CryptBot

Published: 2023-03-16 · Archived: 2026-04-05 18:58:10 UTC


```
{'c2': 'http://erniku42.top/gate.php;',
 'settings': [{'key': 'CookiesEdge', 'value': 'false'},
  {'key': 'HistoryEdge', 'value': 'false'},
  {'key': 'HistoryFirefox', 'value': 'false'},
  {'key': 'EdgeDB', 'value': 'true'},
  {'key': 'Edge', 'value': 'false'},
  {'key': 'Files', 'value': 'false'},
  {'key': 'Opera', 'value': 'false'},
  {'key': 'CookiesOpera', 'value': 'false'},
  {'key': 'HistoryOpera', 'value': 'false'},
  {'key': 'Screenshot', 'value': 'true'},
  {'key': 'Chrome', 'value': 'false'},
  {'key': 'Info', 'value': 'true'},
  {'key': 'HistoryChrome', 'value': 'false'},
  {'key': 'ChromeDB', 'value': 'true'},
  {'key': 'Wallet', 'value': 'true'},
  {'key': 'ChromeExt', 'value': 'true'},
  {'key': 'Firefox', 'value': 'false'},
  {'key': 'CookiesChrome', 'value': 'false'},
  {'key': 'FirefoxDB', 'value': 'true'},
  {'key': 'CookiesFirefox', 'value': 'false'},
  {'key': 'Desktop', 'value': 'true'},
  {'key': 'EdgeExt', 'value': 'true'},
  {'key': 'CookiesFile', 'value': '_AllCookies.txt'},
  {'key': 'HistoryFile', 'value': '_AllHistory.txt'},
  {'key': 'NTFS', 'value': 'true'},
  {'key': 'Key', 'value': 'NkB7vazOVtAR2LZ'},
  {'key': 'DesktopFolder', 'value': '_Desktop'},
  {'key': 'UAC', 'value': 'false'},
  {'key': 'ScreenFile', 'value': '$CREEN.PNG'},
  {'key': 'DeleteAfterEnd', 'value': 'true'},
  {'key': 'MessageAfterEnd', 'value': 'false'},
  {'key': 'FirefoxDBFolder', 'value': '_Firefox'},
  {'key': 'Anti', 'value': 'false'},
  {'key': 'EdgeDBFolder', 'value': '_Edge'},
  {'key': 'UserAgent', 'value': ''},
  {'key': 'Prefix', 'value': 'mrd-'},
  {'key': 'WalletFolder', 'value': '_Wallet'},
  {'key': 'PasswordFile', 'value': '_AllPasswords.txt'},
  {'key': 'ChromeDBFolder', 'value': '_Chrome'},
```

```
    {'key': 'ExternalDownload', 'value': 'http://ovapfa05.top/unfele.dat'},
    {'key': 'FilesFolder', 'value': '_Files'},
    {'key': 'InfoFile', 'value': '_Information.txt'}]}
```

Source: https://research.openanalysis.net/cryptbot/botnet/yara/config/2023/03/16/cryptbot.html