



IBM X-Force如何抵御未知威胁

李承达 IBM全球首席资讯安全架构师



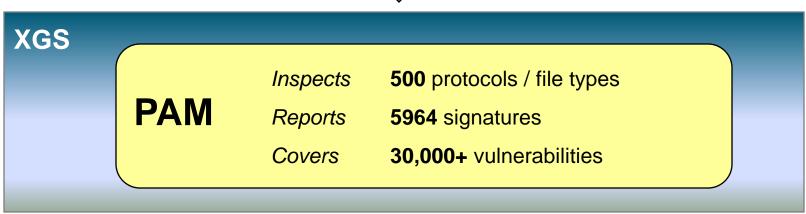


What is PAM?

- The Protocol Analysis Module (PAM) is at the core of many IBM security products
 XGS next-generation intrusion prevention system (IPS)
- PAM uses Deep Packet Inspection (DPI) to thoroughly inspect packets at wire speed
 processes up to 25 Gbps on the XGS 7100 appliance.

network traffic





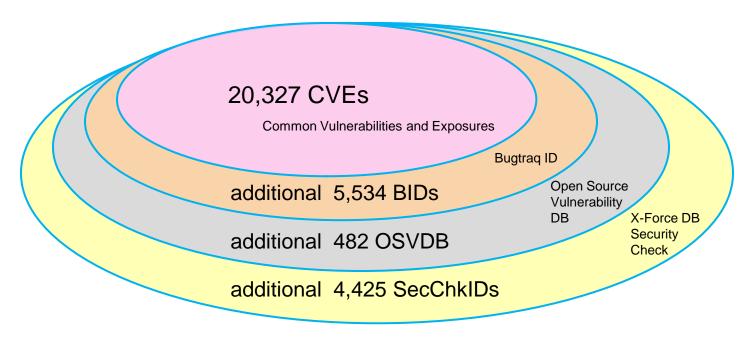


approved network traffic



PAM does more with less

5,459 attack signatures* cover 30,000+ vulnerabilities as of March 2016



^{*} PAM also contains 497 audit signatures and 8 status signatures

<u>Leading industry analysts recently commented</u>:

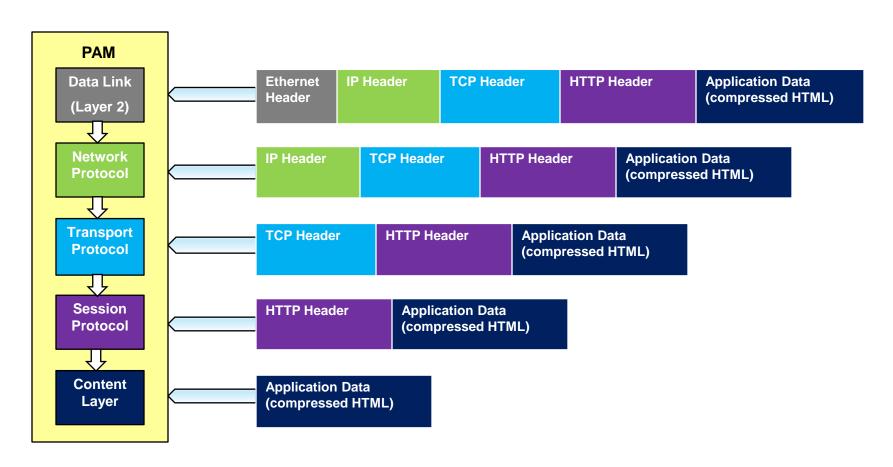
IBM's Protocol Analysis Module (PAM) is still leading the market in its ability to provide low false positives and protection for entire classes of vulnerabilities, with the smallest number of signatures on the market.





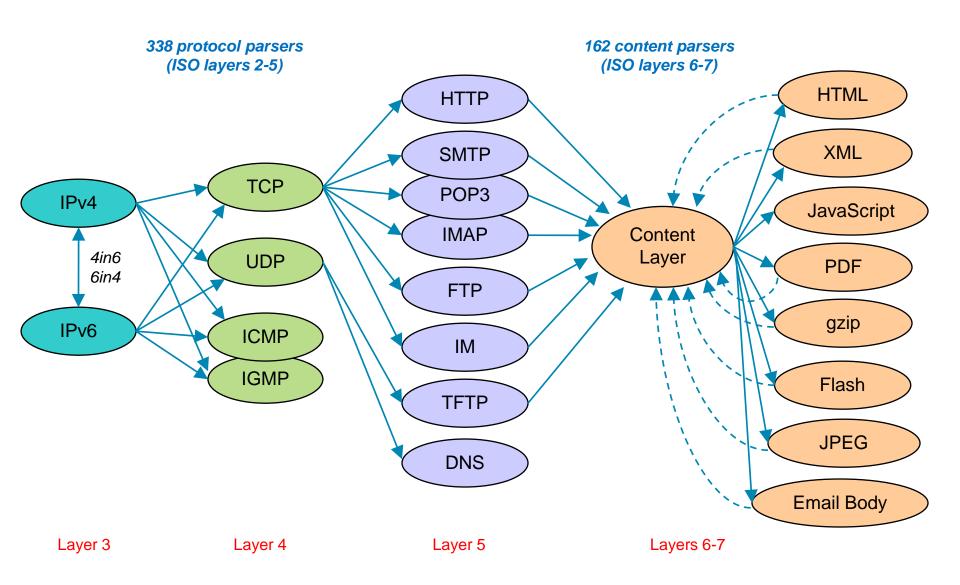
PAM parses each frame, layer by layer

- Deep Packet Inspection continues to the end of the packet in a stateful manner
- PAM signatures may trigger while parsing any layer (2-7)
- Multiple signatures may trigger on the same packet



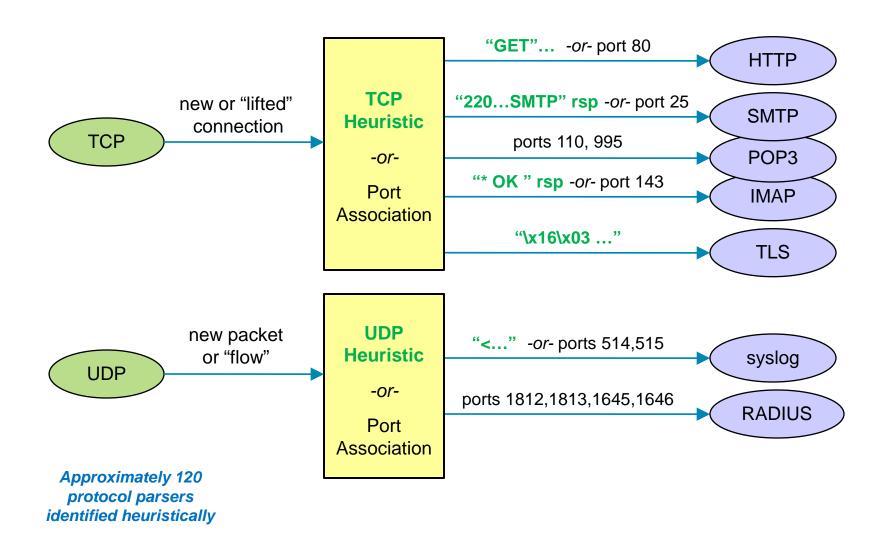


PAM Parser Overview





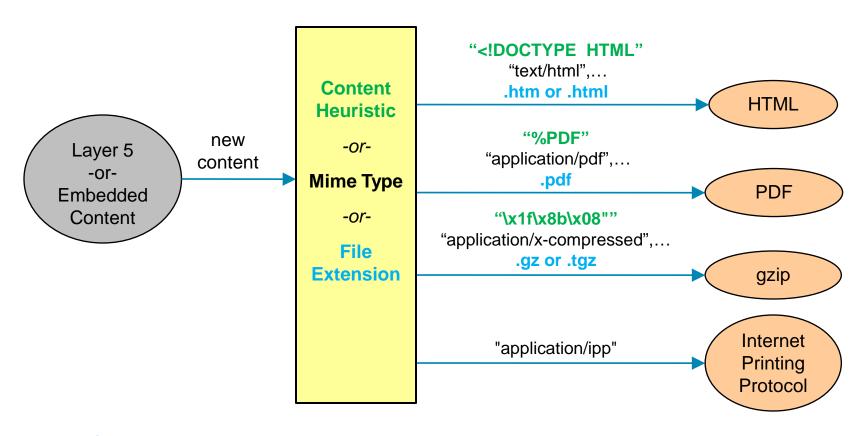
PAM Protocol Heuristics (layer 5)



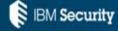




PAM Content Heuristics (layer 6-7)



Approximately 130 content parsers identified heuristically





Example of Deep Packet Inspection (1 of 5)

HTTP 200 response transmitted in 99 TCP segments (packets) over IPv4

```
Frame 268: 749 bytes on wire (5992 bits), 749 bytes captured (5992 bits)
Ethernet II, Src: MarvellS 00:6f:52 (00:50:43:00:6f:52), Dst: BuffaloI 3f:88:a7 (4c:e6:76:3f:88:a7)
Internet Protocol Version 4, Src: 10.1.1.2, Dst: 46.246.42.9
🕀 Transmission Control Protocol, Src Port: http (80), Dst Port: 49825 (49825), Seq: 2719545807, Ack: 3626752787, Len: 695
🕀 [99 Reassembled TCP Segments (398538 bytes): #6(8112), #7(355), #8(4056), #11(8112), #14(8112), #17(8112), #20(8112), #23(8112), #2...
Hypertext Transfer Protocol
  Date: Inu, 26 Sep 2013 02:24:54 UMI\r\n
     <Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n>
     Server: Apache/2.4.6 (Debian)\r\n
     Transfer-Encoding: chunked\r\n
     <Transfer-Encoding: chunked\r\n>
     Content-Type: application/pdf\r\n
     <Content-Type: application/pdf\r\n>
    \r\n
     <Response: True>
     [HTTP response 1/1]
     [Time since request: 9.320314000 seconds]
     [Request in frame: 4]
   HTTP chunked response
     Content-encoded entity body (gzip): 397812 bytes -> 91012590 bytes
Media type: application/pdf (91012590 bytes)
```





Example of Deep Packet Inspection (2 of 5)

The HTTP response uses Chunked Encoding dividing the payload into 46 chunks.

```
Transfer-Encoding: chunked\r\n
  <Transfer-Encoding: chunked\r\n>
  Content-Type: application/pdf\r\n
  <Content-Type: application/pdf\r\n>
  \r\n
  <Response: True>
  [HTTP response 1/1]
  [Time since request: 9.320314000 seconds]
  [Request in frame: 4]
⊟ HTTP chunked response
  ⊕ Data chunk (8106 octets)
  ⊕ Data chunk (8096 octets)
  ± Data chunk (8096 octets)
  ⊕ Data chunk (8096 octets)
  ⊕ Data chunk (8096 octets)
  ± Data chunk (8096 octets)
  ⊕ Data chunk (8096 octets)
  ± Data chunk (8096 octets)
  Data chunk (8096 octets)
  ⊕ Data chunk (8096 octets)
  ⊕ Data chunk (8096 octets)
  Data chunk (8096 octets)
  ⊕ Data chunk (8096 octets)
  Data chunk (8096 octets)
```



Example of Deep Packet Inspection (3 of 5)

The HTTP "chunked" payload is compressed in gzip format!

```
Frame 268: 749 bytes on wire (5992 bits), 749 bytes captured (5992 bits)
Ethernet II, Src: MarvellS 00:6f:52 (00:50:43:00:6f:52), Dst: BuffaloI 3f:88:a7 (4c:e6:76:3f:88:a7)
• Internet Protocol Version 4, Src: 10.1.1.2, Dst: 46.246.42.9
🕀 Transmission Control Protocol, Src Port: http (80), Dst Port: 49825 (49825), Seq: 2719545807, Ack: 3626752787, Len: 695
🕒 [99 Reassembled TCP Segments (398538 bytes): #6(8112), #7(355), #8(4056), #11(8112), #14(8112), #17(8112), #20(8112), #23(8112), #2...
Hypertext Transfer Protocol
  Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n
     <Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n>
     Server: Apache/2.4.6 (Debian)\r\n
    Transfer-Encoding: chunked\r\n
     <Transfer-Encoding: chunked\r\n>
     Content-Type: application/pdf\r\n
     <Content-Type: application/pdf\r\n>
     \r\n
     <Response: True>
     [HTTP response 1/1]
     [Time since request: 9.320314000 seconds]
     [Request in frame: 4]
   ⊕ HTTP chunked response
     Content-encoded entity body (gzip): 397812 bytes -> 91012590 bytes
    Media type: application/pdf (91012590 bytes)
```





Example of Deep Packet Inspection (4 of 5)

The content of the gzip compressed payload is a PDF file.

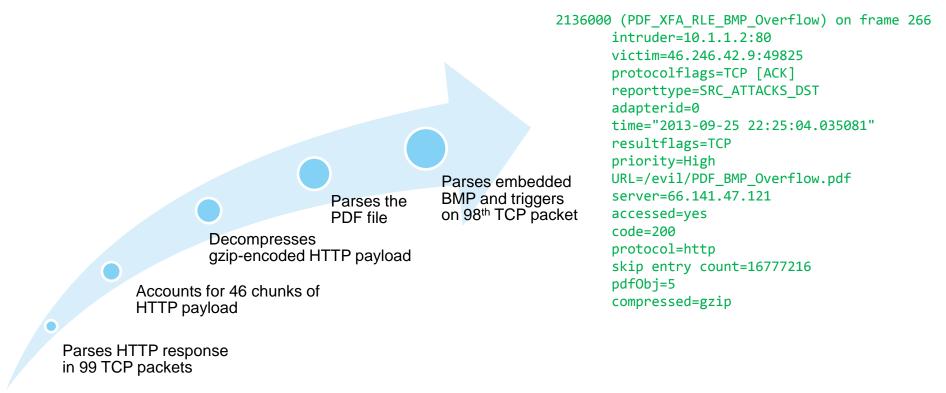
```
Frame 268: 749 bytes on wire (5992 bits), 749 bytes captured (5992 bits)
Ethernet II, Src: MarvellS 00:6f:52 (00:50:43:00:6f:52), Dst: BuffaloI 3f:88:a7 (4c:e6:76:3f:88:a7)
• Internet Protocol Version 4, Src: 10.1.1.2, Dst: 46.246.42.9
🕀 Transmission Control Protocol, Src Port: http (80), Dst Port: 49825 (49825), Seq: 2719545807, Ack: 3626752787, Len: 695
🕒 [99 Reassembled TCP Segments (398538 bytes): #6(8112), #7(355), #8(4056), #11(8112), #14(8112), #17(8112), #20(8112), #23(8112), #2...
Hypertext Transfer Protocol
  Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n
     <Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n>
     Server: Apache/2.4.6 (Debian)\r\n
     Transfer-Encoding: chunked\r\n
     <Transfer-Encoding: chunked\r\n>
     Content-Type: application/pdf\r\n
     <Content-Type: application/pdf\r\n>
     <Response: True>
     [HTTP response 1/1]
     [Time since request: 9.320314000 seconds]
     [Request in frame: 4]
   Content-encoded entity hody (gzin): 397812 hytes -> 91012590 hytes
⊟ Media Type
   Media type: application/pdf (91012590 bytes)
```





Example of Deep Packet Inspection (5 of 5)

Hidden in the PDF file is a malicious .bmp image file, which PAM catches



Ahead of the Threat (AOTT)

OVERVIEW AND EXAMPLES





Ahead of The Threat (AOTT)

AOTT – pre-existing coverage for a vulnerability on the day it is publicly reported



Criteria for AOTT items in this presentation:

- 1. At least 90 days of pre-existing PAM coverage
- 2. Default Blocked if using "Trust X-Force"
- 3. Notable vendor (e.g. Microsoft, Adobe, HP, Oracle)
- 4. Recent 2012 to present
- 5. CVSS base score 5 or higher



X-Force Top 100 Ahead of the Threat Coverage

Blocking coverage at least 90 days ahead of the threat for notable vendors since 2012 with CVSS >=5

Average AOTT = 3.8 yrs

Average CVSS base = 8.6

Adobe		Google		Microsoft (co	int)	Novell	
CVE-2015-5097	E 1 1/10	CVE-2015-3864	8.4 yrs	CVE-2014-6343			2.0
CVE-2015-5097 CVE-2014-8438	5.1 yrs	CVE-2015-3829	8.3 yrs	CVE-2014-6343 CVE-2014-6332	3.6 yrs	CVE-2015-0779	3.0 yrs
	7.6 yrs	CVE-2015-3828	8.3 yrs		0.4 yrs	CVE-2012-0271	0.6 yrs
CVE-2013-3346	1.3 yrs	CVE-2015-3827	6.5 yrs	CVE-2014-2799	0.5 yrs	NED	
CVE-2013-2729	7.2 yrs	CVE-2015-3827 CVE-2015-3826		CVE-2014-2797	0.7 yrs	NTP	
CVE-2013-2555	0.7 yrs	CVE-2015-3824	8.3 yrs	CVE-2014-1811	4.8 yrs	CVE-2013-5211	0.5 yrs
CVE-2013-0634	1.8 yrs		8.3 yrs	CVE-2014-1761	1.3 yrs		
CVE-2012-4170	7.5 yrs	CVE-2015-1539	8.3 yrs	CVE-2013-3906	1.2 yrs	Oracle	
CVE-2012-1535	1.4 yrs	CVE-2015-1538	8.3 yrs	CVE-2013-3893	0.7 yrs	CVE-2013-2465	0.8 yrs
CVE-2012-0769	0.9 yrs	BID-52632	7.0 yrs	CVE-2013-3163	0.5 yrs	CVE-2013-2463	0.8 yrs
CVE-2012-0768	0.9 yrs			CVE-2013-1331	3.7 yrs	CVE-2013-2431	8.2 yrs
BID-52632	7.0 yrs	HP		CVE-2013-1347	2.6 yrs	CVE-2013-0431	0.3 yrs
		CVE-2014-7883	1.1 yrs	CVE-2013-1313	0.5 yrs	CVE-2013-0422	7.9 yrs
Apache		CVE-2014-2625	9.4 yrs	CVE-2013-0026	6.9 yrs	BID-56791	1.5 yrs
CVE-2013-2251	2.4 yrs	CVE-2014-2621	1.1 yrs	CVE-2013-0025	6.9 yrs	BID-56772	1.6 yrs
CVE-2013-2135	2.3 yrs	CVE-2014-2620	1.2 yrs	CVE-2012-4781	6.7 yrs	CVE-2012-3342	0.3 yrs
CVE-2013-2134	2.3 yrs	CVE-2014-2617	1.9 yrs	CVE-2012-2522	0.8 yrs	OVE 2012 3342	0.5 yrs
CVE-2013-2115	2.3 yrs	CVE-2013-6195	0.3 yrs	CVE-2012-1891	1.5 yrs	PHP	
CVE-2013-1966	2.3 yrs	CVE-2013-4799	5.9 yrs	CVE-2012-1879	6.2 yrs		
CVE-2012-0838	1.0 yrs	CVE-2012-5201	6.8 yrs	CVE-2012-1878	6.2 yrs	CVE-2015-4022	7.2 yrs
CVE-2012-0391	0.9 yrs		•	CVE-2012-1876	6.2 yrs	CVE-2014-4049	5.5 yrs
012 2012 0001	0.0).0	Microsoft		CVE-2012-1875	6.2 yrs		
Apple		CVE-2016-0103	0.8 yrs	CVE-2012-0171	6.1 yrs	Power DNS	
	0.0		,	CVE-2012-0170	6.1 yrs	CVE-2015-1868	10.2 yrs
CVE-2012-3753	0.8 yrs	CVE-2015-6143	0.5 yrs	CVE-2012-0169	6.1 yrs		,
		CVE-2015-6142	0.5 yrs	CVE-2012-0159	1.6 yrs	Samba	
CA		CVE-2015-6150	1.4 yrs	CVE-2012-0158	2.7 yrs	CVE-2014-0239	0.8 yrs
BID-51915	7.0 yrs	CVE-2015-6087	4.6 yrs	CVE-2012-0155	5.9 yrs	CVE-2014-0239	0.6 yrs
	•	CVE-2015-2464	3.3 yrs	CVE-2012-0016	1.1 yrs	0. 11	
GNU		CVE-2015-2461	4.7 yrs	CVE-2012-0011	5.9 yrs	Squid	
CVE-2015-0235	9.9 yrs	CVE-2015-2397	1.7 yrs	CVE-2012-0003	0.3 yrs	CVE-2013-4115	8.4 yrs
O V L 2013-0233	0.0 yi3	CVE-2015-1662	4.0 yrs				
ISC		CVE-2015-1002 CVE-2015-0090	1.4 yrs	NGINX			
ISC		CVE-2015-0090 CVE-2015-0086		CVE-2014-3556	3.1 yrs		
CVE-2012-3571	1.9 yrs		4.6 yrs	CVE-2013-2070	8.2 yrs		
CVE-2012-3523	1.2 yrs	CVE-2014-6369	1.1 yrs	-	•		





X-Force Top 100 Ahead of the Threat Coverage

Blocking coverage at least 90 days ahead of the threat for notable vendors since 2012 with CVSS >=5

Let's look at 4 examples

Average AOTT = 3.8 yrs

Average CVSS base = 8.6

Adobe OUE-2015-5607 OUE-2014-8438 OUE-2014-8438 OUE-2014-8438 OUE-2015-3829 OUE-2014-7829 OUE-2014-7879 OUE-2014-7881 OUE-2014-7881 OUE-2014-7881 OUE-2014-7881 OUE-2014-7881 OUE-2013-3893 OUE-2013-3									
CVE-2014-8438 7.6 yrs CVE-2013-3345 1.3 yrs CVE-2013-3245 1.3 yrs CVE-2013-3245 1.3 yrs CVE-2013-3245 1.3 yrs CVE-2013-3255 0.7 yrs CVE-2013-2555 0.5 yrs	Adobe		Google			Microsoft (co	ont)	Novell	
CVE-2014-8438 7.6 /yrs CVE-2013-3348 1.3 /yrs CVE-2013-2725 0.7 yrs CVE-2012-1535 1.4 yrs CVE-2012-20768 0.9 yrs BID-52632 7.0 yrs CVE-2014-2625 9.4 yrs CVE-2013-2135 0.5 yrs CVE-2013-2135 0.3 yrs CVE-2014-2625 9.4 yrs CVE-2013-2135 0.3 yrs C	_CVE-2015-5097	5.1 vrs		8.4 vrs	_				3.0 vrs
CVE-2013-32346 1.3 yrs CVE-2013-3286 8.3 yrs CVE-2013-2797 0.7 yrs CVE-2013-2555 0.7 yrs QuickTime CVE-2013-0634 1.8 yrs Protocol CVE-2012-4170 7.5 yrs CVE-2014-1761 1.3 yrs CVE-2013-383 1.4 yrs anomaly CVE-2015-1538 8.3 yrs CVE-2013-3896 1.2 yrs CVE-2013-3896 1.2 yrs CVE-2012-0768 0.9 yrs CVE-2015-1538 8.3 yrs CVE-2013-3896 1.2	CVF-2014-8438	7.6 vrs				CVF-2014-6332	0.4 vrs		
CVE-2013-2729 7:2 yrs CVE-2013-2729 7:2 yrs CVE-2013-2729 7:2 yrs CVE-2013-2555 0.7 yrs QuickTime CVE-2013-2556 0.7 yrs QuickTime CVE-2012-4170 7.5 yrs CVE-2012-1535 1.8 yrs CVE-2012-1535 1.8 yrs CVE-2012-1538 1.8 yrs CVE-2012-1538 1.4 yrs CVE-2012-0768 0.9 yrs BID-52632 7.0 yrs BID-52632 7.0 yrs BID-52632 7.0 yrs CVE-2013-2251 2.4 yrs CVE-2014-2625 9.4 yrs CVE-2013-2251 2.4 yrs CVE-2014-2626 1.1 yrs CVE-2013-2251 2.3 yrs CVE-2014-2626 1.2 yrs CVE-2013-2134 2.3 yrs CVE-2013-2135 2.3 yrs CVE-2013-2135 2.3 yrs CVE-2013-2135 2.3 yrs CVE-2013-2136 2.3 yrs CVE-2013-2136 2.3 yrs CVE-2013-2136 2.3 yrs CVE-2013-2139 0.9 yrs CVE-2013-2139 0.9 yrs CVE-2012-3893 1.0 yrs CVE-2013-2131 0.5 yrs CVE-2013-2463 0.8 yrs CVE-2013-2434 2.3 yrs CVE-2013-2134 2.3 yrs CVE-2013-2135 2.3 yrs CVE-2013-2136 2.3 yrs CVE-2013-2136 2.3 yrs CVE-2013-2136 2.3 yrs CVE-2013-2139 0.9 yrs CVE-2012-3893 1.0 yrs CVE-2012-3893 0.9 yrs CVE-2012-3893 0.9 yrs CVE-2012-2893 1.0 yrs CVE-2012-3893 0.9 yrs CVE-2012-2893 1.0 yrs CVE-2012-3893 0.9 yrs CVE-2012-3896 0.3 yrs CVE-2012-3996			CVE-2015-3828		•			0.12.0.2.02	0.0).0
CVE-2013-2555			CVE-2015-3827					NTP	
CVE-2013-0634 1.8 yrs		0.7 vrs QuickTime					4.8 vrs VBScript		0.5 vrc
CVE-2012-4170 7.5 yrs		4.0	CVE-2015-3824				4.0	CVL-2013-3211	0.5 yrs
CVE-2012-1535	CVE-2012-4170		CVE-2015-1539			CVE-2013-3906	1.2 yrs X-Force	Oracle	
CVE-2012-0768 0.9 yrs BID-52632 7.0 yrs CVE-2013-3133 3.7 yrs CVE-2013-2431 8.2 yrs CVE-2013-2251 2.4 yrs CVE-2014-2625 9.4 yrs CVE-2013-0026 6.9 yrs CVE-2013-0431 0.3 yrs CVE-2013-2335 2.3 yrs CVE-2014-2620 1.2 yrs CVE-2013-2435 2.3 yrs CVE-2014-2620 1.2 yrs CVE-2013-2413 2.3 yrs CVE-2013-2462 2.3 yrs CVE-2014-2617 1.9 yrs CVE-2013-2415 2.3 yrs CVE-2013-2415 2.3 yrs CVE-2013-2469 2.3 yrs CVE-2013-2469 2.3 yrs CVE-2012-0838 1.0 yrs CVE-2012-0838 1.0 yrs CVE-2012-0838 1.0 yrs CVE-2012-0391 0.9 yrs CVE-2012-0391 0.9 yrs CVE-2012-6142 0.5 yrs CVE-2012-1875 6.2 yrs CVE-2012-1876 6.2 yrs CV	CVE-2012-1535		CVE-2015-1538	8.3 yrs		CVE-2013-3893			0.0
CVE-2012-0768 BID-52632 7.0 yrs BID-52632 7.0 yrs BID-52632 7.0 yrs Apache CVE-2014-7883 1.1 yrs CVE-2013-3131 0.5 yrs CVE-2013-0431 0.5 yrs CVE-2013-0432 0.9 yrs CVE-2013-0425 0.9 yrs BID-56791 1.5 yrs CVE-2013-0426 0.9 yrs BID-56791 1.5 yrs CVE-2013-0421 0.7 yrs CVE-2013-0421 0.7 yrs CVE-2013-0431 0.8 yrs CVE-2012-4781 0.7 yrs CVE-2012-4781 0.7 yrs CVE-2012-4781 0.7 yrs CVE-2012-4781 0.7 yrs CVE-2012-4891 0.9 yrs CVE-2012-1876 0.2 yr	CVE-2012-0769	0.9 yrs	BID-52632	7.0 yrs		CVE-2013-3163	0.5 yrs find		
Apache CVE-2013-2251 2.4 yrs CVE-2013-2251 2.3 yrs CVE-2013-2251 2.3 yrs CVE-2013-2134 2.3 yrs CVE-2013-2135 2.3 yrs CVE-2013-2134 2.3 yrs CVE-2013-2155 2.3 yrs CVE-2013-2155 2.3 yrs CVE-2013-2155 2.3 yrs CVE-2013-2159 2.3 yrs CVE-2013-2015 2.3 yrs CVE-2013-2015 2.3 yrs CVE-2013-2020 2.2 yrs CVE-2012-1889 2.7 yrs CVE-2012-1876 2	CVE-2012-0768	0.9 yrs		•		CVE-2013-1331	3.7 yrs		
Apache CVE-2014-7883 1.1 yrs CVE-2013-0226 6.9 yrs CVE-2012-4781 6.7 yrs CVE-2012-4781 6.2 yrs CVE-2012-4781	BID-52632	7.0 yrs	HP			CVE-2013-1347	2.6 yrs		
Apache CVE-2013-2251		•		1 1 vrs		CVE-2013-1313	0.5 yrs		
CVE-2013-2251 2.4 yrs CVE-2013-2252 2.3 yrs CVE-2013-2135 2.3 yrs CVE-2013-2135 2.3 yrs CVE-2013-2135 2.3 yrs CVE-2013-2136 2.3 yrs CVE-2013-6195 0.3 yrs CVE-2012-1896 2.3 yrs CVE-2012-3753 0.8 yrs CVE-2012-3753 0.8 yrs CVE-2015-6143 0.5 yrs CVE-2012-0375 0.8 yrs CVE-2015-6143 0.5 yrs CVE-2012-0155 6142 0.5 yrs CVE-2012-0155 5.9 yrs CVE-2012-0155 0.9 yrs CVE-2012-0155 5.9 yrs CVE-2012-0003 0.3 yrs CVE-2012-0003 0.3 yrs CVE-2012-0003 0.8 yrs CVE-2013-0086 4.6 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2013-0086 3.1 yrs CVE-2013-0086 4.6 yrs CVE-2013-0086 4.6 yrs CVE-2013-0086 3.1 yrs CVE-2013-0086 4.6 yrs CVE-2013-0086 3.1 yrs CVE-2013-0086 4.6 yrs CVE-2013-0086 3.1 yrs CVE-2013-0086 4.6 yrs CVE-2013-0086 3.1 yrs CVE-2013-0086 4.6 yrs CVE-2013-0086 6.2 yrs CVE-2013-0086 6.2 yrs CVE-2013-0086 6.2	Anache				<u>ZIP</u>				
CVE-2013-2135		2.4 yre			History				
CVE-2013-2134 2.3 yrs CVE-2013-2115 2.3 yrs CVE-2013-1966 2.3 yrs CVE-2012-0838 1.0 yrs CVE-2012-0838 1.0 yrs CVE-2012-0391 0.9 yrs CVE-2012-3753 0.8 yrs CVE-2015-6150 1.4 yrs CVE-2015-0235 9.9 yrs CVE-2015-2464 3.3 yrs CVE-2015-2464 4.7 yrs CVE-2015-0235 9.9 yrs CVE-2015-1662 4.0 yrs CVE-2015-1662 4.0 yrs CVE-2015-1662 4.0 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2012-3573 0.8 yrs CVE-2012-3576 0.2 yrs CVE-2012-1876 6.2 yr				1.2 vrc	-				
CVE-2013-2115 2.3 yrs CVE-2013-6195 0.3 yrs CVE-2012-1891 0.5 yrs CVE-2012-1896 0.2 yrs CVE-2012-0838 1.0 yrs CVE-2012-0391 0.9 yrs CVE-2012-0391 0.9 yrs CVE-2012-3753 0.8 yrs CVE-2015-6143 0.5 yrs CVE-2012-0170 6.1 yrs CVE-2012-0169 6.1 yr					epeats			CVE-2012-3342	0.3 yrs
CVE-2013-1966 2.3 yrs CVE-2012-0838 1.0 yrs CVE-2012-0391 0.9 yrs CVE-2012-0391 0.9 yrs CVE-2012-5201 6.8 yrs CVE-2012-1876 6.2 yrs CVE-2012-0171 6.1 yrs CVE-2012-0171 6.1 yrs CVE-2012-0170 6.1 yrs CVE-2012-0169 6.1 yrs CVE-2012-0155 5.9 yrs CVE-2012-0155 5.9 yrs CVE-2012-0155 5.9 yrs CVE-2012-0016 1.1 yrs CVE-2012-0010 1.9 yrs CVE-2012-0003 0.3 yrs CVE-2013-4115 8.4 yrs CVE-2013-4115 8.4 yrs CVE-2013-2070 8.2 yrs			CVE-2013-6195					DUD	
CVE-2012-0838			CVF-2013-4799	5 9 vrs					
CVE-2012-0391 0.9 yrs Microsoft CVE-2012-1876 6.2 yrs CVE-2012-1875 6.2 yrs CVE-2012-1875 6.2 yrs CVE-2012-1875 6.2 yrs CVE-2012-0171 6.1 yrs CVE-2012-0170 6.1 yrs CVE-2012-0170 6.1 yrs CVE-2015-6143 0.5 yrs CVE-2012-0169 6.1 yrs CVE-2015-6142 0.5 yrs CVE-2012-0169 6.1 yrs CVE-2012-0169 6.1 yrs CVE-2015-1868 10.2 yrs CVE-2012-0159 1.6 yrs CVE-2012-0159 2.7 yrs CVE-2012-0155 5.9 yrs CVE-2012-0155 5.9 yrs CVE-2012-0016 1.1 yrs CVE-2015-2464 3.3 yrs CVE-2015-2461 4.6 yrs CVE-2012-0016 1.1 yrs CVE-2012-0003 0.3 yrs CVE-2013-4115 8.4 yrs CVE-2013-2070 8.2 yrs CVE-2013-2070			CVE-2012-5201	6.8 yrs					
Apple CVE-2012-1875 6.2 yrs CVE-2012-0171 6.1 yrs PowerDNS CVE-2012-3753 0.8 yrs CVE-2015-6143 0.5 yrs CVE-2012-0170 6.1 yrs CVE-2015-1868 10.2 yrs CA CVE-2015-6142 0.5 yrs CVE-2012-0169 6.1 yrs CVE-2015-1868 CVE-2015-1868 10.2 yrs BID-51915 7.0 yrs CVE-2015-6180 1.4 yrs CVE-2012-0159 1.6 yrs CVE-2012-0159 1.6 yrs CVE-2012-0159 1.6 yrs Samba CVE-2015-6180 1.4 yrs CVE-2012-0155 5.9 yrs CVE-2014-0239 0.8 yrs GNU CVE-2015-2464 3.3 yrs CVE-2012-0016 1.1 yrs CVE-2012-0011 5.9 yrs CVE-2015-0235 9.9 yrs CVE-2015-2397 1.7 yrs Newest AOTT ISC CVE-2015-0086 4.6 yrs CVE-2014-3556 3.1 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs								CVE-2014-4049	5.5 yrs
Apple CVE-2016-0103 0.8 yrs CVE-2012-0170 6.1 yrs CVE-2012-0169 6.1 yrs CVE-2012-0169 1.6 yrs CVE-2012-0159 1.6 yrs CVE-2012-0159 2.7 yrs CVE-2012-0158 2.7 yrs CVE-2012-0158 2.7 yrs CVE-2012-0155 5.9 yrs CVE-2012-0155 5.9 yrs CVE-2012-0160 1.1 yrs CVE-2012-0150 5.9 yrs CVE-2012-0010 1.1 yrs CVE-2012-0011 5.9 yrs CVE-2012-0003 0.3 yrs CVE-2013-4115 8.4 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2014-3556 3.1 yrs CVE-2013-2070 8.2 yrs		,	Microsoft						
CVE-2012-3753 0.8 yrs	Annle			0.8 vre					
CA BID-51915 7.0 yrs CVE-2015-6142 0.5 yrs CVE-2012-0159 1.6 yrs CVE-2012-0158 2.7 yrs CVE-2012-0155 5.9 yrs CVE-2015-2464 3.3 yrs CVE-2015-2461 4.7 yrs CVE-2015-0235 9.9 yrs CVE-2015-1662 4.0 yrs CVE-2015-0090 1.4 yrs CVE-2012-0010 1.1 yrs CVE-2012-0011 5.9 yrs CVE-2012-0011 5.9 yrs CVE-2012-0011 5.9 yrs CVE-2012-0011 5.9 yrs CVE-2012-0003 0.3 yrs CVE-2013-4115 8.4 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2013-2070 8.2 yrs		O 9 vre		•				CVE-2015-1868	10.2 yrs
CA BID-51915 7.0 yrs CVE-2015-6150 1.4 yrs CVE-2015-6087 4.6 yrs CVE-2015-2464 3.3 yrs CVE-2015-2461 4.7 yrs CVE-2015-0235 9.9 yrs CVE-2015-1662 4.0 yrs CVE-2015-1662 4.0 yrs CVE-2015-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2015-0086 4.6 yrs CVE-2012-0158 2.7 yrs CVE-2012-0155 5.9 yrs CVE-2012-0016 1.1 yrs CVE-2012-0011 5.9 yrs CVE-2012-0003 0.3 yrs CVE-2013-4115 8.4 yrs CVE-2013-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2013-3570 3.1 yrs CVE-2013-3070 8.2 yrs	CVL-2012-3733	0.0 yrs							
BID-51915 7.0 yrs CVE-2015-6087 4.6 yrs CVE-2015-2464 3.3 yrs CVE-2015-2461 4.7 yrs CVE-2015-0235 9.9 yrs CVE-2015-1662 4.0 yrs CVE-2015-397 1.9 yrs CVE-2015-0090 1.4 yrs CVE-2012-3571 1.9 yrs CVE-2015-086 4.6 yrs CVE-2013-2070 8.2 yrs CVE-20	CA							Samba	
GNU CVE-2015-2464 CVE-2015-2461 CVE-2015-2001 CVE-2012-0011 CVE-2012-0003 CVE-2013-4115 Squid CVE-2013-4115 Squid CVE-2013-4115 SQUID CVE-2013-4115 SQUID CVE-2013-4115 CV		7.0						CVE-2014-0239	0.8 vrs
GNU CVE-2015-2461 CVE-2015-2461 CVE-2015-2461 CVE-2015-2461 CVE-2015-2461 CVE-2015-2397 CVE-2015-2397 CVE-2015-1662 CVE-2015-1662 CVE-2015-1662 CVE-2015-1662 CVE-2015-0090 CVE-2015-0090 CVE-2015-0090 CVE-2015-0090 CVE-2015-0090 CVE-2015-0090 CVE-2013-2070 Squid CVE-2013-4115 CVE-20	BID-51915	7.0 yrs		•					, .
CVE-2015-2461 4.7 yrs CVE-2015-0235 9.9 yrs CVE-2015-2397 1.7 yrs CVE-2015-1662 4.0 yrs CVE-2015-0090 1.4 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2013-2070 8.2 yrs CVE-2013-4115 8.4 yrs CVE-2013-4115 8.4 yrs CVE-2013-4115 8.4 yrs CVE-2013-2070 8.2 yrs	0.111			Ja	vaScript			Sauid	
CVE-2015-0235 9.9 yrs CVE-2015-2397 1.7 yrs CVE-2015-1662 4.0 yrs CVE-2015-1662 4.0 yrs CVE-2015-0090 1.4 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2014-3556 3.1 yrs CVE-2013-2070 8.2 yrs				4. / yrs					8 / vre
ISC CVE-2015-0090 1.4 yrs CVE-2014-3556 3.1 yrs CVE-2012-3571 1.9 yrs CVE-2014-3556 CVE-2013-2070 8.2 yrs	CVE-2015-0235	9.9 yrs		1.1 y 13		0 · 2 20 · 2 0000	0.0).0	OVE 2013-4113	0. 4 y13
CVE-2015-0090 1.4 yrs CVE-2014-3556 3.1 yrs CVE-2012-3571 1.9 yrs CVE-2015-0086 4.6 yrs CVE-2013-2070 8.2 yrs				,	AUTI	NGINX			
CVE-2012-35/1 1.9 yrs	ISC						2.1 vrc		
CVE-2012-3523 1.2 yrs CVE-2014-6369 1.1 yrs CVL-2013-2070 0.2 yrs	CVE-2012-3571	1.9 yrs							
OVE 2012 0020 1.2 yil	CVE-2012-3523	1.2 yrs	CVE-2014-6369	1.1 yrs		OVL-2013-2010	0.2 y13		





AOTT coverage with MOV_Container_Overflow

1: QuickTime

Protocol anomaly

released April 10, 2007

detects malformed QuickTime (.mov) files having an atom whose size exceeds its container size

2007: Protocol signature MOV_Container_Overflow (no CVE, no known exploits)

2009: Microsoft DirectX QuickTime code execution, CVE-2009-1539

```
00000000: moov <0> atomSize=0x0000018b, extent=0x0000018b
00000008: trak <1> atomSize=0x00000178, extent=0x00000180
00000010: tkhd
                 <2> atomSize=0x0000005c, extent=0x0000006c
0000006c: mdia
                 <2> atomSize=0x000000f0, extent=0x0000015c
00000074: mdhd
                 <3> atomSize=0x00000020, extent=0x00000094
00000094: hdlr
               <3> atomSize=0x00000024, extent=0x000000b8
000000b8: minf
                 <3> atomSize=0x000000a4, extent=0x0000015c
000000c0: stbl
                 <4> atomSize=0x0000009c, extent=0x0000015c
000000c8: stsd
                    <5> atomSize=0x00000020, extent=0x000000e8
                                                                           atom overflows container
000000d8: AAAA
                     <6> atomSize=0x41414141, extent=0x41414219
000000e8: stts
                    <5> atomSize=0x00000030, extent=0x00000118
```

2012: Real Networks RealPlayer .mp4 code execution, CVE-2012-1904

2014: Adobe Flash Player and Adobe Air code execution, CVE-2014-8438

2015: Google Android Stagefright media engine covr integer underflow, CVE-2015-3827





AOTT coverage with **Script_DOM_Unconditional_Undo**

2: JavaScript

released June 9, 2015

detects a web script using .execCommand() followed unconditionally by .execCommand('Undo')

2015: Microsoft Internet Explorer code execution, CVE-2015-1753

Reported: June 9, 2015

2015: Microsoft Internet Explorer code execution, CVE-2015-6142

Microsoft Internet Explorer code execution, CVE-2015-6143

Reported: Dec 8, 2015

2016: Microsoft Internet Explorer code execution, CVE-2016-0103

```
Reported: Mar 8, 2016
```

```
... [details under NDA]
....execCommand("Delete", false, null);
document.execCommand("Undo", false);
```





AOTT coverage with **Zip_Directory_Traversal**

3: ZIP history repeats

released May 9, 2006 detects a 'zip' file having a filename containing "../" or "..\"

file=../../../ROOT/f4pbhNrwDT9dQt7QLY3Aq8Fc53Yn9Zh.jsp

2006: IBM Lotus Notes compressed file preview directory traversal, CVE-2005-2619

Reported: February 10, 2006

A remote attacker could traverse directories and delete arbitrary files.

2010: Apache Tomcat WAR directory traversal, CVE-2009-2693

Reported: January 25, 2010

A remote attacker could create arbitrary files on the system outside of the Web root.

2013: Multiple HP products code execution, CVE-2012-5201

Reported: March 7, 2013

An attacker could execute arbitrary code on the system with SYSTEM privileges.

2015: ManageEngine ServiceDesk uploaded files code execution, SecChkId 105842 (no CVE)

Reported: August 20, 2015

An attacker could execute arbitrary code on the system.





AOTT coverage with **Script_Array_Overflow**

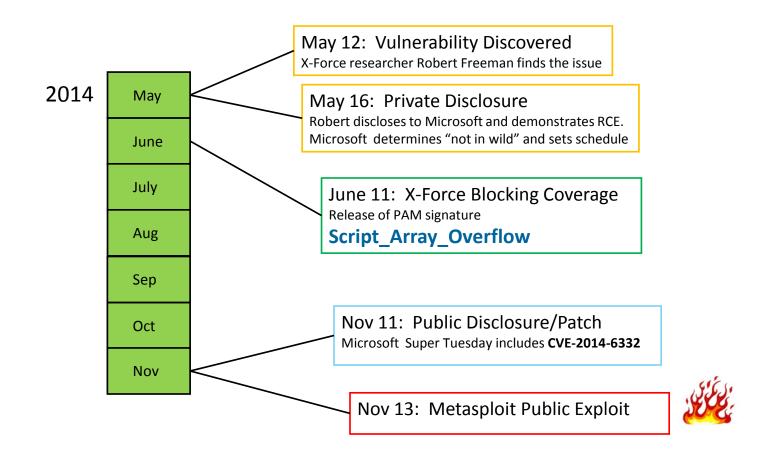
4: VBScript internal find

released June 11, 2014 detects VBScript code that overflows an array

CVE-2014-6332 Microsoft OLE automation array code execution

"Unicorn"

arbitrary code execution caused by improperly accessing an object in memory





Pattern Matching vs. Deep Packet Inspection



Advantages: Pattern Matching vs. Deep Packet Inspection

Rules-based Pattern Matching

- Customization and collaboration
- Faster time-to-market for new coverage
- Visibility of detection logic
 - But, hackers have visibility too!

Deep Packet Inspection (PAM)

- Ahead of the Threat coverage
- Fewer false negatives (mutation detection)
- Detection of traffic on unexpected ports via protocol heuristics
- Protocol anomaly signatures
 (MOV_Container_Overflow, TLS_Zero_Length_Record)
- Heuristics-based signatures
 (SQL Injection, Java_Malicious_Applet, Script_Suspicious_Score)
- Shellcode heuristics
 (PDF_Shellcode_Detected, JavaScript_Shellcode_Detected)
- Flood detection and mitigation
 (DNS_Dot_Query_Flood, SMB_Mass_Login, Syslog_Flood)
- Complex data leakage protection (social security AND credit card in any order)





X-Force Top 100 Ahead of the Threat Coverage

Blocking coverage at least 90 days ahead of the threat for notable vendors since 2012 with CVSS >=5

Average AOTT = 3.8 yrs

Average CVSS base = 8.6

Adobe CVE-2015-5097 CVE-2014-8438 CVE-2013-3346	5.1 yrs 7.6 yrs 1.3 yrs	Google CVE-2015-3864 CVE-2015-3829 CVE-2015-3828	8.4 yrs 8.3 yrs 8.3 yrs	1	Microsoft (cc CVE-2014-6343 CVE-2014-6332 CVE-2014-2799	3.6 yrs 0.4 yrs 0.5 yrs	Novell CVE-2015-0779 CVE-2012-0271	3.0 yrs 0.6 yrs
CVE-2013-2729 CVE-2013-2555	7.2 yrs 0.7 yrs QuickTime	CVE-2015-3827 CVE-2015-3826 CVE-2015-3824	6.5 yrs 8.3 yrs 8.3 yrs		CVE-2014-2797 CVE-2014-1811	0.7 yrs 4.8 yrs VBScript	NTP CVE-2013-5211	0.5 yrs
CVE-2013-0634 CVE-2012-4170 CVE-2012-1535 CVE-2012-0769 CVE-2012-0768 BID-52632	1.8 yrs 7.5 yrs 1.4 yrs 0.9 yrs 0.9 yrs 7.0 yrs	CVE-2015-3824 CVE-2015-1539 CVE-2015-1538 BID-52632	8.3 yrs 8.3 yrs 7.0 yrs		CVE-2014-1761 CVE-2013-3906 CVE-2013-3893 CVE-2013-3163 CVE-2013-1331 CVE-2013-1347	1.3 yrs 1.2 yrs 0.7 yrs 0.5 yrs 3.7 yrs 2.6 yrs	Oracle CVE-2013-2465 CVE-2013-2463 CVE-2013-2431 CVE-2013-0431	0.8 yrs 0.8 yrs 8.2 yrs 0.3 yrs
Apache		CVE-2014-7883 CVE-2014-2625 CVE-2014-2621	1.1 yrs 9.4 yrs 1.1 yrs	<u>ZIP</u> History	CVE-2013-1313 CVE-2013-0026 CVE-2013-0025	0.5 yrs 6.9 yrs 6.9 yrs	CVE-2013-0422 BID-56791	7.9 yrs 1.5 yrs
CVE-2013-2251 CVE-2013-2135 CVE-2013-2134	2.4 yrs 2.3 yrs 2.3 yrs	CVE-2014-2621 CVE-2014-2620 CVE-2014-2617	1.1 yrs 1.2 yrs 1.9 yrs	repeats	CVE-2012-4781 CVE-2012-2522	6.7 yrs 0.8 yrs	BID-56772 CVE-2012-3342	1.6 yrs 5.3 yrs
CVE-2013-2115 CVE-2013-1966	2.3 yrs 2.3 yrs	CVE-2013-6195 CVE-2013-4799	0.3 yrs 5 9 yrs		CVE-2012-1899 CVE-2012-1879 CVE-2012-1878	1.5 yrs 6.2 yrs 6.2 yrs	PHP CVE-2015-4022	7.2 yrs
CVE-2012-0838 CVE-2012-0391	1.0 yrs 0.9 yrs	CVE-2012-5201 Microsoft	6.8 yrs		CVE-2012-1876 CVE-2012-1875	6.2 yrs 6.2 yrs	1 112 2 -4049	5.5 yrs
Apple CVE-2012-3753	0.8 yrs	CVE-2016-0103 CVE-2015-6143	0.8 yrs 0.5 yrs		CVE-2012-0171 CVE-2012-0170 CVE-2012-0169	6.1 yrs yrs yre XON	PowerDNS 015-1868	10.2 yrs
CA BID-51915	7.0 yrs	CVE-2015-6142 CVE-2015-6150 CVE-2015-6087	0.5 yrs 1.4 yrs 4.6 yrs		CVE-2012-0159 CVE-2012-0158 CVE-2012-0155	2.7 yrs 5.9 yrs	5amba CVE-2014-0239	0.8 yrs
GNU	7.0 yis	CVE-2015-0007 CVE-2015-2464 CVE-2015-2461		lavaScript	CVE-2012-0016 CVE-2012-0011	1.1 yrs 5.9 yrs Pa	ttern	
CVE-2015-0235	9.9 yrs	CVE-2015-2397 CVE-2015-1662	1.7 yrs 4.0 yrs	Newest AOTT	CVE-2012-0003	0.5 yrs	CVE-2013-4115	8.4 yrs
ISC CVE-2012-3571 CVE-2012-3523	1.9 yrs 1.2 yrs	CVE-2015-0090 CVE-2015-0086 CVE-2014-6369	1.4 yrs 4.6 yrs 1.1 yrs		NGNX CVE-2014-3556 CVE-2013-2070	3.1 yrs Ma 1 8.2 yrs	tching	



Pattern Matching: False Negative 2009: Microsoft DirectX QuickTime code execution. CVE-2009-1539

1: QuickTime

Protocol anomaly

PAM signature (2007): MOV_Container_Overflow

```
if ((state->depth > 0) && (extent > state->atomExtent[state->depth-1]))
```

Snort coverage: ... flow:to_client,established; file_data; content: "AAAAAAAA|00 00 00|0stts|04 00 00 00|"; ...

```
00000000: moov <0> atomSize=0x0000018b, extent=0x0000018b
2009 PoC:
                       00000008: trak <1> atomSize=0x00000178, extent=0x00000180
                                       <2> atomSize=0x0000005c, extent=0x0000006c
                       00000010: tkhd
                       0000006c: mdia
                                       <2> atomSize=0x000000f0, extent=0x0000015c
                       00000074: mdhd
                                       <3> atomSize=0x00000020, extent=0x00000094
                       00000094: hdlr
                                         <3> atomSize=0x00000024, extent=0x000000b8
                                         <3> atomSize=0x000000a4, extent=0x0000015c
                       000000b8: minf
                                        <4> atomSize=0x0000009c, extent=0x0000015c
                       000000c0: stbl
                       000000c8: stsd
                                         <5> atomSize=0x00000020, extent=0x000000e8
       overflow
                                           <6> atomSize=0x41414141, extent=0x41414219
                      > 000000d8: AAAA
                       000000e8: stts
                                           <5> atomSize=0x00000030, extent=0x00000118
```





Pattern Matching: A rule for each exploit

2: JavaScript

2015-2016: Related Microsoft IE code execution vulnerabilities

```
PAM signature (2015): if (state->saw_execCommand && execCommandVulnerable && isUndo)
Script_DOM_Unconditional_Undo
```

Snort coverage:

```
CVE-2015-1753 Reported: June 9, 2015
```

```
... flow:to_server,established; file_data; ... content:".execCommand"; within:100; nocase; ...
nocase; content:".scrollIntoView"; within:100; nocase; content:".execCommand"; nocase;
content:"Undo"; within:25; nocase; ...
```

CVE-2015-6142 Reported: Dec 8, 2015

```
... flow:to_server,established; file_data; content:"ms-beginUndoUnit"; fast_pattern:only; content:"execCommand"; nocase; content:"undo"; within:10; nocase; ...
```

CVE-2015-6143 Reported: Dec 8, 2015

```
... flow:to_server,established; file_data; content:".addEventListener"; nocase;
content:"DOMAttrModified"; within:25; nocase; content:".execCommand"; nocase; ... nocase;
content:".execCommand"; nocase; content:"undo"; within:15; nocase; ...
```

CVE-2016-0103 Reported: Mar 8, 2016 ???





Pattern Matching: Lack of Coverage

2006-2015: Related Zip Traversal vulnerabilities

3: ZIP history repeats

```
PAM signature (2006):
                           if (dirClimb(psom, &dirClimbState, zip->file.name, zip->file.nameLen))
Zip Directory Traversal
```

Snort coverage:

2006: IBM Lotus Notes compressed file preview directory traversal, CVE-2005-2619

--- no Snort coverage ---

2010: Apache Tomcat WAR directory traversal, CVE-2009-2693

--- no Snort coverage ---



2013: Multiple HP products code execution, CVE-2012-5201

```
... flow:to server,established; content:"/imc/webdm/mibbrowser/mibFileUpload";
fast_pattern:only; http_uri; content:"..|5C|..|5C|..|5C|..|5C|..|5C|"; http_client_body; ...
... flow:to server,established; content:"/imc/webdm/mibbrowser/mibFileUpload";
fast_pattern:only; http_uri; content:"../../../"; http_client_body; ...
```

2015: ManageEngine ServiceDesk code execution, SecChkId 105842 (no CVE)

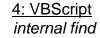
--- no Snort coverage ---





Pattern Matching: Large Rule Set





```
PAM signature (2014): Script_Array_Overflow
```

Snort coverage (14 rules):

- ./rules/browser-ie.rules:alert top SEXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data; content:"redim";
 nocase; content:"preserver; within:20; nocase; content:"(&h"; within:20; byte_test:6,>,1000,0,relative,string,hex; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service smtp;
 reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32473; rev:4;
- ./rules/browser-ie.rules:alert tcp \$EXTERNAL_NET any -> \$\$MTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data; content:"redim"; nocase; content:"preserve"; within:20; nocase; content:"spreserve"; within:20; nocase; content:"s
- ./rules/browser-ie.rules:alert top \$EXTERNAL.NET \$FILE_DATA_PORTS -> \$HOME_NET any (msg!*BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt*; flow:to_client,established; file_data; content:"preserve"; within:20; nocase; content:"(ah; within:20; byte_test:6,>,1000,0,relative,string,hex; metadata; policy max-detect-ips drop, policy max-detect-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:cve,2014-6332; reference:cve,1cm-nus/security/bulletin/ms14-064; classtype:attempted-dos; sid:32471; rev:4;)
- ./rules/browser-ie.rules:alert top \$EXTERNAL.NET \$FILE_DATA_PORTS -> \$HOME_NET any (msg: "BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data; content: "preserve"; within:20; nocase; content:"(; within:20; nocase; content:"(; within:20; nocase; content) balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:cve, 2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32470; rev:4;)
- ./rules/browser-ie.rules:alert top \$EXTERNAL.NET any -> \$SMTP_SERVERS 25 (msg:"RROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data; content:"array"; content:"drw"; within:10; content:"drw"; within:20; content:"drw"; within:2
- ./rules/browser-ie.rules:alert top \$EXTERNAL_NET \$FILE_DATA_PORTS -> \$HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client.established; file_data; content:"myarray"; content:"chrw"; within:10; content:"chrw"; within:20; content:"strent; "atthin:20; content:"policy metadata; policy max-detect-ips drop, policy security-ips drop, service ftp-data, service http, service pop3; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:atthempted-dos; sid:32564; rev:4;)
- ./rules/browser-ie.rules:alert tcp \$EXTERNAL_NET any -> \$\$MTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data; content:"redim Preserve arr(&h8000002)"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service smtp; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32630; rev:21)
- ./rules/browser-ie.rules:alert tcp \$EXTERNAL_NET \$FILE_DATA_PORTS -> \$HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data; content:"redim Preserve arr(&h8000002)"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:cve,2014-6332;
- reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32629; rev:2:)
 ./rules/browser-ie.rules:alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg: BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt*; flow:to_server,established; file_data;
 content:"HIVIauuKF619p*q11wE81*znjk3Y18td*; fast_pattern:only.imetadata:policy balanced-ips drop, policy security-ips drop, service smtp; reference:cve, 2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-
- content: "HIVlauuKF619P*q11WE60" znjx:Y18td"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service smtp; reference:cve, 2014-6332; reference:url, technet.microsoft.com/en-us/security/bulletin/msl 064; classtype:attempted-dos; sid:33116; rev:2;)

 ./rules/browser-ie.rules:alert top \$EXTERNAL.NET \$FILE_DATA_PORTS -> \$HOME_NET any (msg: "BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data;
- reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:33115; rev:2;)
- ./rules/browser-ie.rules:alert top SEXTERNAL_NET any -> SSMTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server.established; file_data; content:"%6723"; content:"wrhc"; within:10; content:"wrhc"; within:10; content:"yarraym"; within:10; metadata:policy balanced-ips drop, policy security-ips drop, service smtp; reference:cve,2014-6332; referenc
- ./rules/browser-ie.rules:alert tcp \$EXTERNAL_NET \$FILE DATA_PORTS -> \$HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data; content:"wrhc"; within:10; content:"wrhc"; within:20; content:"wrhc"; wrhc"; wr
- ./rules/browser-ie.rules:# alert top \$EXTERNAL_NET any -> \$HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; content:"mew ActiveXObject"; content:"Mscript.Shell?: within:30; content:"Run("; within:30; metadata:policy max-detect-ips drop, policy security-ips drop, service http; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-user; sid:36896; rev:1;)
- ./rules/exploit-kit.rules:# alert tcp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"EXPLOIT-KIT Known exploit kit obfuscation routine detected"; flow:to_client,established; content:"bscript>"; content:"Split("; within:40; content:"Bound("; within:40; content:"Left-within:40; content:"Left-within:40;





Powered by PAM provides broad threat coverage

Comprehensive protection, visibility, and control over network traffic

Deep Packet Inspection

Fully classifies network traffic, regardless of address, port, or protocol

SSL Visibility

Identifies inbound and outbound traffic threats, without needing a separate appliance

Identity and Application Awareness

Associates users and groups with their network activity, application usage and actions



Network Traffic and Flows

Outbound Traffic

Application A Attack Traffic

Application B Clean Traffic

Employee A Good Application

Employee B Prohibited Application

Employee C Botnet Traffic

500+

Protocols and file formats analyzed

25+ Billion

URLs classified in 70 categories

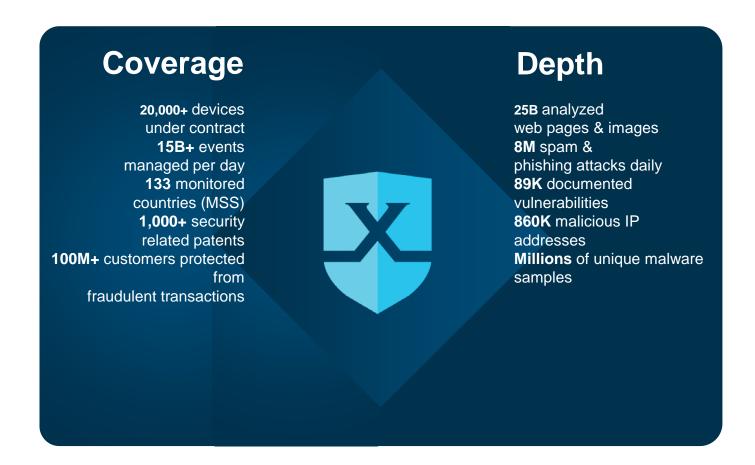
2,000+

Applications and actions identified

Ш,

Ш,

IBM X-Force monitors and analyzes the changing threat landscape





IBM X-Force® Exchange



A platform to discover, collaborate, and act on threat intelligence

IBM X-Force Exchange is

OPEN

a robust platform with access to a wealth of threat intelligence data

SOCIAL

a collaborative platform for sharing threat intelligence

ACTIONABLE

an integrated solution to help quickly stop threats

Backed by the reputation and scale of IBM X-Force





THANK YOU

FOLLOW US ON:



ibm.com/security



securityintelligence.com



xforce.ibmcloud.com



@ibmsecurity



youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBMs current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

