Erel Regev

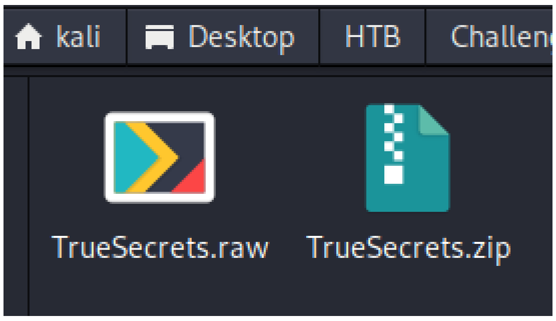
Table of Contents

Intro

Challenge Description by HTB:

Our cybercrime unit has been investigating a well-known APT group for several months. The group has been responsible for several high-profile attacks on corporate organizations. However, what is interesting about that case, is that they have developed a custom command & control server of their own. Fortunately, our unit was able to raid the home of the leader of the APT group and take a memory capture of his computer while it was still powered on. Analyze the capture to try to find the source code of the server.

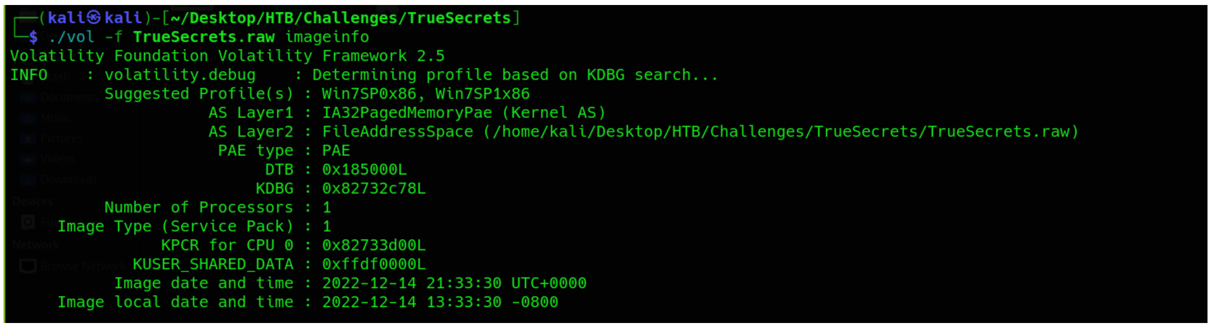
I received the following files:



Seems to be a memory file.

Memory Analysis

Trying to get the profile of the investigated memory:

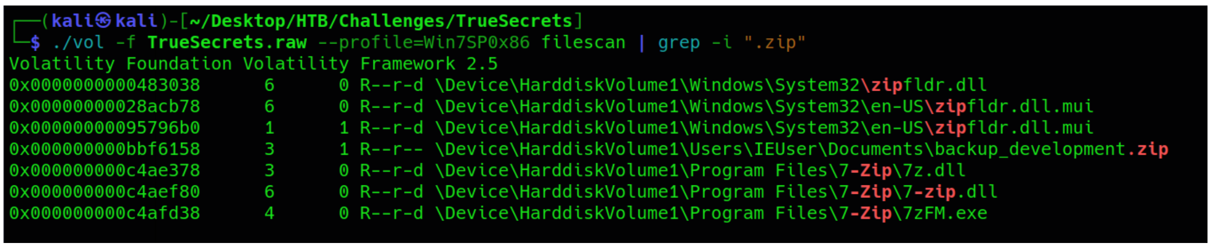


```
┌──(kali㉿kali)-[~/Desktop/HTB/Challenges/TrueSecrets]
└─$ ./vol -f TrueSecrets.raw imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/HTB/Challenges/TrueSecrets/TrueSecrets.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82732c78L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82733d00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2022-12-14 21:33:30 UTC+0000
     Image local date and time : 2022-12-14 13:33:30 -0800
```

Looks like WindowS 7 OS.

I started to look for interesting file extensions, starting with .zip.

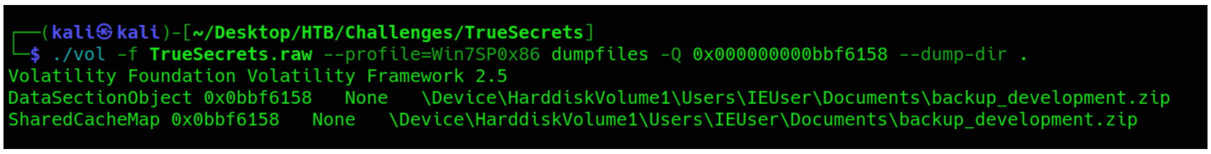
I used the filescan plugin command of volatility, using the found profile



```
┌──(kali㉿kali)-[~/Desktop/HTB/Challenges/TrueSecrets]
└─$ ./vol -f TrueSecrets.raw --profile=Win7SP0x86 filescan | grep -i ".zip"
Volatility Foundation Volatility Framework 2.5
0x0000000000483038      6      0 R--r-d \Device\HarddiskVolume1\Windows\System32\zipfldr.dll
0x00000000028acb78      6      0 R--r-d \Device\HarddiskVolume1\Windows\System32\en-US\zipfldr.dll.mui
0x00000000095796b0      1      1 R--r-d \Device\HarddiskVolume1\Windows\System32\en-US\zipfldr.dll.mui
0x000000000bbf6158      3      1 R--r-- \Device\HarddiskVolume1\Users\IEUser\Documents\backup_development.zip
0x000000000c4ae378      3      0 R--r-d \Device\HarddiskVolume1\Program Files\7-Zip\7z.dll
0x000000000c4aef80      6      0 R--r-d \Device\HarddiskVolume1\Program Files\7-Zip\7-zip.dll
0x000000000c4afd38      4      0 R--r-d \Device\HarddiskVolume1\Program Files\7-Zip\7zFM.exe
```

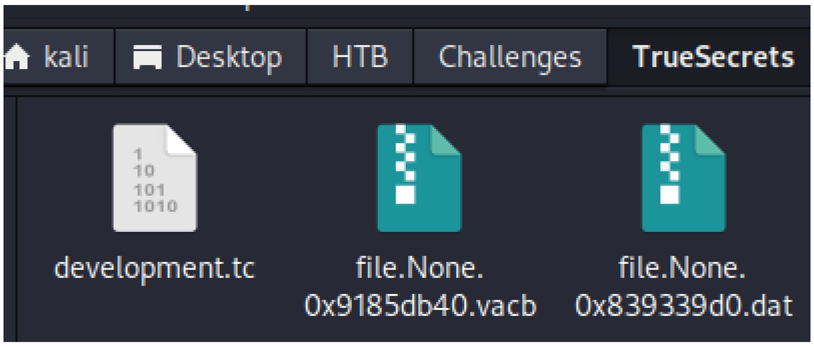
There is a file on IEUSER profile called backup_development.zip.

Dumping the file using the physical offset:



```
┌──(kali㉿kali)-[~/Desktop/HTB/Challenges/TrueSecrets]
└─$ ./vol -f TrueSecrets.raw --profile=Win7SP0x86 dumpfiles -Q 0x000000000bbf6158 --dump-dir .
Volatility Foundation Volatility Framework 2.5
DataSectionObject 0x0bbf6158   None   \Device\HarddiskVolume1\Users\IEUser\Documents\backup_development.zip
SharedCacheMap 0x0bbf6158   None   \Device\HarddiskVolume1\Users\IEUser\Documents\backup_development.zip
```

Extracted the .tc file:



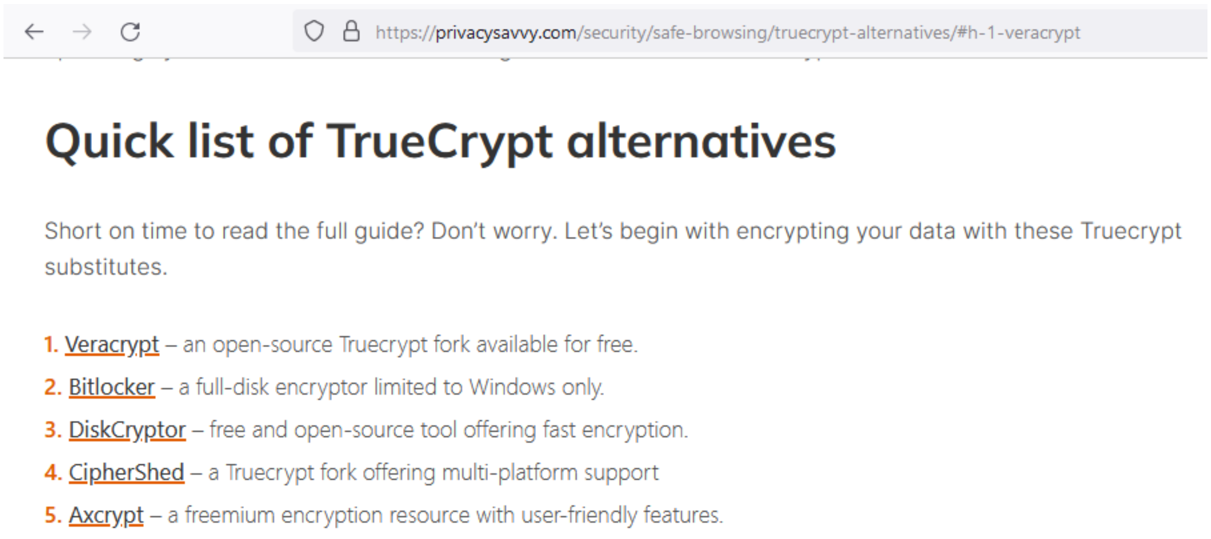
HTB Challenge - TrueSecrets -Subject: Forensics -Difficulty: Easy

Erel Regev

Note regarding the .tc extension:

Virtual encrypted disk created by TrueCrypt, an open-source disk encryption program that creates real-time (on-the-fly) encrypted volumes.

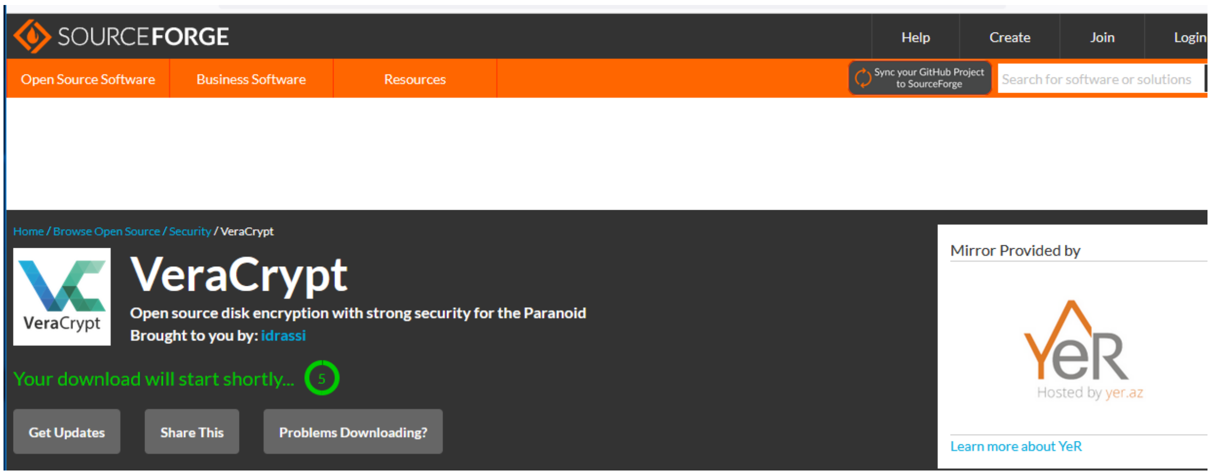
After reading about TrueCrypt, it is not recommended and unsafe to use it. I looked for alternatives and the first on the list was VeraCrypt:


https://privacysavvy.com/security/safe-browsing/truecrypt-alternatives/#h-1-veracrypt

Quick list of TrueCrypt alternatives

Short on time to read the full guide? Don't worry. Let's begin with encrypting your data with these Truecrypt substitutes.

1. Veracrypt – an open-source Truecrypt fork available for free.
2. Bitlocker – a full-disk encryptor limited to Windows only.
3. DiskCryptor – free and open-source tool offering fast encryption.
4. CipherShed – a Truecrypt fork offering multi-platform support
5. Axcrypt – a freemium encryption resource with user-friendly features.



VeraCrypt

Open source disk encryption with strong security for the Paranoid

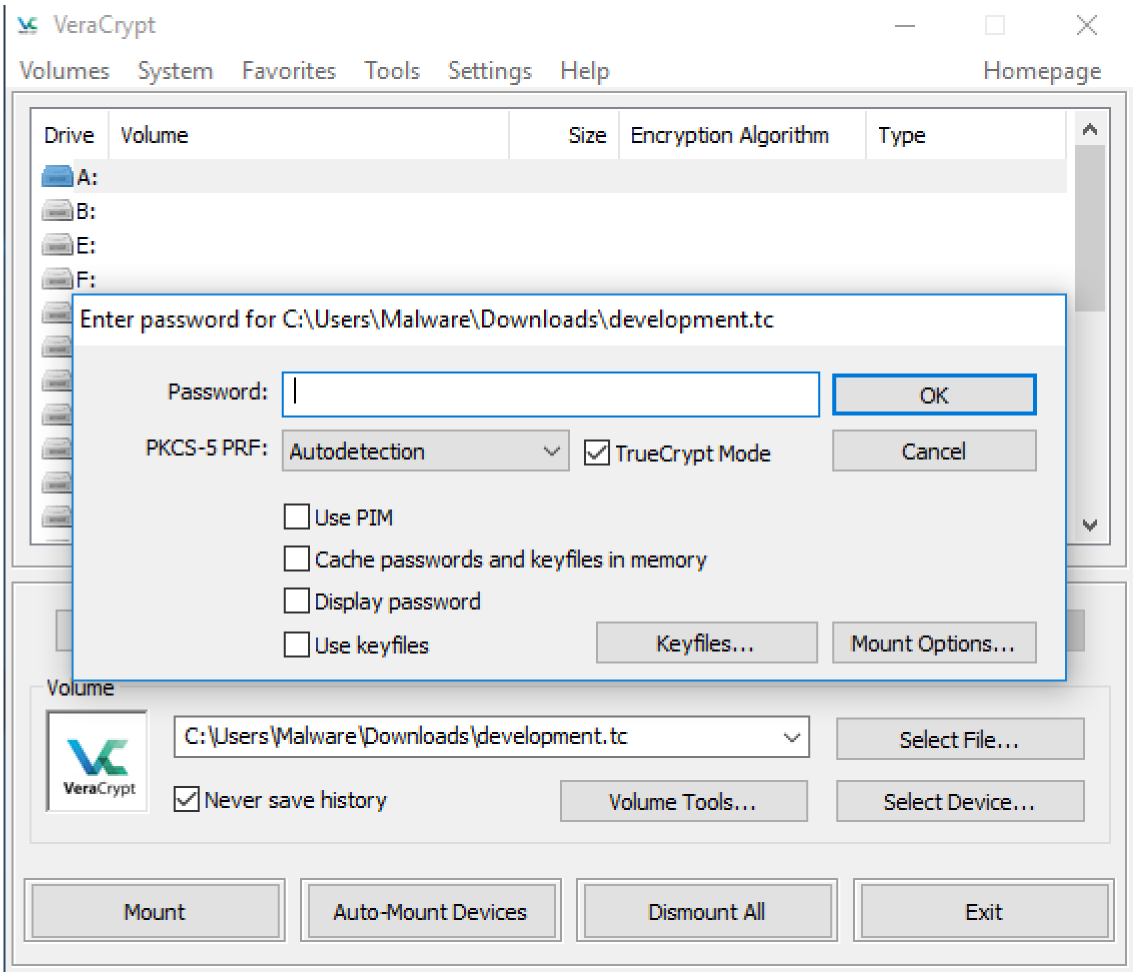
Brought to you by: idrassi

Your download will start shortly... 5

HTB Challenge - TrueSecrets -Subject: Forensics -Difficulty: Easy

Erel Regev

It seems to have a password behind it:



Enter password for C:\Users\Malware\Downloads\development.tc

PKCS-5 PRF: Autodetection

[✓] TrueCrypt Mode

[ ] Use PIM

[ ] Cache passwords and keyfiles in memory

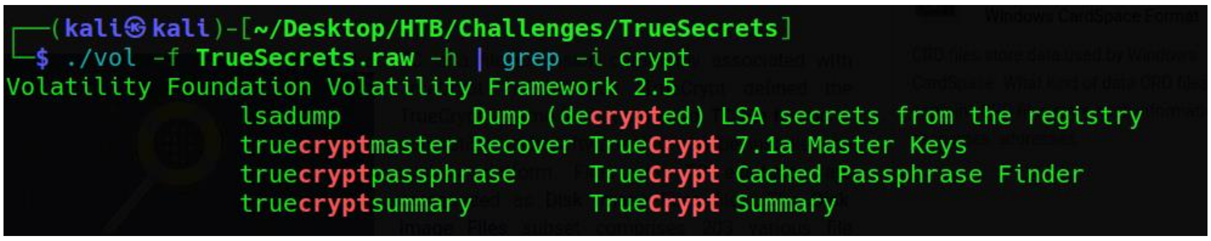
[ ] Display password

[ ] Use keyfiles

Volume: C:\Users\Malware\Downloads\development.tc

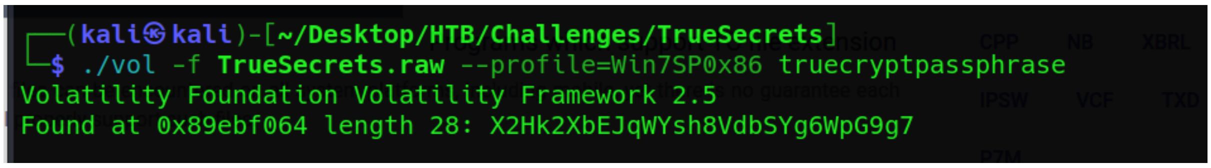
[✓] Never save history

Volatility can try and extract TrueCrypt keys:



```
┌──(kali㉿kali)-[~/Desktop/HTB/Challenges/TrueSecrets]
└─$ ./vol -f TrueSecrets.raw -h | grep -i crypt
Volatility Foundation Volatility Framework 2.5
                lsadump         Dump (decrypted) LSA secrets from the registry
                truecryptmaster Recover TrueCrypt 7.1a Master Keys
                truecryptpassphrase  TrueCrypt Cached Passphrase Finder
                truecryptsummary     TrueCrypt Summary
```

Got the passphrase. Cool stuff.

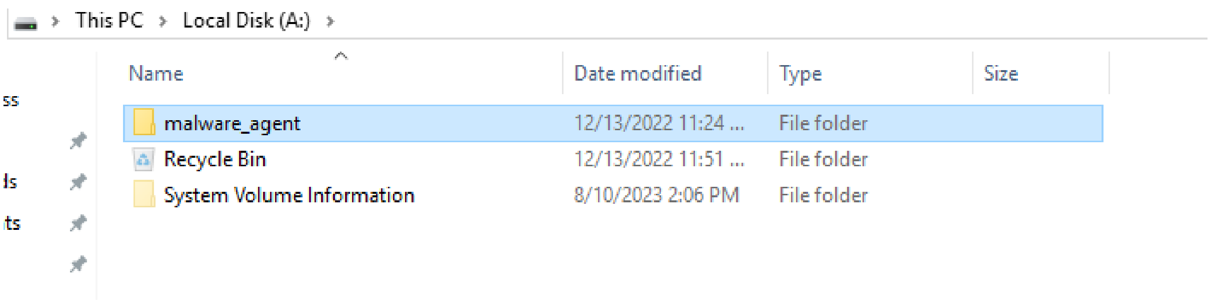


```
┌──(kali㉿kali)-[~/Desktop/HTB/Challenges/TrueSecrets]
└─$ ./vol -f TrueSecrets.raw --profile=Win7SP0x86 truecryptpassphrase
Volatility Foundation Volatility Framework 2.5
Found at 0x89ebf064 length 28: X2Hk2XbEJqWYsh8VdbSYg6WpG9g7
```

HTB Challenge - TrueSecrets -Subject: Forensics -Difficulty: Easy

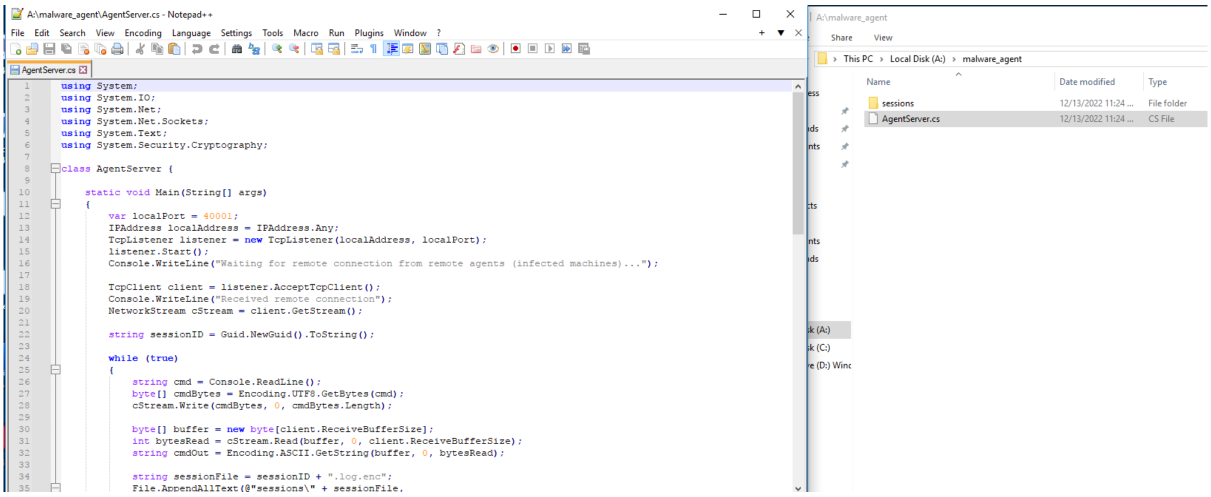
Erel Regev

I entered the password in the VeraCrypt application and received a new drive, with the following files:



This PC > Local Disk (A:)

Name	Date modified	Type	Size
malware_agent	12/13/2022 11:24 ...	File folder	
Recycle Bin	12/13/2022 11:51 ...	File folder	
System Volume Information	8/10/2023 2:06 PM	File folder	



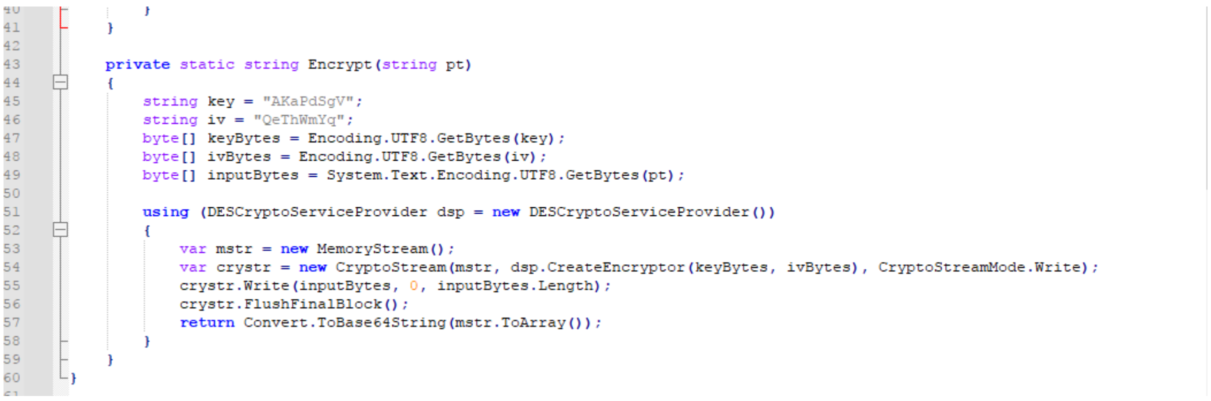
A:\malware_agent\AgentServer.cs - Notepad++

```
using System;
using System.IO;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Security.Cryptography;

class AgentServer {

    static void Main(String[] args)
    {
        var localPort = 40001;
        IPAddress localAddress = IPAddress.Any;
        TcpListener listener = new TcpListener(localAddress, localPort);
        listener.Start();
        Console.WriteLine("Waiting for remote connection from remote agents (infected machines)...");

        TcpClient client = listener.AcceptTcpClient();
        Console.WriteLine("Received remote connection");
        NetworkStream cStream = client.GetStream();

        string sessionID = Guid.NewGuid().ToString();

        while (true)
        {
            string cmd = Console.ReadLine();
            byte[] cmdBytes = Encoding.UTF8.GetBytes(cmd);
            cStream.Write(cmdBytes, 0, cmdBytes.Length);

            byte[] buffer = new byte[client.ReceiveBufferSize];
            int bytesRead = cStream.Read(buffer, 0, client.ReceiveBufferSize);
            string cmdOut = Encoding.ASCII.GetString(buffer, 0, bytesRead);

            string sessionFile = sessionID + ".log.enc";
            File.AppendAllText(@"sessions\" + sessionFile,
```

A:\malware_agent > This PC > Local Disk (A:) > malware_agent

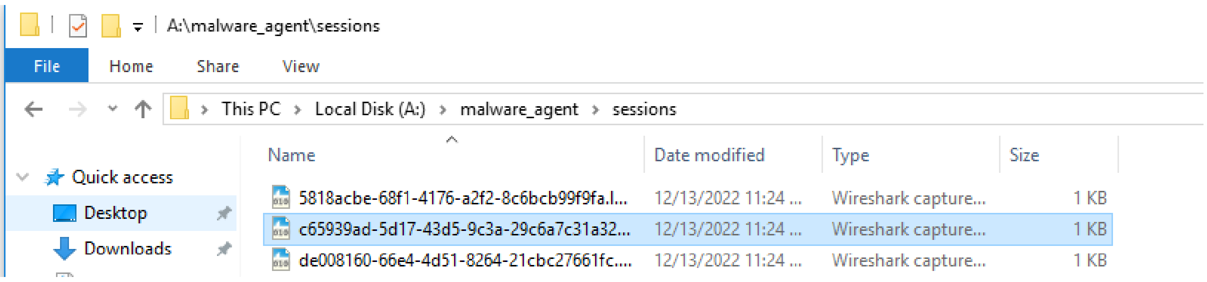
Name	Date modified	Type
sessions	12/13/2022 11:24 ...	File folder
AgentServer.cs	12/13/2022 11:24 ...	CS File

Looks like a C# code. Inside, there are private keys for something.



```
            }
        }

        private static string Encrypt(string pt)
        {
            string key = "AKaPdSgV";
            string iv = "QeThWmYq";
            byte[] keyBytes = Encoding.UTF8.GetBytes(key);
            byte[] ivBytes = Encoding.UTF8.GetBytes(iv);
            byte[] inputBytes = System.Text.Encoding.UTF8.GetBytes(pt);

            using (DESCryptoServiceProvider dsp = new DESCryptoServiceProvider())
            {
                var mstr = new MemoryStream();
                var crystr = new CryptoStream(mstr, dsp.CreateEncryptor(keyBytes, ivBytes), CryptoStreamMode.Write);
                crystr.Write(inputBytes, 0, inputBytes.Length);
                crystr.FlushFinalBlock();
                return Convert.ToBase64String(mstr.ToArray());
            }
        }
}
```

More files found:



A:\malware_agent\sessions

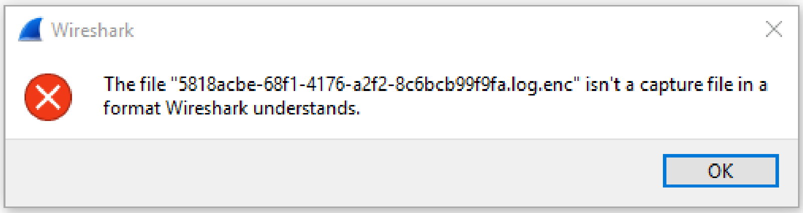
This PC > Local Disk (A:) > malware_agent > sessions

Name	Date modified	Type	Size
5818acbe-68f1-4176-a2f2-8c6bcb99f9fa.l...	12/13/2022 11:24 ...	Wireshark capture...	1 KB
c65939ad-5d17-43d5-9c3a-29c6a7c31a32...	12/13/2022 11:24 ...	Wireshark capture...	1 KB
de008160-66e4-4d51-8264-21cbc27661fc....	12/13/2022 11:24 ...	Wireshark capture...	1 KB

HTB Challenge - TrueSecrets -Subject: Forensics -Difficulty: Easy

Erel Regev

When trying to access the PCAP files I received the following error:

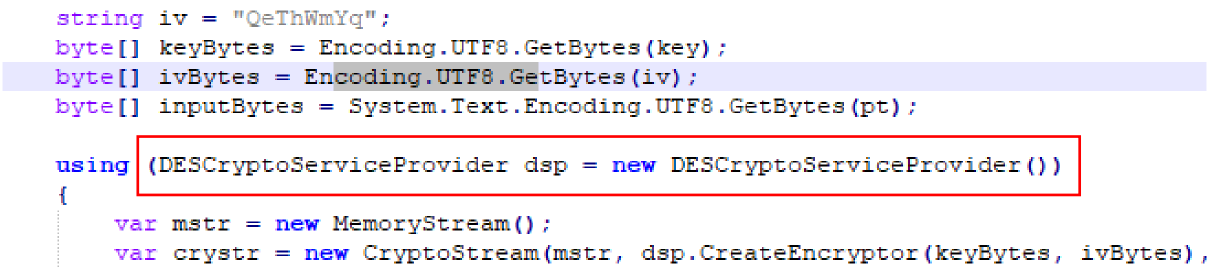

Wireshark

The file "5818acbe-68f1-4176-a2f2-8c6bcb99f9fa.log.enc" isn't a capture file in a format Wireshark understands.

OK

It looks like its an encrypted file (.enc). maybe the secret keys that were found in the C# code can help?

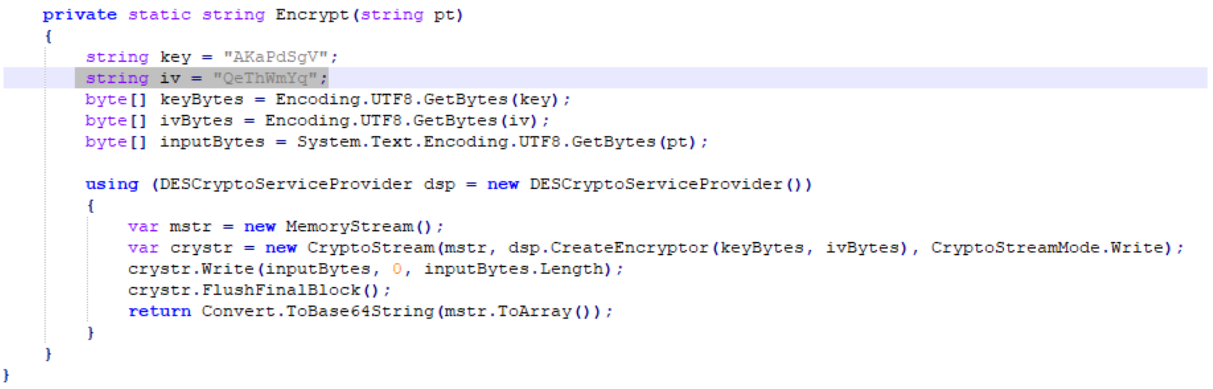
It is using the following service mentioned in the C# code:

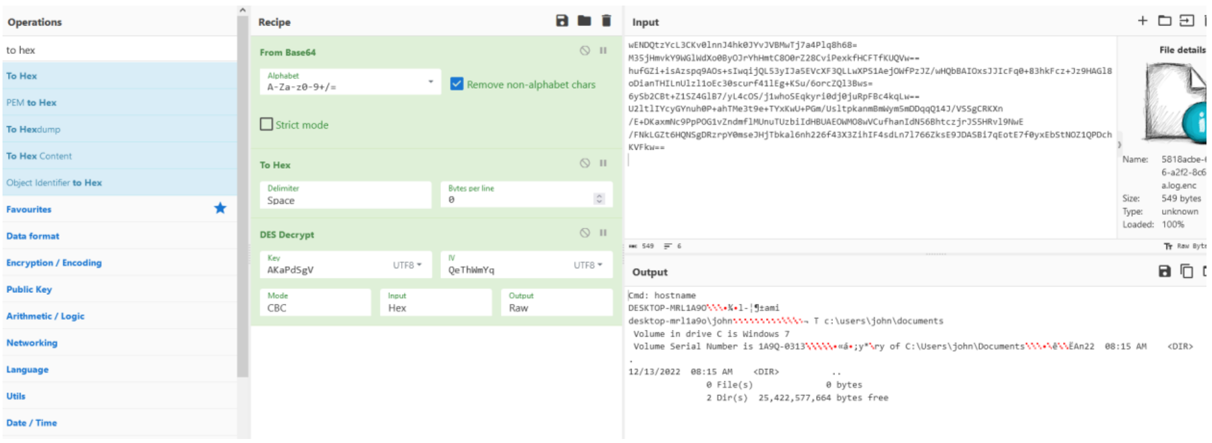

```
string iv = "QeThWmYq";
byte[] keyBytes = Encoding.UTF8.GetBytes(key);
byte[] ivBytes = Encoding.UTF8.GetBytes(iv);
byte[] inputBytes = System.Text.Encoding.UTF8.GetBytes(pt);

using (DESCryptoServiceProvider dsp = new DESCryptoServiceProvider())
{
    var mstr = new MemoryStream();
    var crystr = new CryptoStream(mstr, dsp.CreateEncryptor(keyBytes, ivBytes),
```

I used CyberChef for decryption:

Using the DES Decrypt Plugin and infront of that from base64 to hex plugins.

Using both of the secret keys found earlier in the C# code:


```
    private static string Encrypt(string pt)
    {
        string key = "AKaPdSgV";
        string iv = "QeThWmYq";
        byte[] keyBytes = Encoding.UTF8.GetBytes(key);
        byte[] ivBytes = Encoding.UTF8.GetBytes(iv);
        byte[] inputBytes = System.Text.Encoding.UTF8.GetBytes(pt);

        using (DESCryptoServiceProvider dsp = new DESCryptoServiceProvider())
        {
            var mstr = new MemoryStream();
            var crystr = new CryptoStream(mstr, dsp.CreateEncryptor(keyBytes, ivBytes), CryptoStreamMode.Write);
            crystr.Write(inputBytes, 0, inputBytes.Length);
            crystr.FlushFinalBlock();
            return Convert.ToBase64String(mstr.ToArray());
        }
    }
}
```



From Base64
Alphabet: A-Za-z0-9+/=
[✓] Remove non-alphabet chars
[ ] Strict mode

To Hex
Delimiter: Space
Bytes per line: 0

DES Decrypt
Key: AKaPdSgV UTF8
IV: QeThWmYq UTF8
Mode: CBC
Input: Hex
Output: Raw

Input
```
wENDQtzYcL3CKv0lnnJ4hk0JYvJVBMwTj7a4Plq8h68=
M35jHmvkY9WGlWdXo0ByOJrYhHmtC8O0rZ28CviPexkfHCFTfKUQVw==
hufGZi+isAzspq9AOs+sIwqijQL53yIJa5EVcXF3QLLwXPS1AejOWfPzJZ/wHQbBAIOxsJJIcFq0+83hkFcz+Jz9HAGl8
oDianTHILnUlzl1oEc30scurf41lEg+KSu/6orcZQl3Bws=
6ySb2CBt+Z1SZ4GlB7/yL4cOS/j1whoSEqkyri0dj0juRpFBc4kqLw==
U2ltlIYcyGYnuh0P+ahTMe3t9e+TYxKwU+PGm/UsltpkanmBmWym5mDDqqQ14J/VSSgCRKXn
/E+DKaxmNc9PpPOG1vZndmflMUnuTUzbiIdHBUAEOWMO8wVCufhanIdN56BhtczjrJS5HRvl9NwE
/FNkLGZt6HQNSgDRzrpY0mseJHjTbkal6nh226f43X3ZihIF4sdLn7l766ZksE9JDASBi7qEotE7f0yxEbStNOZ1QPDch
KVFkw==
```
549 6

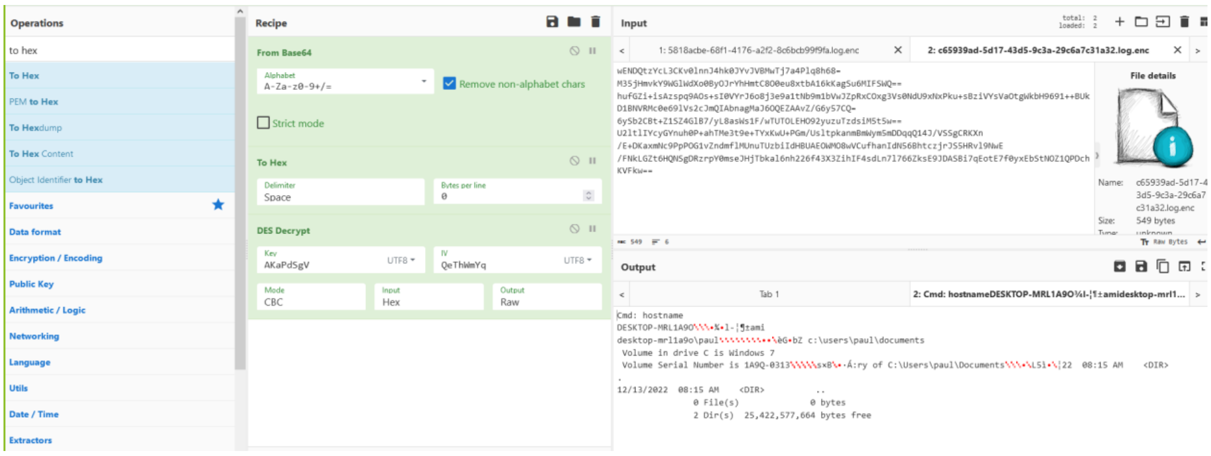
File details
Name: 5818acbe-6-a2f2-8c6 a.log.enc
Size: 549 bytes
Type: unknown
Loaded: 100%

Output
```
Cmd: hostname
DESKTOP-MRL1A9O\\\•¾•l-¦¶±ami
desktop-mrl1a9o\john\\\\\\\\\\\\\\¬ T c:\users\john\documents
 Volume in drive C is Windows 7
 Volume Serial Number is 1A9Q-0313\\\\\\•«á•;y*\ry of C:\Users\john\Documents\\\•\ê\\ËAn22  08:15 AM    <DIR>
.
12/13/2022  08:15 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  25,422,577,664 bytes free
```

File can be read. Before investigating the data, I will do the same process for the other 2 files:”

HTB Challenge - TrueSecrets -Subject: Forensics -Difficulty: Easy

Erel Regev


Recipe: From Base64 — Alphabet A-Za-z0-9+/= — Remove non-alphabet chars ✓ — Strict mode ☐; To Hex — Delimiter Space — Bytes per line 0; DES Decrypt — Key AKaPdSgV (UTF8) — IV QeThWmYq (UTF8) — Mode CBC — Input Hex — Output Raw

Input: 1: 5818acbe-68f1-4176-a2f2-8c6bcb99f9fa.log.enc — 2: c65939ad-5d17-43d5-9c3a-29c6a7c31a32.log.enc

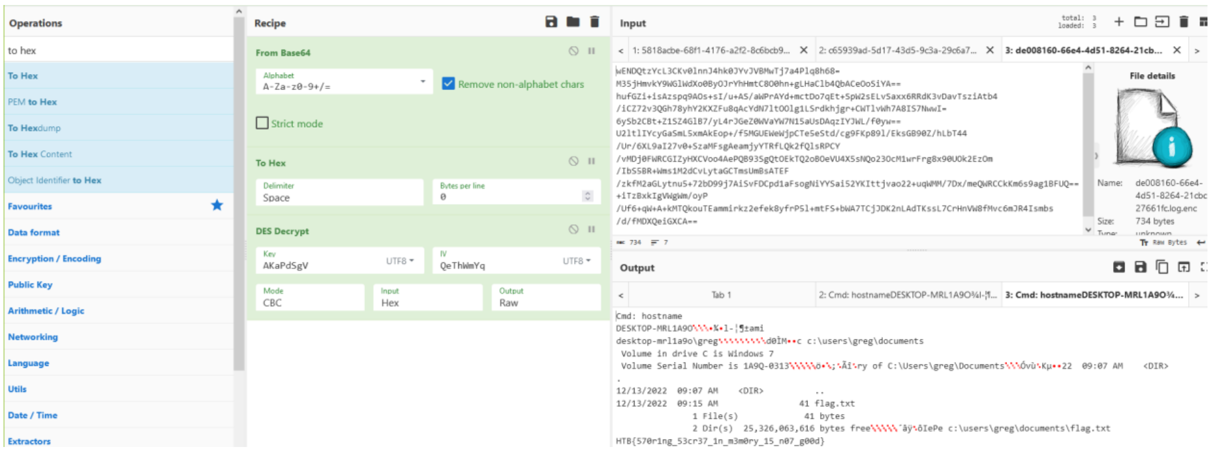
```
wENDQtzYcL3CKv0lnnJ4hk0JYvJVBMwTj7a4Plq8h68=
M35jHmvkY9WGlWdXo0ByOJrYhHmtC8O0eu8xtbA16kKagSu6MIFSWQ==
hufGZi+isAzspq9AOs+sI0VYrJ6o8j3e9a1tNb9m1bVwJZpRxCOxg3Vs0NdU9xNxPku+sBziVYsVaOtgWkbH9691++BUk
D1BNVRMc0e69lVs2cJmQIAbnagMaJ6OQEZAAvZ/G6y57CQ=
6ySb2CBt+Z1SZ4GlB7/yL8asWs1F/wTUTOLEHO92yuzuTzdsiM5t5w==
U2ltlIYcyGYnuh0P+ahTMe3t9e+TYxKwU+PGm/UsltpkanmBmWym5mDDqqQ14J/VSSgCRKXn
/E+DKaxmNc9PpPOG1vZndmflMUnuTUzbiIdHBUAEOWMO8wVCufhanIdN56BhtczjrJS5HRvl9NwE
/FNkLGZt6HQNSgDRzrpY0mseJHjTbkal6nh226f43X3ZihIF4sdLn7l766ZksE9JDASBi7qEotE7f0yxEbStNOZ1QPDch
KVFkw==
```

File details — Name: c65939ad-5d17-43d5-9c3a-29c6a7c31a32.log.enc — Size: 549 bytes

Output: Tab 1 — 2: Cmd: hostnameDESKTOP-MRL1A9O¾l-¦¶±amidesktop-mrl1...

```
Cmd: hostname
DESKTOP-MRL1A9O•%•l-¦¶±ami
desktop-mrl1a9o\paul••èG•bZ c:\users\paul\documents
 Volume in drive C is Windows 7
 Volume Serial Number is 1A9Q-0313sxB•·Á:ry of C:\Users\paul\Documents•L5i•¦22  08:15 AM    <DIR>
.
12/13/2022  08:15 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  25,422,577,664 bytes free
```

And the last one:


Recipe: From Base64 — Alphabet A-Za-z0-9+/= — Remove non-alphabet chars ✓ — Strict mode ☐; To Hex — Delimiter Space — Bytes per line 0; DES Decrypt — Key AKaPdSgV (UTF8) — IV QeThWmYq (UTF8) — Mode CBC — Input Hex — Output Raw

Input: 1: 5818acbe-68f1-4176-a2f2-8c6bcb9... — 2: c65939ad-5d17-43d5-9c3a-29c6a7... — 3: de008160-66e4-4d51-8264-21cb...

```
wENDQtzYcL3CKv0lnnJ4hk0JYvJVBMwTj7a4Plq8h68=
M35jHmvkY9WGlWdXo0ByOJrYhHmtC8O0hn+gLHaClb4QbACeOoSiYA==
hufGZi+isAzspq9AOs+sI/u+AS/aWPrAYd+mctDo7qEt+SpW2sELvSaxx6RRdK3vDavTsziAtb4
/iCZ72v3QGh78yhY2KXZFu8qAcYdN7ltOOlg1LSrdkhjgr+CWTlvWh7A8IS7NwwI=
6ySb2CBt+Z1SZ4GlB7/yL4rJGeZ0WVaYW7N15aUsDAqzIYJWL/f0yw==
U2ltlIYcyGaSmL5xmAkEop+/f5MGUEWeWjpCTe5eStd/cg9FKp89l/EksGB90Z/hLbT44
/Ur/6XL9aI27v0+SzaMFsgAeamjyYTRfLQk2fQlsRPCY
/vMDj0FWRCGIZyHXCVoo4AePQB93SgQtOEkTQ2oBOeVU4X5sNQo23OcM1wrFrg8x90UOk2EzOm
/IbS5BR+Wms1M2dCvLytaGCTmsUmBsATEF
/zkfM2aGLytnu5+72bD99j7AiSvFDCpd1aFsogNiYYSai52YKIttjvao22+uqWMM/7Dx/meQWRCCkKm6s9ag1BFUQ==
+iTzBxkIgVWgWm/oyP
/Uf6+qW+A+kMTQkouTEammirkz2efek8yfrP5l+mtFS+bWA7TCjJDK2nLAdTKssL7CrHnVW8fMvc6mJR4Ismbs
/d/fMDXQeiGXCA==
```

File details — Name: de008160-66e4-4d51-8264-21cbc27661fc.log.enc — Size: 734 bytes

Output: Tab 1 — 2: Cmd: hostnameDESKTOP-MRL1A9O¾l-¦¶... — 3: Cmd: hostnameDESKTOP-MRL1A9O¾...

```
Cmd: hostname
DESKTOP-MRL1A9O•%•l-¦¶±ami
desktop-mrl1a9o\gregd0İM••c c:\users\greg\documents
 Volume in drive C is Windows 7
 Volume Serial Number is 1A9Q-0313ö•;Ãí•ry of C:\Users\greg\DocumentsŐvù•Kµ••22  09:07 AM    <DIR>
.
12/13/2022  09:07 AM    <DIR>          ..
12/13/2022  09:15 AM                41 flag.txt
               1 File(s)             41 bytes
               2 Dir(s)  25,326,063,616 bytes free¨ãÿ•õIePe c:\users\greg\documents\flag.txt
HTB{570r1ng_53cr37_1n_m3m0ry_15_n07_g00d}
```

Flag found.

Conclusion