# Oski Stealer: Indicators of Compromise

## MALICIOUS SAMPLES

- aa33731aa48e2ea6d1eaab7c425f9001182c0e73e0226eb01145d6b78d7cb9eb
- 6f213642729883 68a75692e2e30970ce18e625bd7b2bcb154353415b31816d4e
- 946d4d332a06b9af10da38beb3e8195054840b59a870a2f9027e6471f4869dc6
- f38a38d97bd96a42e8c3f985f1e65daca97dce229b36c8c80c9229666826f325
- 1e433ad9b3a8bb067865903abd9ccac597ad73352c2f18d6d55fbf83ba0a8da2
- 1e0608ba01db4c6a953d5a2bf144a944d5939790fd9e0acd7c06a37563470add
- 911bd853436509e0a95c187e080a534a9ea050fb86ee64584c76e9a9b1768ff3
- 03830b7509fe6e46ea89d7fe60f732120cca1501473c5fc477e2d96b01f7f050
- b1e2aea01a76f1372aa5cf60e58e994022638b9e10184d49ee07383f6c03d946
- fdd060d4ee221701282ca13c743cc95965708d71a975691f04e300a99fd23916

## NETWORK COMMUNICATION

- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz
- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz/softokn3.dll
- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz/sqlite3.dll
- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz/freebl3.dll
- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz/mozglue.dll
- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz/msvcp140.dll
- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz/nss3.dll
- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz/vcruntime140.dll
- http://sl9XA73g7u3EO07WT42n7f4vIn5fZH[.]biz/main.php

OR

- http://f0457102.xsph.ru/1.jpg
- http://f0457102.xsph.ru/2.jpg
- http://f0457102.xsph.ru/3.jpg
- http://f0457102.xsph.ru/4.jpg
- http://f0457102.xsph.ru/5.jpg
- http://f0457102.xsph.ru/6.jpg
- http://f0457102.xsph.ru/7.jpg

## MALICIOUS ACTIVITY

Cmd.exe /c taskkill /pid <pid> & erase <path> & RD /S /Q <working_folder>* & exit

## C&Cs

- http://zver[.]tech
- http://watchmovie[.]life
- http://l10992ea[.]justinstalledpanel[.]com
- http://45[.]143[.]93[.]152
- http://Xenicoln[.]gb[.]net
- http://52[.]246[.]250[.]237
- http://194[.]87[.]236[.]221
- http://databasecontrol[.]xyz
- http://admin[.]foa[.]ae
- http://tgp[.]opcache[.]xyz
- http://gfxapanbnqdqjhf[.]pw
- http://45[.]143[.]92[.]129
- http://oski[.]aprendiendoaver[.]com
- http://178[.]32[.]145[.]141
- http://onlinemseof[.]site
- http://45[.]151[.]144[.]128
- http://travelgidblog[.]top
- http://194[.]87[.]95[.]5
- http://hostisgerhg[.]tk
- http://proxy[.]bonch[.]dev
- http://masadproject[.]life/base
- http://85[.]209[.]91[.]120
- http://shlyapa[.]website
- http://4llion[.]com
- http://l009fa92[.]justinstalledpanel[.]com
- http://topteamover9000[.]fun
- http://80[.]89[.]238[.]87
- http://89[.]223[.]123[.]36
- http://miklem[.]website
- http://liilldshar[.]space
- http://firstnamehello[.]com
- http://194[.]87[.]234[.]156
- http://5[.]187[.]7[.]144
- http://poiuytrewq2[.]site
- http://pablopanuroere[.]pw
- http://162[.]0[.]224[.]159
- http://194[.]87[.]147[.]13
- http://cmd3490ghbdtn3[.]ru
- http://188[.]227[.]57[.]121
- http://bergamot[.]nu
- http://j6g3fzp[.]5k5[.]ru
- http://173[.]232[.]146[.]69
- http://92[.]53[.]124[.]88
- http://xenicoln[.]gb[.]net
- http://yrhealth[.]life
- http://kepler071[.]site
- http://45[.]141[.]84[.]143
- http://ggtyyu[.]pw
- http://80[.]89[.]228[.]202
- https://admin[.]913alerts[.]com
- http://195[.]133[.]197[.]21
- http://91[.]245[.]227[.]131
- http://195[.]133[.]147[.]113
- http://46[.]17[.]96[.]25
- http://guputhy[.]site
- http://176[.]113[.]81[.]170
- http://45[.]8[.]228[.]100
- http://eessss[.]online
- http://datamon[.]cc/zoom
- http://l93015ad[.]justinstalledpanel[.]com
- http://la8204a3[.]justinstalledpanel[.]com

## GRABBER CONFIGURATIONS

The configuration extracted from different C&Cs.

```
1;USERPROFILE\Desktop;*.txt;
Documents;USERPROFILE\Documents;*.dat,*.key,*.txt,*.rar,*.doc,*.xls,*.jpeg,*.xlsx,*.docx,*.jpg,*.pdf;Desktop;USERPROFILE\Desktop;*.dat,*.key,*.txt,*.rar,*.doc,*.xls,*.jpeg,*.xlsx,*.docx,*.jpg,*.pdf;
Desktop;USERPROFILE\Desktop;*.kdbx,*.key,*.2fa*.jpg,*2fa*.png,*2fa*.txt,*account*.doc,*account*.txt,*auth*.doc*,*auth*.jpg,*auth*.pdf,*auth*.png,*auth*.txt,*backup*.jpg,*backup*.png,*backup*.txt,*backup*.doc,*backup*.docx,*bibox*,*binance*,*bitcoin*,*bitfinex*,*bitflyer*,*bitforex*,*bithimb*,*bithumb*,*bitinka*,*bitmart*,*bitmex*,*bitstamp*,*bittrex*,*blockchain*,*coin*.doc*,*coin*.txt,*coin*.xls*,*coinb*,*coincheck*,*coinegg*,*coinomi*,*crypto*,*cryptonator*,*dash*,*digifinex*,*electrum*,*eth*.docx,*eth*.json,*eth*.txt,*exodus*,*gdax*,*gemini*,*hitbtc*,*huobi*,*idax*,*jaxx*,*key*.txt,*kraken*,*kucoin*,*livecoin*,*metamask*,*monero*,*oex*,*okex*,*pass*.doc*,*pass*.xls*,*password*,*poloniex*,*private*,*recovery*.doc,*recovery*.txt,*recovery*.png,*recovery*.txt,*recovery*.pdf,*secret*.pdf,*secret*.txt,*secret*.doc,*seed*.pdf,*seed*.txt,*simex*,*tidex*,*trade*,*upbit*,*upbit,*verge*,*wallet*,*waves*,*yobit*,*zb.com*,UTC-*,*localbitcoins*,*quadrigacx*;
Documents;USERPROFILE\Documents;*.kdbx,*.key*,*2fa*.jpg,*2fa*.png,*2fa*.txt,*account*.doc,*account*.txt,*auth*.doc*,*auth*.jpg,*auth*.pdf,*auth*.png,*auth*.txt,*backup*.jpg,*backup*.png,*backup*.txt,*backup*.doc,*backup*.docx,*bibox*,*binance*,*bitcoin*,*bitfinex*,*bitflyer*,*bitforex*,*bithimb*,*bithumb*,*bitinka*,*bitmart*,*bitmex*,*bitstamp*,*bittrex*,*blockchain*,*coin*.doc*,*coin*.txt,*coin*.xls*,*coinb*,*coincheck*,*coinegg*,*coinomi*,*crypto*,*cryptonator*,*dash*,*digifinex*,*electrum*,*eth*.docx,*eth*.json,*eth*.txt,*exodus*,*gdax*,*gemini*,*hitbtc*,*huobi*,*idax*,*jaxx*,*key*.txt,*kraken*,*kucoin*,*livecoin*,*metamask*,*monero*,*oex*,*okex*,*pass*.doc*,*pass*.xls*,*password*,*poloniex*,*private*,*recovery*.doc,*recovery*.txt,*recovery*.png,*recovery*.txt,*recovery*.pdf,*secret*.pdf,*secret*.txt,*secret*.doc,*seed*.pdf,*seed*.txt,*simex*,*tidex*,*trade*,*upbit*,*upbit,*verge*,*wallet*,*waves*,*yobit*,*zb.com*,UTC-*,*localbitcoins*,*quadrigacx*;
AppData;APPDATA\;*.kdbx,*.key*,*2fa*.jpg,*2fa*.png,*2fa*.txt,*account*.doc,*account*.txt,*auth*.doc*,*auth*.jpg,*auth*.pdf,*auth*.png,*auth*.txt,*backup*.jpg,*backup*.png,*backup*.txt,*backup*.doc,*backup*.docx,*bibox*,*binance*,*bitcoin*,*bitfinex*,*bitflyer*,*bitforex*,*bithimb*,*bithumb*,*bitinka*,*bitmart*,*bitmex*,*bitstamp*,*bittrex*,*blockchain*,*coin*.doc*,*coin*.txt,*coin*.xls*,*coinb*,*coincheck*,*coinegg*,*coinomi*,*crypto*,*cryptonator*,*dash*,*digifinex*,*electrum*,*eth*.docx,*eth*.json,*eth*.txt,*exodus*,*gdax*,*gemini*,*hitbtc*,*huobi*,*idax*,*jaxx*,*key*.txt,*kraken*,*kucoin*,*livecoin*,*metamask*,*monero*,*oex*,*okex*,*pass*.doc*,*pass*.xls*,*password*,*poloniex*,*private*,*recovery*.doc,*recovery*.txt,*recovery*.png,*recovery*.txt,*recovery*.pdf,*secret*.pdf,*secret*.txt,*secret*.doc,*seed*.pdf,*seed*.txt,*simex*,*tidex*,*trade*,*upbit*,*upbit,*verge*,*wallet*,*waves*,*yobit*,*zb.com*,UTC-*,*localbitcoins*,*quadrigacx*;
Documents;USERPROFILE\Documents;*.jpg,*.img,*.json,*.txt;
desktop;USERPROFILE\Desktop;*.jpg,*.img,*.json,*.txt;
Desktop;USERPROFILE\Desktop;*.txt,*.json;
Desktop;USERPROFILE\Desktop;*.txt;
gg;USERPROFILE\Desktop;*.txt;
Documents;USERPROFILE\Documents;*.dat,*.key,*.txt,*.rar,*.doc,*.xls,*.jpeg,*.xlsx,*.docx,*.jpg,*.pdf;Desktop;USERPROFILE\Desktop;*.dat,*.key,*.txt,*.rar,*.doc,*.xls,*.jpeg,*.xlsx,*.docx,*.jpg,*.pdf;
Tg;APPDATA\Telegram Desktop\tdata\;*map*,*D877F783D5D3EF8C*;
Doc;USERPROFILE\Documents;*.txt;
Desktop;USERPROFILE\Desktop;*.txt;
sdfdsfds;USERPROFILE\Desktop;*coin*.*txt*,*wallet*.*txt*,*btc*.*txt*,*eth*.*txt*,*seed*.*txt*,*privat*.*txt*,*phrase*.*txt*,*btc*.*xlsl*,*wallet*.*xlsl*,*coin*.*xlsl*,*seed*.*xlsl*,*eth*.*xlsl*,*exodus*.*xlsl*,*jaxx*.*xlsl*,*exodus*.*txt*,*jaxx*.*txt*;
123;USERPROFILE\;*coin*.*txt*,*wallet*.*txt*,*btc*.*txt*,*eth*.*txt*,*seed*.*txt*,*privat*.*txt*,*phrase*.*txt*,*btc*.*xlsl*,*wallet*.*xlsl*,*coin*.*xlsl*,*seed*.*xlsl*,*eth*.*xlsl*,*exodus*.*xlsl*,*jaxx*.*xlsl*,*exodus*.*txt*,*jaxx*.*txt*;
coines;USERPROFILE\Desktop;*coin*.doc;
coines;USERPROFILE\Desktop;*wallet*.doc;
coines;USERPROFILE\Desktop;*wallet*.txt;
coines;USERPROFILE\Desktop;*btc*.txt;
coines;USERPROFILE\Desktop;*coin*.txt;
coines;USERPROFILE\Desktop;*2fa*.txt;
coines;LOCALAPPDATA\;*2fa*.txt;
1;USERPROFILE\Desktop;*.txt;
dock;USERPROFILE\Documents;*.txt;
desk;USERPROFILE\Desktop;*.txt;
Documents;USERPROFILE\Documents;*.dat,*.key,*.txt,*.rar,*.doc,*.xls,*.jpeg,*.xlsx,*.docx,*.jpg,*.pdf;Desktop;USERPROFILE\Desktop;*.dat,*.key,*.txt,*.rar,*.doc,*.xls,*.jpeg,*.xlsx,*.docx,*.jpg,*.pdf;
zip;USERPROFILE\Desktop;*.rar,*.zip;
doc;USERPROFILE\Documents;*.jpg,*.txt,*.png,*.jpeg,*.key,*docx;
took;USERPROFILE\Desktop;*.jpg,*.txt,*.png,*.jpeg,*.key;
Documents;USERPROFILE\Documents;*.dat,*.key,*.txt,*.rar,*.doc,*.xls,*.jpeg,*.xlsx,*.docx,*.jpg,*.pdf;Desktop;USERPROFILE\Desktop;*.dat,*.key,*.txt,*.rar,*.doc,*.xls,*.jpeg,*.xlsx,*.docx,*.jpg,*.pdf;
```