

Google ads lead to fake software pages pushing IcedID (Bokbot)

By SANS Internet Storm Center

Archived: 2026-04-02 11:53:37 UTC

Introduction

Fake sites for popular software have occasionally been used by cyber criminal groups to push malware. Campaigns pushing IcedID malware (also known as Bokbot) also [use this method](#) as a distribution technique (we also commonly see IcedID sent through email).

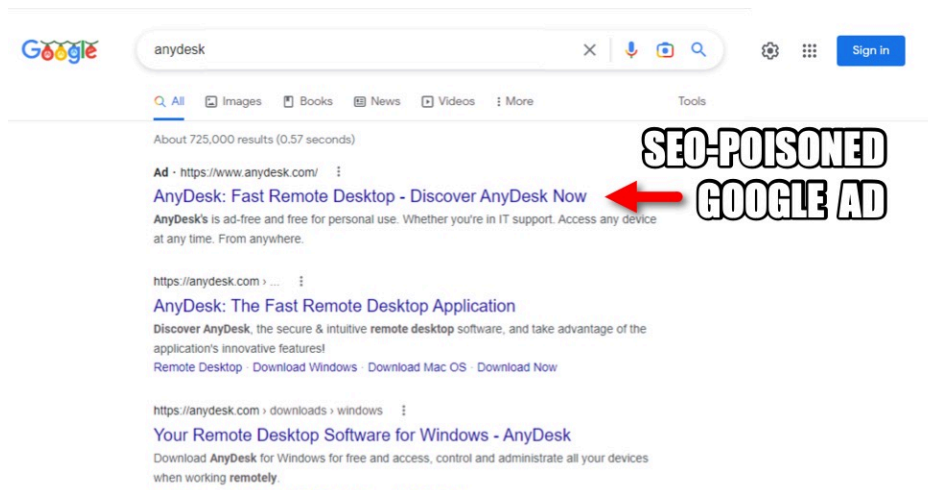
This week, a new round of reports appeared about Google Ads leading to a new sites pushing IcedID.

- <https://infosec.exchange/@bencryptd/109508166164779496>
- https://infosec.exchange/@th3_protoCOL/109513090531163473

Based on these reports, on Wednesday 2022-12-14, I fired up my lab environment and did a Google search for AnyDesk and got a Google ad as my top result. Although the Google ad showed a legitimate AnyDesk URL, it led to a fake site after I clicked the ad.

Today's diary reviews my IcedID infection from this fake AnyDesk site.

Details



Shown above: Search results when I did a quick Google search for AnyDesk.

Search Engine Optimization (SEO) is a technique that websites use to increase their visibility for search engines like Google. Cyber criminals occasionally use SEO to direct search traffic to malicious advertisement links. These ads redirect users to fake software sites based on specific search terms. I've heard this technique referred to as "SEO poisoning."

The above image shows the top search results after I typed **anydesk** into Google search. The top result is a Google ad for AnyDesk, which shows a legitimate URL for the official AnyDesk site.

I clicked on the ad, and it generated the following Google Ad Services URL:

```
https://www.googleadservices[.]com/pagead/aclk?  
sa=L&ai=DChcSEWjh1bP_3_n7AhXbFdQBHdF9AqwYABAAGgJvYQ&ohost=www.google.com&cid=CAASJeRovgWCSOUdKVM_De2wE7MnzlXJ  
Lks&sig=AOD64_3NZNQWkb8O_B18hKIs9Q3klfDfBw&q&adurl&ved=2ahUKEwjHl6v_3_n7AhVrkmoFHdIpAG4Q0Qx6BAGDEAE&nis=8
```

That generated the following URL:

```
https://clickserve.dartsearch[.]net/link/click?&ds_dest_url=https://oferialerkal[.]online/81HqPxz2?  
https://anydesk.com/en/features/unattended-access&id=4&gclid=EAIaIqobChMI4dWz_9_5-  
wIV2xXUAR3RfQKsEAAYASAAEgLqA_D_BwE
```

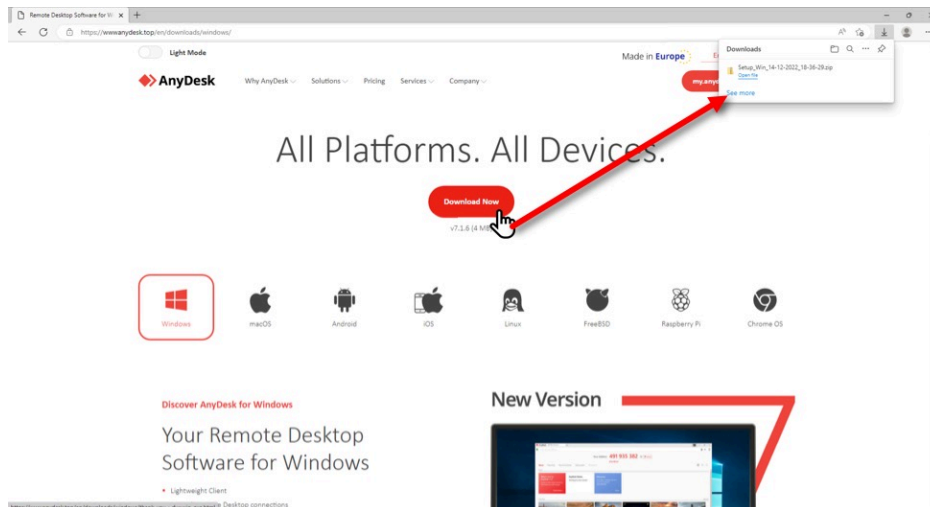
This led to a URL from a malicious traffic distribution system (TDS) domain **oferialerkal[.]online**. These malicious TDS domains frequently change multiple times each day. The above URL generated HTTPS traffic to **oferialerkal[.]online**, which then led to the following fake AnyDesk URL:

```
https://wwwanydesk[.]top/en/downloads/windows
```

This is a fake AnyDesk page, with a button to download a malicious zip archive hosted on a Google Firebase Storage URL at:

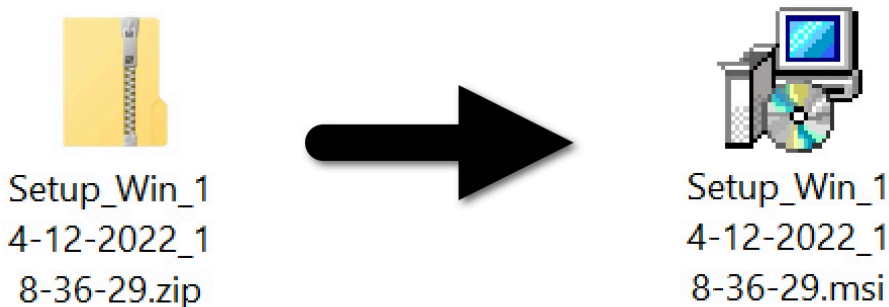
https://firebasestorage.googleapis.com/v0/b/our-audio-370812.appspot.com/o/wnitFn4RCG%2FSetup_Win_14-12-2022_18-36-29.zip?alt=media&token=3ef517f1-eb72-46bc-ac4b-3fb41f92d373

As I wrote this diary, the above URL still worked, and it delivered a the malicious zip archive.

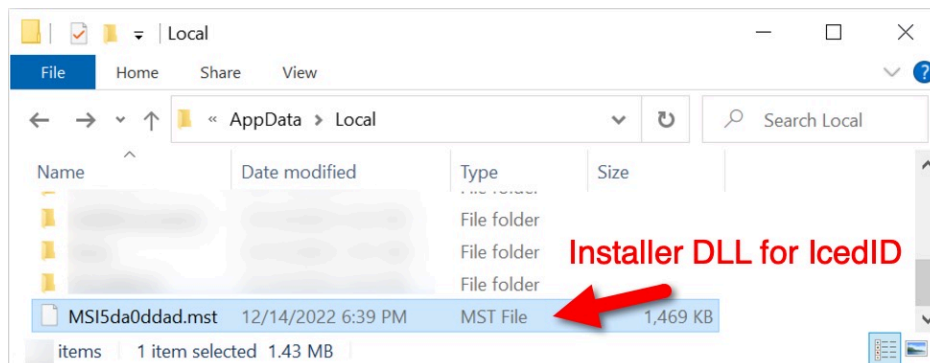


Shown above: Fake AnyDesk site delivering the malicious zip archive.

The zip archive contained a Microsoft Installer (.msi) file. Double-clicking the .msi file on a vulnerable Windows host caused it to drop and run a DLL to install IcedID on the victim's system.



Shown above: Downloaded zip archive and extracted .msi file.



Shown above: The installer DLL for IcedID.

Traffic from the infected Windows host

Time	Dst	Port	Host	Info
2022-12-14 18:36:35	142.250.68.162	443	www.googleadservices.com	Client Hello
2022-12-14 18:36:35	142.251.116.138	443	clickserve.dartsearch.net	Client Hello
2022-12-14 18:36:36	31.41.244.54	443	oferialerka.online	Client Hello
2022-12-14 18:36:36	31.41.244.54	443	oferialerka.online	Client Hello
2022-12-14 18:36:37	45.8.229.109	443	wwanydesk.top	Client Hello
2022-12-14 18:36:37	45.8.229.109	443	wwanydesk.top	Client Hello
2022-12-14 18:36:41	45.8.229.109	443	wwanydesk.top	Client Hello
2022-12-14 18:36:41	45.8.229.109	443	wwanydesk.top	Client Hello
2022-12-14 18:36:41	45.8.229.109	443	wwanydesk.top	Client Hello
2022-12-14 18:36:41	99.86.74.120	443	www.anydesk.com	Client Hello
2022-12-14 18:36:42	45.8.229.109	443	wwanydesk.top	Client Hello
2022-12-14 18:36:42	104.16.89.20	443	cdn.jsdelivr.net	Client Hello
2022-12-14 18:36:42	69.16.175.42	443	code.jquery.com	Client Hello
2022-12-14 18:36:42	172.67.185.105	443	go.smoothiediet.com	Client Hello
2022-12-14 18:36:42	172.67.185.105	443	go.smoothiediet.com	Client Hello
2022-12-14 18:36:43	204.79.197.239	443	edge.microsoft.com	Client Hello
2022-12-14 18:37:12	20.7.2.167	443	client.wns.windows.com	Client Hello
2022-12-14 18:37:24	142.251.45.42	443	firebasestorage.googleapis.com	Client Hello
2022-12-14 18:37:50	204.79.197.200	443	www.bing.com	Client Hello
2022-12-14 18:38:04	104.208.16.88	443	v10.events.data.microsoft.com	Client Hello
2022-12-14 18:38:13	204.79.197.222	443	fp.msedge.net	Client Hello
2022-12-14 18:39:04	143.198.92.88	80	klepdrafoop.com	GET / HTTP/1.1
2022-12-14 18:40:11	94.140.114.40	443	primsenetwork.com	Client Hello
2022-12-14 18:40:14	94.140.114.40	443	primsenetwork.com	Client Hello
2022-12-14 18:40:14	94.140.114.40	443	primsenetwork.com	Client Hello
2022-12-14 18:40:22	94.140.114.40	443	onyxinnov.lol	Client Hello
2022-12-14 18:43:17	52.249.36.206	443	fe2cr.update.microsoft.com	Client Hello
2022-12-14 18:43:18	51.132.193.104	443	v10.events.data.microsoft.com	Client Hello
2022-12-14 18:43:19	40.77.2.164	443	fe3cr.delivery.mp.microsoft.com	Client Hello
2022-12-14 18:43:21	51.132.193.104	443	v10.events.data.microsoft.com	Client Hello
2022-12-14 18:44:18	13.107.4.50	80	ctldl.windowsupdate.com	GET /msdownload/upd...
2022-12-14 18:45:14	94.140.114.40	443	onyxinnov.lol	Client Hello
2022-12-14 18:48:17	40.74.108.123	443	settings-win.data.microsoft.com	Client Hello
2022-12-14 18:48:22	52.113.194.132	443	ecs.office.com	Client Hello
2022-12-14 18:50:16	94.140.114.40	443	onyxinnov.lol	Client Hello
2022-12-14 18:55:18	94.140.114.40	443	onyxinnov.lol	Client Hello
2022-12-14 18:55:21	94.140.114.40	443	onyxinnov.lol	Client Hello
2022-12-14 19:00:21	94.140.114.40	443	onyxinnov.lol	Client Hello
2022-12-14 19:03:19	52.140.118.28	443	settings-win.data.microsoft.com	Client Hello
2022-12-14 19:03:24	20.189.173.6	443	v10.events.data.microsoft.com	Client Hello
2022-12-14 19:05:23	94.140.114.40	443	onyxinnov.lol	Client Hello
2022-12-14 19:06:25	51.195.169.87	8080		[SYN] S
2022-12-14 19:07:07	51.195.169.87	8080		[SYN] S
2022-12-14 19:08:23	52.113.194.132	443	ecs.office.com	Client Hello
2022-12-14 19:08:23	40.126.29.5	443	login.microsoftonline.com	Client Hello
2022-12-14 19:08:24				Client Hello
2022-12-14 19:08:25				Client Hello
2022-12-14 19:08:32	20.189.173.12	443	self.events.data.microsoft.com	Client Hello
2022-12-14 19:10:26	94.140.114.40	443	onyxinnov.lol	Client Hello
2022-12-14 19:11:03	158.255.211.126	443	trashast.wiki	Client Hello
2022-12-14 19:16:04	158.255.211.126	443	trashast.wiki	Client Hello
2022-12-14 19:17:18	51.195.169.87	8080		49837 → 8080 [SYN] S
2022-12-14 19:21:06	158.255.211.126	443	trashast.wiki	Client Hello

Shown above: Traffic from the infection filtered in Wireshark, part 1.

Time	Dst	Port	Host	Info
2022-12-14 20:26:34	158.255.211.126	443	trashast.wiki	Client Hello
2022-12-14 20:29:56	176.105.202.212	80	176.105.202.212	GET /adcs4 HTTP/1.1
2022-12-14 20:30:17	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:31:08	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:31:36	158.255.211.126	443	trashast.wiki	Client Hello
2022-12-14 20:31:52	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:31:54	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:32:37	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:32:48	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:33:29	51.132.193.104	443	v10.events.data.microsoft.com	Client Hello
2022-12-14 20:33:35	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:33:39	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:34:26	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:34:31	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:35:19	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:35:21	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:36:05	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:36:07	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:36:38	158.255.211.126	443	trashast.wiki	Client Hello
2022-12-14 20:36:39	199.127.62.132	80	199.127.62.132	GET /download/h.exe HTTP/1.1
2022-12-14 20:36:50	108.177.235.187	443	bukifide.com	Client Hello
2022-12-14 20:36:50	91.199.212.52	80	crt.sectigo.com	GET /SectigoRSADomainValidat...
2022-12-14 20:36:53	108.177.235.187	443	bukifide.com	Client Hello
2022-12-14 20:36:53	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:36:57	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:36:57	108.177.235.187	443	bukifide.com	Client Hello
2022-12-14 20:36:58	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:36:59	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:37:00	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:37:01	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 20:37:02	172.67.130.194	443	kingoflake.com	Client Hello

Shown above: Traffic from the infection filtered in Wireshark, part 2.

Time	Dst	Port	Host	Info
2022-12-14 21:42:40	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:40	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:42	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:43	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:43	190.61.121.35	443	190.61.121.35:443	GET /static/ZillaSlab-Bold.subset.e96c
2022-12-14 21:42:44	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:45	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:46	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:47	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:49	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:49	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:50	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:51	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:53	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:54	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:55	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:56	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:57	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:42:58	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:00	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:04	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:06	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:07	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:08	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:08	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:09	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:09	46.4.182.102	80		Client Hello
2022-12-14 21:43:11	46.4.182.102	80		Client Hello
2022-12-14 21:43:11	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:12	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:13	172.67.130.194	443	kingoflake.com	Client Hello
2022-12-14 21:43:14	172.67.130.194	443	kingoflake.com	Client Hello

**BINARY WITH
SHELLCODE AND
64-BIT EXE**

**TLSv1.3
TRAFFIC OVER
TCP PORT 80**

Shown above: Traffic from the infection filtered in Wireshark, part 3.

Indicators of Compromise

Traffic generated by IcedID installer DLL for gzip binary:

- 143.198.92[.]88 port 80 - klepdrafoop[.]com - GET / HTTP/1.1

IcedID post-infection C2 traffic:

- 94.140.114[.]40 port 443 - primsenetwolk[.]com - HTTPS traffic
- 94.140.114[.]40 port 443 - onyxinnov[.]lol - HTTPS traffic
- 158.255.211[.]126 port 443 - trashast[.]wiki - HTTPS traffic

IcedID backchannel traffic with VNC:

- 51.195.169[.]87 port 8080

First Cobalt Strike:

- 176.105.202[.]212 port 80 - 176.105.202[.]212 - GET /adcs4
- 172.67.130[.]194 port 443 - kingoflake[.]com - HTTPS traffic

Second Cobalt Strike:

- 199.127.62[.]132 port 80 - 199.127.62[.]132 - GET /download/h.exe
- 108.177.235[.]187 port 443 - bukifide[.]com - HTTPS traffic

Sliver and/or DonutLoader:

- 190.61.121[.]35 port 443 - 190.61.121[.]35:443 - GET /static/ZillaSlab-Bold.subset.e96c15f68c68.woff/CEx6_0FDJn4RWxBZcsquwwUk57-n7pCuR5k24zUnBepPlxY9gqn968ZXnXAtC2GwTONSpEx3Pnz_lvqz2c2E5B_7n2IMU3wZ7Yeqb9yK90FsqEQnybJ3Thr_uiJpi3X5yQI3puCyeMxD8EcfWPoPWF8lqYiHLRDP1rKGIpBbW
- 46.4.182[.]102 port 80 - post-infection TLSv1.3 HTTPS traffic

Associated malware:

Downloaded zip and extracted .msi file:

SHA256 hash: [19265aac471f7d72fcddb133e652e04c03a547727b6f98a80760dcfb43f95627](#)

File size: 1,108,416 bytes

File name: Setup_Win_14-12-2022_18-36-29.zip

SHA256 hash: [63a7d98369925d6e98994cdb5937bd896506665be9f80dc55de7eb6df00f7607](#)

File size: 1,966,080 bytes

File name: Setup_Win_14-12-2022_18-36-29.msi

IcedID files from an infected Windows host:

SHA256 hash: [7e5da5fcd0da494da85cdc76384b3b08f135f09f20e582e049486e8ae2f168e](#)

File size: 1,503,408 bytes

File location: C:\Users\[username]\AppData\Local\MSI5da0ddad.mst

File description: 64-bit DLL to install IcedID dropped by above .msi file

Run method: rundll32.exe [filename],init

SHA256 hash: [53639070024366d23c3de5ba1d074cbd1d8b9e78d46f75c32ef02fc20c279fc3](#)

File size: 1,503,408 bytes

File location: hxxp://klepdrafooiip[.]com/

File description: gzip binary from klepdrafooiip[.]com retrieved by IcedID installer DLL

SHA256 hash: [205fb52fafd456388d3ef80ff00498c90295791a91811725fea94052dc4fe7a](#)

File size: 364,202 bytes

File location: C:\Users\[username]\AppData\Roaming\GenreAttract\license.dat

File description: Data binary used to run persistent IcedID DLL

Note: First submitted to VirusTotal on 2022-11-08.

SHA256 hash: [bfa3eb36beea65334abe81cdd870e66b37da3e478d1615697160244fd087b48](#)

File size: 1,499,312 bytes

File location: C:\Users\[username]\AppData\Roaming\{12A3307B-B372-BBC6-7E4B-4992C7C7842B}\{6127EF7F-696C-8BDF-5350-88ECC5774CA5}\uwurth4.dll

File description: persistent IcedID DLL

Run method: rundll32.exe [filename],init --tu="[path to license.dat]"

Cobalt Strike files:

SHA256 hash: [7486c3585d6aa7c2febd8b4f049a86c72772fda6bd1dc9756e2fb8c5da67bafa](#)

File size: 1,894,758 bytes

File location: htttp://176.105.202[.]1212/adcs4

File description: PowerShell script for first instance of Cobalt Strike activity

SHA256 hash: [e8f2c929e1b84a389fede03bff9a4ee951cf563a64809b06f2f76201536fdd7](#)

File size: 1,001,472 bytes

File location: hxxp://199.127.62[.]132/download/h.exe

File location: C:\Users\[username]\AppData\Local\Temp\Dimuak.exe

File description: 64-bit EXE for second instance of Cobalt Strike activity

Sliver and/or DonutLoader:

SHA256 hash: [40194a07a5afa1ef8e0ea4125a62d4ff5b70a14849b154a4694cfd08e40eb22b](#)

File size: 17,085,660 bytes

File location: hxxp://190.61.121[.]135:443/static/ZillaSlab-

Bold.subset.e96c15f68c68.woff/CEX6_0FDJn4RWxBZcsquwwUk57-

n7pCuR5k24zUnBepPlxY9gqn968ZXnXAtC2GwTONSpEx3Pnz_lvqz2c2E5B_7n2IMU3wZ7Yeqb9yK9OFsqEQnybJ3Thr_uiJpi3X5yQ13puCyecatd8A
MxD8EcfWPoPWF8lqYiHLRDP1rKGIpBbW

File description: binary with shellcode and 64-bit EXE, for Sliver-based and/or DounutLoader malware

SHA256 hash: [08dd1a4861f4d2b795efb71847386bd141caa0a7ce141798e251db8acd63d3a9](#)

File size: 17,081,991 bytes

File description: above binary with shellcode removed

File type: PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows

Final words

We'll likely continue to see criminal groups abusing Google ads through SEO poisoning and using fake websites to impersonate popular software. This is an effective way for criminals to distribute their malware.

Traffic and malware samples from today's infection are available [here](#).

Brad Duncan

brad [at] malware-traffic-analysis.net