌های مخرب اطلاعاتی از کاربر به سرقت نمی‌برد اما می‌توانند به دلیل میزان تبلیغاتی که نشان می‌دهند، آزاردهنده باشند. همچنین در بعضی موارد به سایت‌هایی که دارای تهدیدات خطرناک‌تر هستند هدایت می‌شوند.

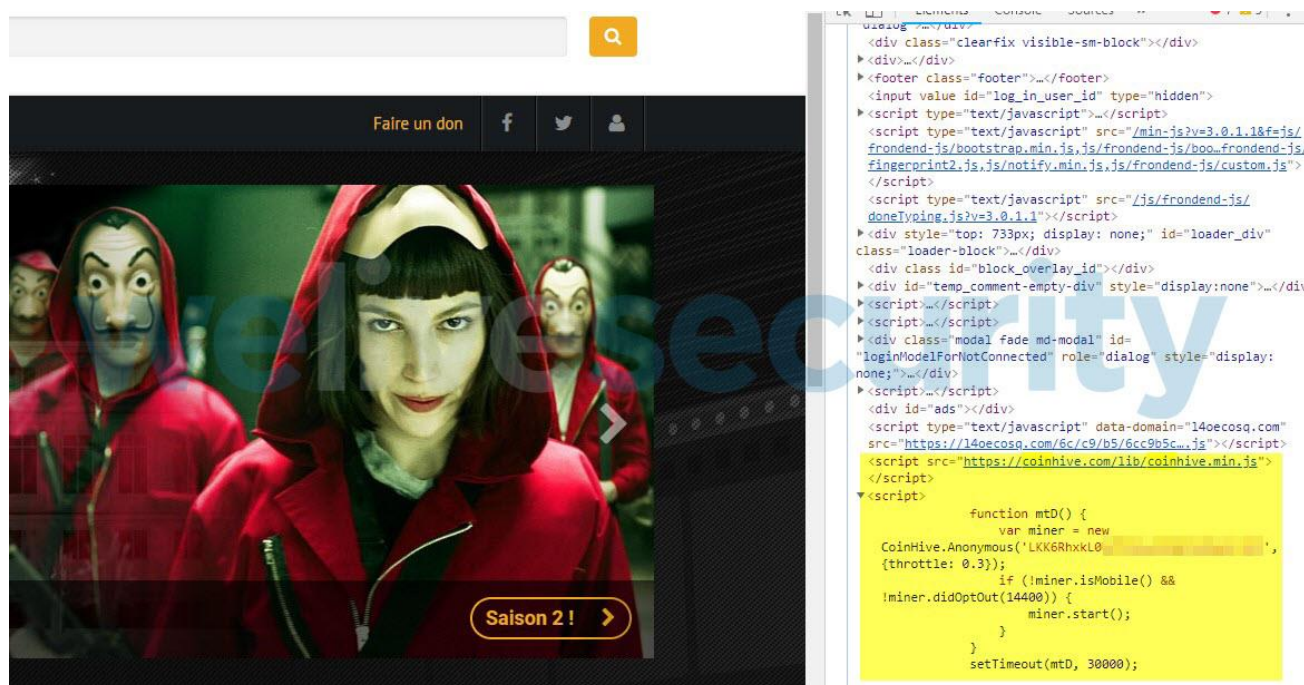
ماینرها در سایت‌های استریم

در طی جستجوهای انجام شده وبسایت‌هایی یافته شده‌اند که استخراج ارز رمزی (cryptocurrency mining) هدف اصلی آن‌ها بود. این یک پدیده رو به رشد است که در آن سایت‌های ورزشی و فیلم‌های استریمی بیشتر مورد استفاده قرار می‌گیرند.



شکل ۸ مثالی از سایت‌های استخراج کننده ارز دیجیتال بر روی دستگاه‌های موبایل

برخی از این استخراج‌کننده‌های ارز دیجیتال به طور ویژه برای دستگاه‌های موبایل آماده شده‌اند.



شکل ۹ استخراج‌کننده‌های ارز دیجیتال همچنین بر روی دستگاه‌های موبایلی کار می‌کنند

همانطور که ما در ابتدای این مقاله گفتیم، این فقط چند نمونه از سوء استفاده مجرمان از آنچه کاربران می‌توانند در اینترنت به دنبال سایت‌های استریمی برای تماشای مسابقات جام جهانی باشد. در حالی که همه سایت‌های بازدید شده، رفتار بدی داشتند و از آنها رفتارهایی ثبت شده بود که به کاربر آسیب رسانده بودند.