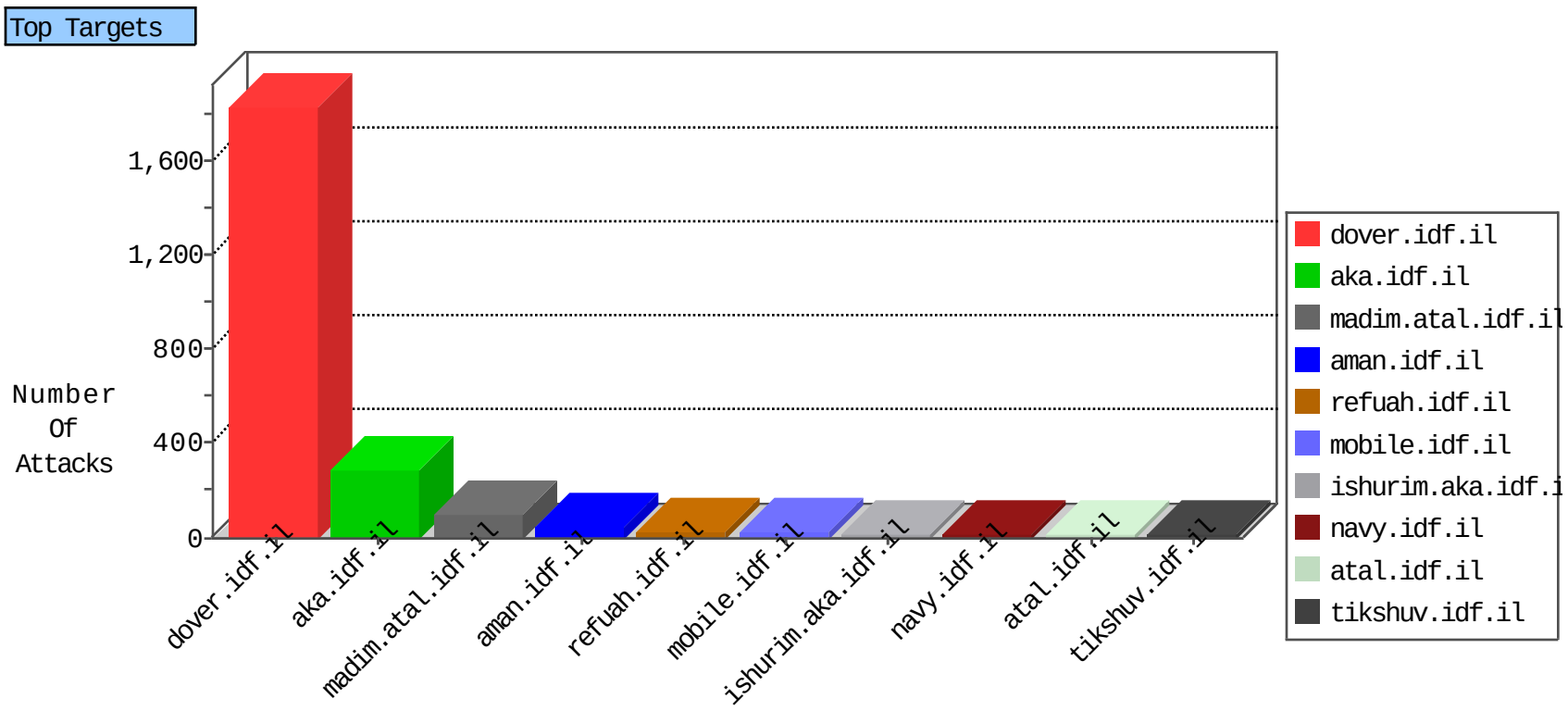
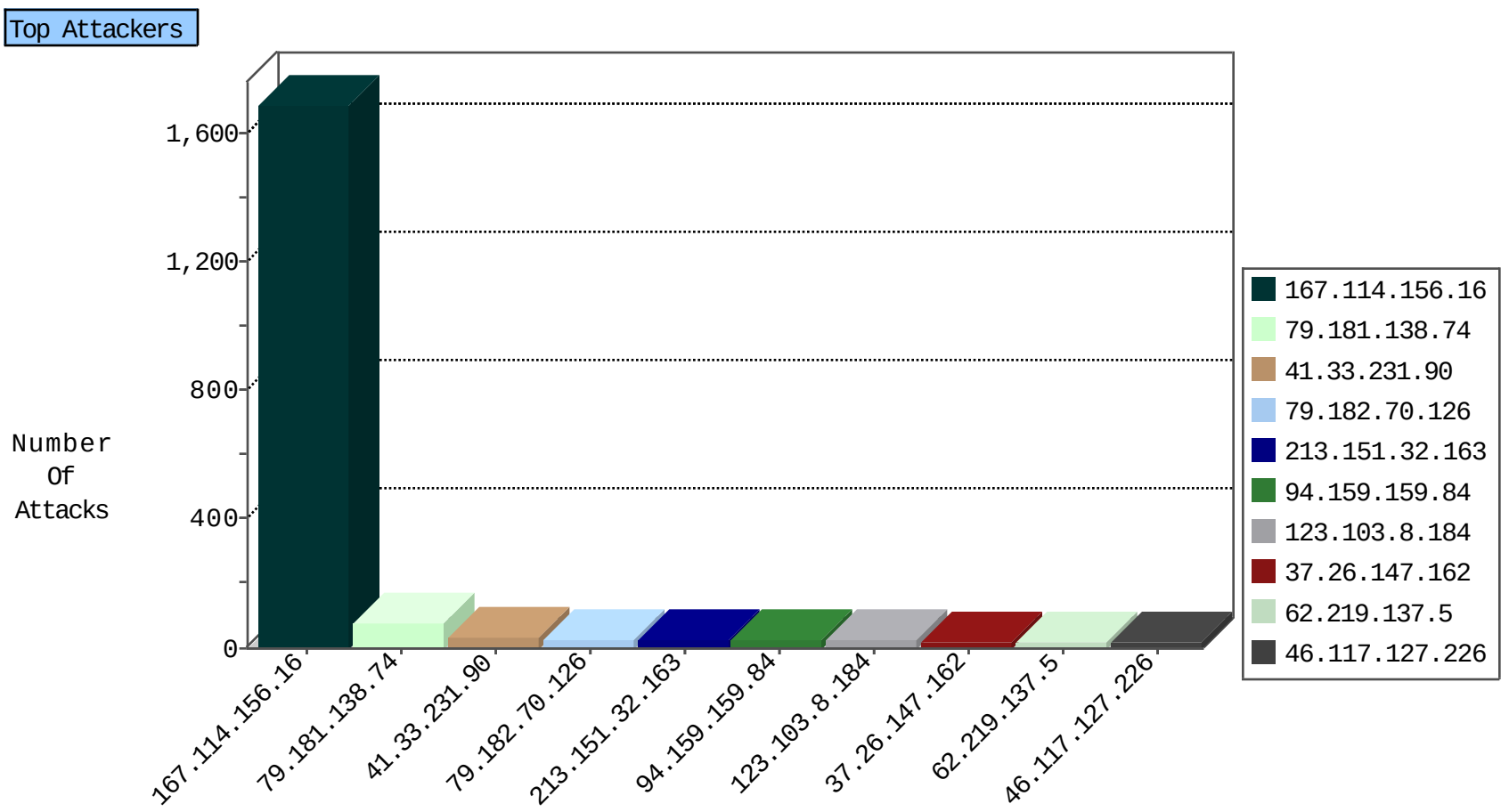
12-16-2015-23:04:09 to 12-17-2015-00:04:09

IDF Under Attack
Daily Report





12-16-2015-23:04:09 to 12-17-2015-00:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3139
79.178.205.9	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.183.122.211	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

12-16-2015-23:04:09 to 12-17-2015-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.119	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.129	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-16-2015-23:04:09 to 12-17-2015-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
187.252.214.158	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
175.143.53.17	147.237.0.16	Malaysia	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
113.106.129.219	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
64.147.86.71	147.237.76.30	Bermuda	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
5.28.185.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.252.214.158	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.143.53.17	147.237.0.16	Malaysia	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
166.63.125.149	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
73.17.14.46	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1

12-16-2015-23:04:09 to 12-17-2015-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
94.159.159.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
123.103.8.184	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
185.3.146.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
79.179.196.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.64.182.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.150	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
62.219.137.5	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
62.219.137.5	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
37.26.147.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	8
37.26.147.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
77.127.3.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.48.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
83.130.110.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.143.74	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
207.229.156.214	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
83.130.110.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.138.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.8.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.227.236.78	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.64.204.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.204.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.127.226	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.52.45.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.148.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.117.127.226	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	4
5.102.254.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.136.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.190.147	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.147.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.61.193	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
49.180.161.64	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
82.81.0.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.137	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
89.134.236.78	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.117.127.226	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.182.150.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.25.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.10.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.127.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.177.21.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.127.226	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
2.54.15.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
149.88.66.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.181.154.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-16-2015-23:04:09 to 12-17-2015-00:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.138.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
79.181.138.74	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.138.74	Block	31
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
176.228.212.22	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 176.228.212.22	Block	8
212.235.16.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	5
176.228.188.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
207.46.13.169	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
109.64.204.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.137.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
93.173.36.7	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 47 Headers	Block	1
69.30.244.186	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
46.19.86.87	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
122.224.8.111	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckfinder	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.182.70.126	Block	1
2.54.149.79	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
95.86.90.222	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String Â?U?ÃŸ>Ã›2â€¹fÂ¢e[[#24]] on [[#28]]tÂ¿bÂµaâ,¬j×?h×°Ö²Â£Â²Ã–	Block	1
185.35.62.11	Switzerland	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
84.108.13.232	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
157.55.39.18	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.182.70.126	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Malformed URL 8t×•Â¹{{×?Â±â€Žâ€™hÖ²a×¤Ö½{Ã»;Ã–×±meÂ´Â-Â¿1z×”.ËœÂŸ[[#5]]&â€“Â¦iy[[#27]]rk)Ö¸Ã»Ã‰%}s×ƒ[[#16]]Â¾â,ª*1×¥â€žâ€”â€˜fÂ³Â´[[#5]]aÖ¼Ö°ÂŒÂ§Ã™Â´>vÂ¨]â€¹gÂ?×'hÂ?4×°'Â¸[[#8]]â€?jâ€¢t[[#25]]Â?×§ÂŸ[[#25]]{Ã·l[[#2]]ÂœÃœ[[#4]][[#15]]râ€š[[#23]]sd0×²×”Öµ'×?+â€”â€š}gjÃ·â€ºj[[#26]]Ö»;5Ë†Ã¼	Block	1
213.8.204.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.44.138.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
89.38.150.47	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-signup.php	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ;Ã• [[#1]]cÂ¾Â?Â±Â¶[[#24]]Ã§Â‰Ã°%[[#5]]Â³Ã?NÃ¾Ã¶Âª[[#7]]Âœ [[#6]]>J[[#2]]Ã‡5Â Ã'ÃŸÂ‹[[#5]]Â¶hfÃ®w[[#17]]ÂŸÂµÃˆ[[#17]]2Ã– =hWQ(!Ã™^),Â-o!Ã"[[#29]]Ã"Â¼Ã¤[[#26]]NYÃŸ6Ã…[[#27]][[#22]]}Â‹ jÂ¯lMo$Ã¸ [[#20]]ÃªÂŒYÂ¦Ã¹/[[#19]]Ã?,m"Ã• Â¡Ã²xf`Ã-Â?Ã¨@Ã·-[[#4]]Ã¦8Â°99KÃ¾Â¥^Â-Â¾Âƒ«Ã'Â†Âœ [[#17]]$[[#31]]Â–9rÂŸ&mkÃ¸Ã'Ã¦Â,]#Ã´.Ã€ÂµÃ¾Â½Â¹Ã†Ã¸eÂ¬Â›Ã‡ Ã¦t[[#29]]TÂ'Â¬Â˜Â²[[#30]]Ã‹	Block	1
203.133.168.167	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter l in www.chinuch.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Ã„Âœ[^Â¤ÂŽ[[#12]]U in URL 8t×•Â¹{{×?Â±â€Žâ€™hÖ²a×¤Ö½{Ã»	Block	1
69.30.244.186	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
183.91.14.219	Vietnam	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
128.232.110.29	United Kingdom	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.182.70.126	Block	1
2.54.183.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.108.132.178	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/8/638.pdf	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL 8t×•Â¹{{×?Â±â€Žâ€™hÖ²a×¤Ö½{Ã»;Ã–×±meÂ´Â-Â¿1z×”.ËœÂŸ[[#5]]&â€“Â¦iy[[#27]]rk)Ö¸Ã»Ã‰%}s×ƒ[[#16]]Â¾â,ª*1×¥â€žâ€”â€˜fÂ³Â´[[#5]]aÖ¼Ö°ÂŒÂ§Ã™Â´>vÂ¨]â€¹gÂ?×'hÂ?4×°'Â¸[[#8]]â€?jâ€¢t[[#25]]Â?×§ÂŸ[[#25]]{Ã·l[[#2]]ÂœÃœ[[#4]][[#15]]râ€š[[#23]]sd0×²×”Öµ'×?+â€”â€š}gjÃ·â€ºj[[#26]]Ö»;5Ë†Ã¼	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.181.138.74	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
185.35.62.11	Switzerland	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
84.108.45.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.182.70.126	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.194	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.182.70.126	Block	1
213.57.209.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-16-2015-23:04:09 to 12-17-2015-00:04:09