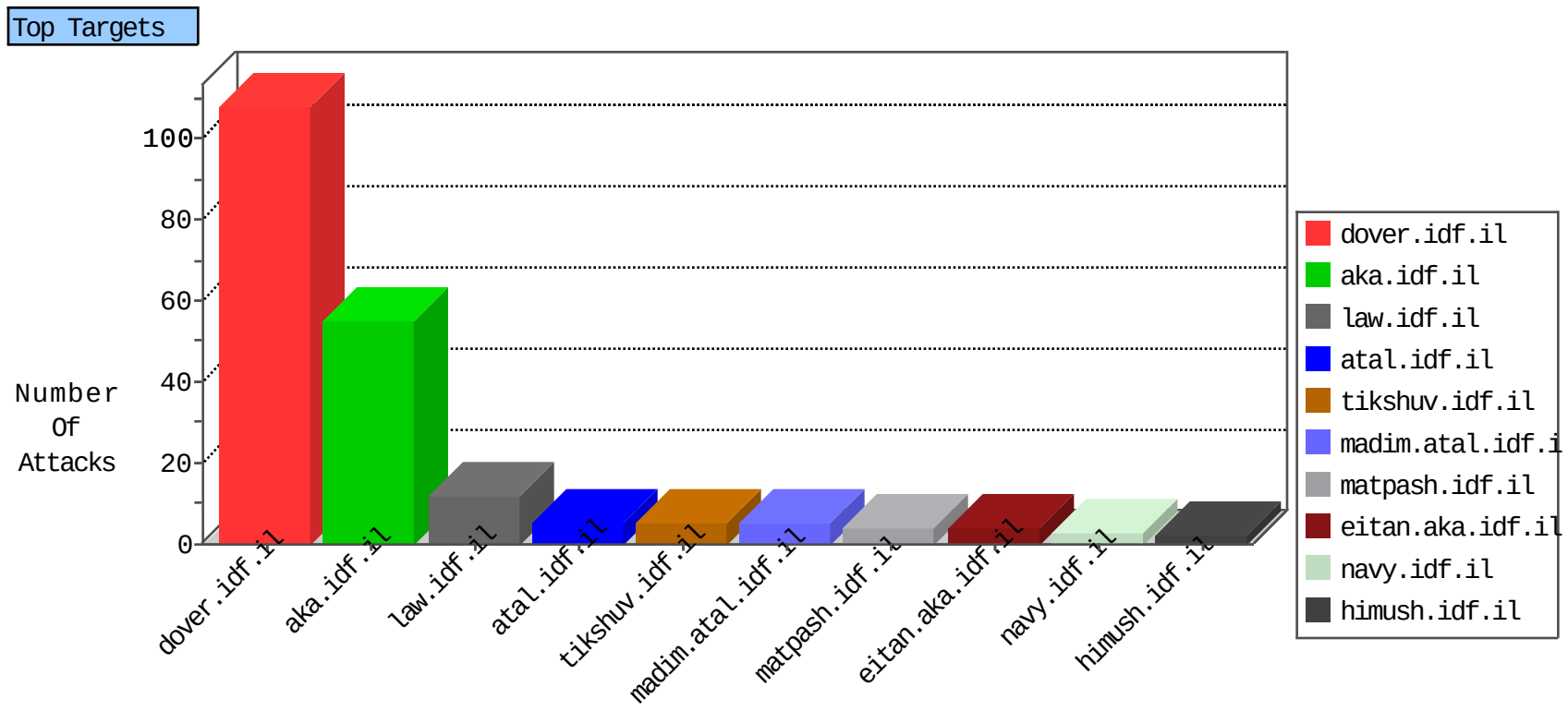
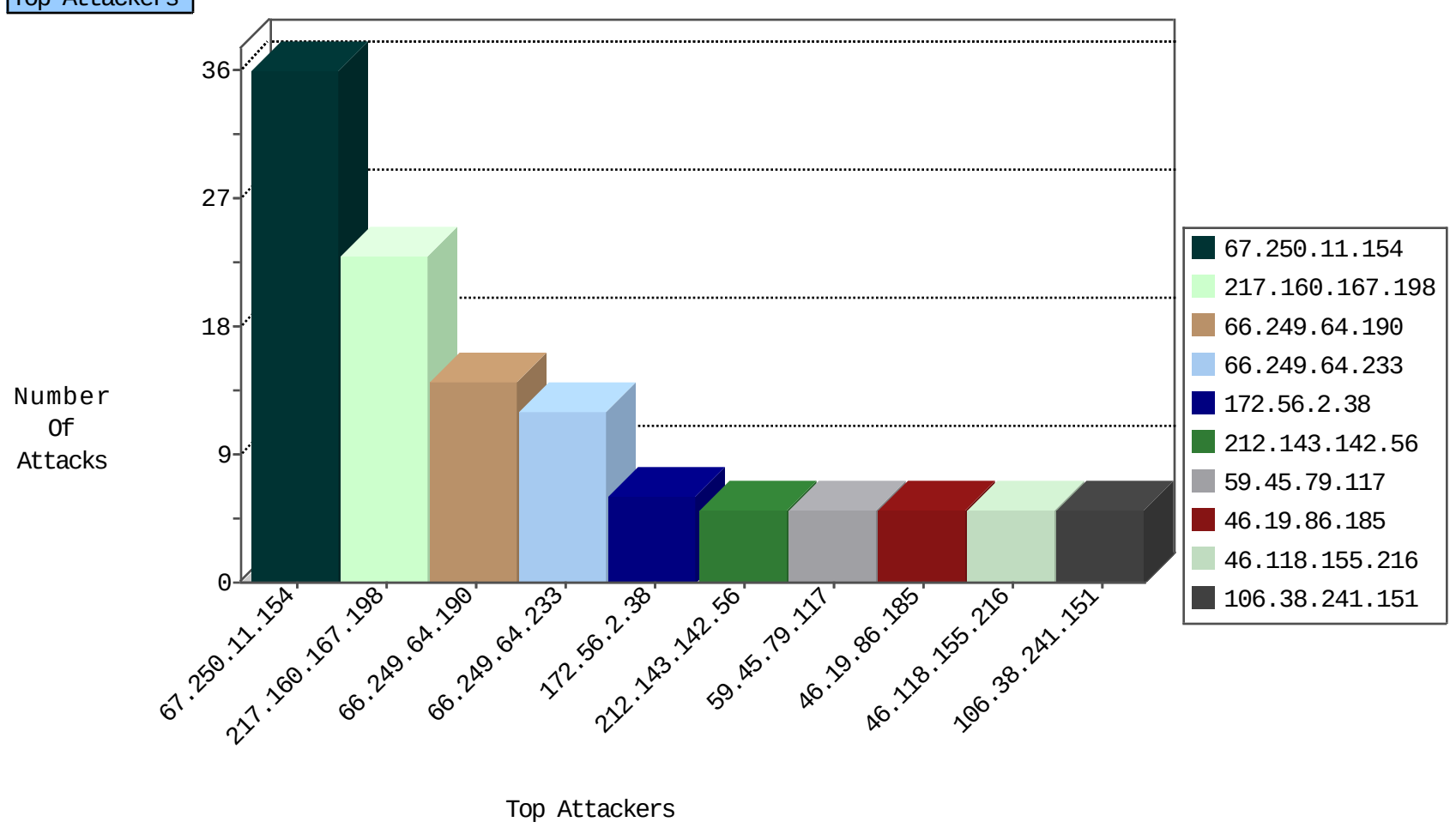
03-06-2016-03:04:04 to 03-06-2016-04:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-06-2016-03:04:04 to 03-06-2016-04:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	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	forward	2
139.162.152.84	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.226	United States	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1

03-06-2016-03:04:04 to 03-06-2016-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-06-2016-03:04:04 to 03-06-2016-04:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.8.243	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
190.216.146.143	147.237.76.199	Chile	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
190.216.146.143	147.237.76.30	Chile	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.238	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
190.216.146.143	147.237.76.176	Chile	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
190.82.107.106	147.237.76.30	Chile	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.74	China	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
52.87.243.150	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.148	United States	gqcenter.aka.idf.il	ET DROP Dshield Block Listed Source	1

03-06-2016-03:04:04 to 03-06-2016-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
67.250.11.154	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
172.56.2.38	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
106.38.241.151	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.69.120.154	Poland	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
98.208.239.205	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.228.197.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
122.52.104.38	Philippines	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
141.212.122.230	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.205.134.118	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.38.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.251	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.102.48.193	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
73.205.134.118	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.245.122.129	United States	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
94.102.48.193	Netherlands	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
207.46.13.60	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.19	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.71	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.227	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.135	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.76	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
68.199.130.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	12
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
2.54.152.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
113.67.188.45	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	2
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 217.160.167.198	Block	1
66.249.66.127	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name [[#12]]Én•¨¹÷ë×Ç‹Xý¢ ÎIØÛ[[#0]]ßeXšRÀ	Block	1
197.35.225.175	Egypt	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
89.138.106.196	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 217.160.167.198	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 13	Block	1
207.241.229.33	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/eitan/pratim/pirteyerua	Block	1
41.35.174.87	Egypt	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Too Many Headers per Request - 34 Headers	Block	1
176.101.2.153	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 217.160.167.198	Block	1
66.249.75.218	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
197.39.212.177	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	NULL Character in Header Name at [[#12]]Én•¨¹÷ë×Ç‹Xý¢ ÎIØÛ[[#0]]ßeXšRÀ	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Malformed URL ı	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter D.. in www.aka.idf.il/giyus/general/	None	1
207.241.229.33	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
41.35.174.87	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Unknown HTTP Request Method H¹[[#16]][[#15]]¾œÿ[[#0]]ðÔ–4È'[[#19]]™+}n4[[#8]]K©6[[#0]]R in URL	Block	1
185.24.76.136	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 217.160.167.198	Block	1
87.70.2.90	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.120.156.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$ 103 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method H¹[[#16]][[#15]]¾œÿ[[#0]]ðÔ–4È'[[#19]]™+}n4[[#8]]K©6[[#0]]R	Block	1
197.39.212.177	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
41.35.103.33	Egypt	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
113.67.188.45	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	NULL Character in Method H¹[[#16]][[#15]]¾œÿ[[#0]]ðÔ–4È'[[#19]]™+}n4[[#8]]K©6[[#0]]R	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 217.160.167.198	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
41.35.174.87	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
185.24.76.136	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Multiple Malformed URL from 217.160.167.198	Block	1
87.70.2.90	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.120.156.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$ 71 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL ¸[[#3]]שת|''÷<'m¿°'h×i3[[#0]]j›פדe¬ק z_nd"Ž'[[#11]][[#6]]t'¢v'>Ü	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
41.35.103.33	Egypt	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
113.67.188.45	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	NULL Character in URL ¸[[#3]]שת|''÷<'m¿°'h×i3[[#0]]j›פדe¬ק z_nd"Ž'[[#11]][[#6]]t'¢v'>Ü	Block	1