# From Cracks to Empty Wallets – How Popular Cracks Lead to Digital Currency and Data Theft

labs.bitdefender.com/2021/04/from-cracks-to-empty-wallets-how-popular-cracks-lead-to-digital-currency-and-data-theft/

Anti-Malware Research

3 min read

*For about three years, hackers have been stealing cryptocurrency from victims' Monero wallets using powerful malware delivered through software cracks for popular apps.*

Cracks and patches have been around since the advent of commercial software. Easy to use and widely available on specialized sharing websites, these small apps let people bypass commercial protections in popular software and use applications without paying for them. However, besides the legal implications of unauthorized software use, the cyber-security risks are serious.

Bitdefender analysts have recently uncovered a series of attacks that leverage office tools and image-editing software cracks to compromise computers, hijack crypto-currency wallets and exfiltrate information via the TOR network.

Once executed, the crack drops an instance of ncat.exe (a legitimate tool to send raw data over the network) as well as a TOR proxy. The Netcat and TOR proxy files are dropped on disk as either `%syswow64%\nap.exe` or `%syswow64%\ndc.exe` for the first one and `%syswow64\tarsrv.exe` for the latter. Additionally, a batch file is dropped at `%syswow64%\chknap.bat` (for nap.exe) and `%syswow64%\nddcf.cmd` (for ndc.exe) that contains the command-line for the Ncat component, which cycles through ports 8000 to 9000 on a .onion domain, as shown in the screenshot below.

*Fig. 1: Example of batch file containing the command-line for the Ncat component*

The tools work together to create a powerful backdoor that communicates through TOR with its command and control center: the ncat binary uses the listening port of the TOR proxy (`–proxy 127.0.0.1:9075`) and uses the standard `–exec` parameter, which allows all input from the client to be sent to the application and responses to be sent back to the client over the socket (reverse shell behavior).

The crack creates persistence mechanisms for the TOR proxy file and the Ncat binary on the machine with a service and a scheduled task that runs every 45 minutes, respectively. Our investigation reveals that – most likely – the backdoor is being used interactively by a human operator rather than sending automated requests to the victims. Some of the actions we observed are:

- File exfiltration. Ncat can receive local files to send over TOR to the command and control centers.
- BitTorrent client execution. We believe attackers are using BitTorrent clients to exfiltrate data.
- Turning off the firewall in preparation for data exfiltration.
- Theft of Firefox browser profile data (history, credentials and session cookies). Before exfiltration, attackers archive the profile folder with 7zip to generate one file that contains everything.
- Theft of the Monero wallet via the legitimate CLI client `monero-wallet-cli.exe`.

This list of actions is non-exhaustive, as attackers have complete control of the system and can adapt campaigns based on their current interests.

## Distribution

## Indicators of Compromise

### File paths:

```
%SYSWOW64%\ncat.exe
%SYSWOW64%\ndc.exe
%SYSWOW64%\chknap.bat
%SYSWOW64%\nddcf.cmd
%SYSWOW64%\tarsrv.exe
%SYSTEM32%\ncat.exe
%SYSTEM32%\ndc.exe
%SYSTEM32%\tarsrv.exe
%SYSTEM32%\nddcf.cmd
%SYSTEM32%\tarsrv.exe
```

## File hashes:

### Ncat:

1859a996f978bf73798f337d4b6c7029d14c1cc272e4b8ef522497e61554041c

b65a7bbc6448e871c2d68d3bfb91760869877863ce1250b142e180a373fed891

930d414567d27eec1dbb59616dbdce0aa9cdece0135666dafa83bb9c260496c4

f29aecc2d0bca9fe874e2687adc4d0b0d21c8e7371cff291531dbbc6997abf5c

### Ncat-executing batch file:

d93fab085d15448e6540cde779189e753a45f5a13daea5dfea32d736091cdefd

782bac6a0d5d913ec5b20414fe226219c1e21124de2aaa5665375f712f3b6a51

18a432feca1f2e66986e19006a301cacb8cd2f1d89b340d72aac4f79eff70937

4f959c4b69af3604002f292aff87e3a603d45cee67f432d3bb34627c044d9afc

e02c70044e45c840aec446f4e9a7bc8708c4a37da534a1fecc75ad0937b94526

### Tor proxy:

97a9b6db3aee2308af341413f2671c86079c8d010e0b7f4c2324004553bc17a8

ef09d109eb6fe8d999247bf2a175b4642d6412ebf289957376761ab8bb63dbc5

f08d24a42c5befbf323507ca90b76a8d0152c5998bcfe86e34941c4e731748ae

e0569c36ad6c8f08cc0b64f25a10228cdf318b7a970ef0c203e1f3e69289ffc4

964c75385ec8389df2e0a4dda803910298284l9986d052ba442d33048eb45e72

24399c64b4382100bee197b0753fe5ca4c01b7f773c61e7247d6b4acf82a98fd

### Droppers:

ddc39ecf007b1e36b16182a73c73f4c7c9e37d69d55870f56dcc2cbdecb81827

156bcba04147d7e2bc2778a50c2bd434b9d50efd7fdf3f541a8e25d42c052cc0

e82606c6ce6d303456f26311d83715cd41716be4eed61b9aa3364f2c69a35620

e43db8e57a9829202458775f9eb5232a643eaf7603be737ade74355bb1f3a068

865f87c430271f1538f9535cbb8e3fb908abf4a87b13fce228232d726fb38b6b

21328a4185729349421fe01f53b1707745ccf30ad17061a6d965e047c50da131

## Onion domains

4wye25lxiiws2n2uh7gyftn7cnas45o7adf5jjmnkusmhevaortywsad.onion
pya3iu6oldo62qn6yhimjztryxz3tqhb7bqkspfmdaqu5lqmspxxt5qd.onion
qmev4br46su73tn7wco5yx3f5ckcljchmgwtm56nvxbzkzngt777uoqd.onion
rxa3aqwxcz2sqthq5b4epmxjweaipq2phadfk6cmpvgdzqpyhfss4ryd.onion
s5dthib3esbzbbp4v6txpd4al2ozfpitkqk72hsdontvcmig3qdfacad.onion
wbjp5c5nfu6mnxb6pdtqgfhssdrzjf4756tj4bhhupnvqhv4sidfqgqd.onion
yzffgdbyrci3zdgerrarmx6faadvmtmcxboj25qvjb334cfuemh5t4ad.onion
cbjpyldwxfc5bzdszzbrcatrjlevjr5qsk44enytvkovkv2thzxmjhyd.onion
snbrrmnu3j7awyxu.onion

### TAGS

anti-malware research

### AUTHOR

## Eduard BUDACA

I'm a security researcher at Bitdefender. When not dissecting malware, I enjoy coding and playing video games.

View all posts

## Bogdan BOTEZATU

Information security professional. Living my second childhood at @Bitdefender as director of threat research.

View all posts