Operation Photoshop

Description:

- In this report, I will be analyzing a collection of “free” or “cracked” Photoshop malware samples. These samples have been identified as malicious and have been collected for further analysis and research. I only will provide Indicators of Comprise for these samples as there are too many to induvially analyze, and there are other write-ups on the stealers in this report.
- The malware samples were collected from various sources such as Youtube, Google Drive and random websites claiming to have cracks for these tools. The samples were found to be distributed as “free” or “cracked” versions of Adobe Photoshop. However, upon analysis, it was discovered that these versions contained malicious code designed to perform information stealing specifically designed to steal credentials, history and profiles from browsers like Microsoft Edge and Chrome.
- The malware samples were analyzed using various tools and techniques, including static and dynamic analysis. The following IOCs were identified during the analysis:

File hashes:

SHA256's:

```
f8c08ee89c855a5c4667ca859e193e05ce5073c7b89e4f3d4fbf6bdb0c50f243
901c7ca0adfc6fe126d7832b7301388abbe9db0a4ecf898af6937bde6ecf8235
e1fd2d534eed837ebb0fb3b0f25732dadaf4bfd95de92b6c44935d624d991dab
e842fef8dc197785add80f6c7221fed9273dfabbca53573f831078ac5bcdba83
6f660f20b028535681b17bebde60ffc3bb0b5b2748a6ef38fb258ac371fad450
b9736626a522b3d6301ede70895f1ffbb592d88b2f9e7a9908797e0a0249b00c
c9716a41f6865025271a42553f3240810b678f89bffaa2a5c69a0576757947ab
91b8833d045e42de89fceb8698a75cd45b3a1b45fc67d1115cf9a181d7ca100b
39429ddce866fb8657c3fe04c9ec8a2eef27b73680835e4abcec6d3afb63f66e
c751b386ba177fa63844bee350b500cd85b6c745266646f49955b8f5925ff637
807dba280d2922afbdb7334fe3e0a602f59dcf597276c6b4948e8140090bc19b
d462eb9334417cb33132a253cc5a14e353fdfbb9c017206d4245dcb0adba1286
9b288865300a7261da921b78271ead94f23ac05573956b1d1bb9497843740b20
823ed9160c90cb222748a1dace33e1d5c9557c4a0ecb3db3ce9eeea43b6dfcbd
6a46524a57257a6e245db4de83af275b0905172e2ec03c16c42c68b4fa2cb9b8
eec127c8585ed227e340df5d4f9eb3850a83f5d863ba05ad96b0290ac9533707
c1b8be1b0a269685906c3ed30054ebe6dcf3ef2485f487c1897dae7301ae989d
a95e8e313e93553a7c4a541803a26620fb30a9a0a87a69c014ab8d5d9c43ef82
bdaf728aee883c0dca1c6e54834cac55013c35c31e29e7aaa81966a8233ccf8b
15c93ace10b30d5dd311c426bd203ee600bdee351542c601d52787537037648f
cac690dac1ab7f072111eaca623baec624101ee38fe13b3dcd83118826d2f5c4
```

e4ebd8a12c039824c90f23ee142e2437f69028bcb4919ad2e0a6322fd4933eca
4d7197c26f7e892d7a71fcd35b87955409a1be229d0363363bbcba41fc1260aa

File names:

ApplicationSetupFile13.92.exe
Installer.exe
setu .exe.exe
Setup2.exe
S u .exe
Setup.exe
Setup_x64.exe
Adobe Photoshop crack.exe
Installer2.exe
Installer.scr
Predictor.exe
lic.exe
Activat-Photoshop-CC-2019-v20.0.5.27259-64-bit-By-Rover-Egy.exe
Adobe photoshop cs6 keygen.exe
adobe.cs6.all.products.activator.exe
Adobe Photoshop CS6 Extended 13.1.2 Extended RePack by JFK2005 Upd. 12.04.2013.exe
Adobe Photoshop Keys + Crack Generator.exe

Network indicators:

http://83[.]217[.]11[.]34
http://83[.]217[.]11[.]35
http://78[.]46[.]254[.]12:80
http://116[.]203[.]11[.]45/670
https://t.me/noktasinawatchthisepson.zip
http://45[.]15[.]156[.]239/
http://77[.]73[.]134[.]24/Clip1.exe
http://45[.]9[.]74[.]170
http://77[.]73[.]134[.]35/bebra.exeh
http://45[.]9[.]74[.]170/df10bec8b1422e27e94111cd0e1fe32e
http://77[.]73[.]134[.]43
http://78[.]46[.]235[.]109/hera.zip
http://89[.]40[.]14[.]155/MmKOeuvnwAbxqUTz.exe
http://88[.]198[.]108[.]245/c
167[.]172[.]68[.]26:81
185[.]106[.]93[.]132:800
45[.]141[.]215[.]90:21913
82[.]115[.]223[.]46:57672
176[.]113[.]115[.]24:37118
83[.]217[.]11[.]34
77[.]73[.]134[.]24

```
77[.]73[.]134[.]35
82[.]115[.]223[.]46:57672
194[.]87[.]31[.]171
104[.]193[.]254[.]97
185[.]106[.]93[.]132:800
167[.]172[.]68[.]26:81
```

In conclusion, this report highlights the presence of malicious code in "free" or "cracked" versions of Adobe Photoshop. The identified IOCs can be used to detect and prevent similar malware from infecting systems and networks.

If you would like to take a look at the files they are all posted here:

- https://bazaar.abuse.ch/user/1422334716322136069/