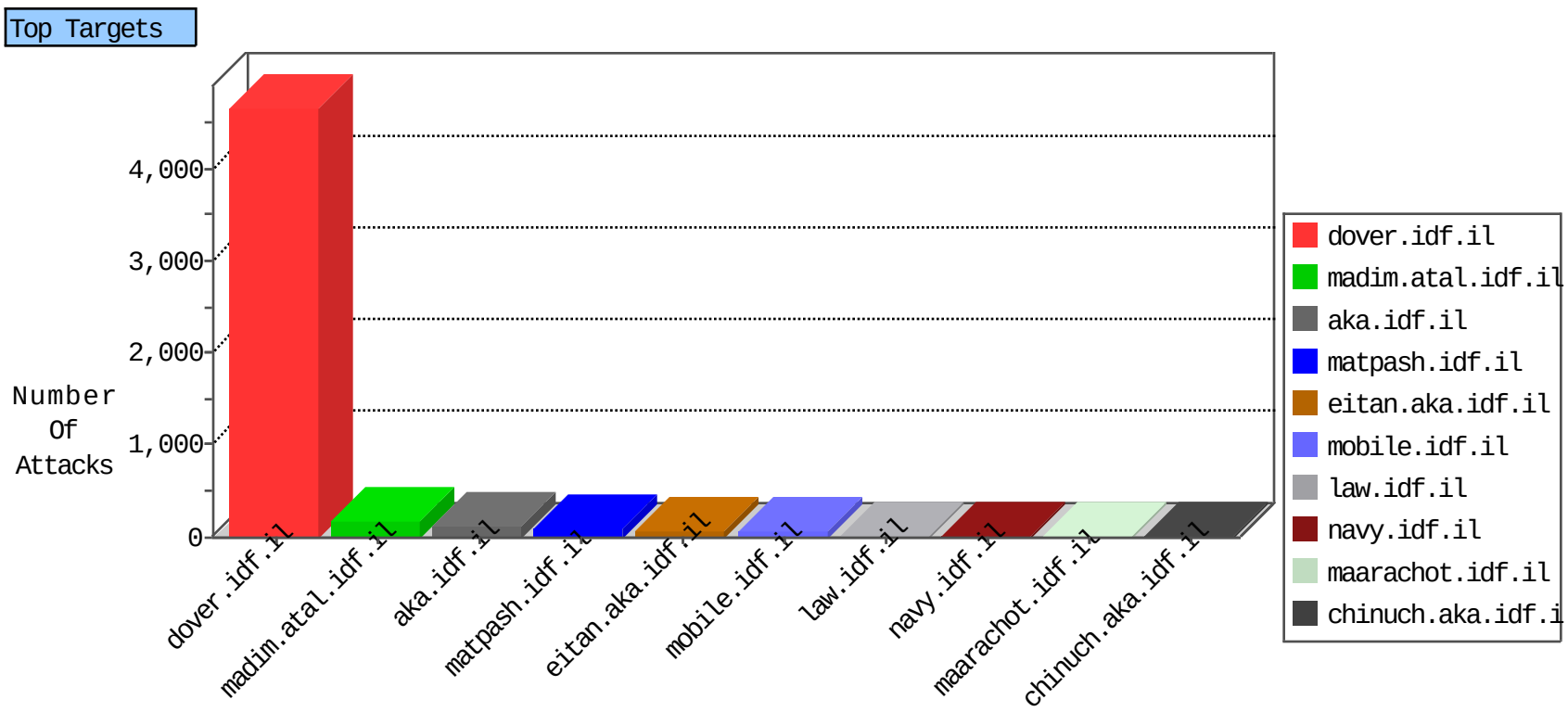
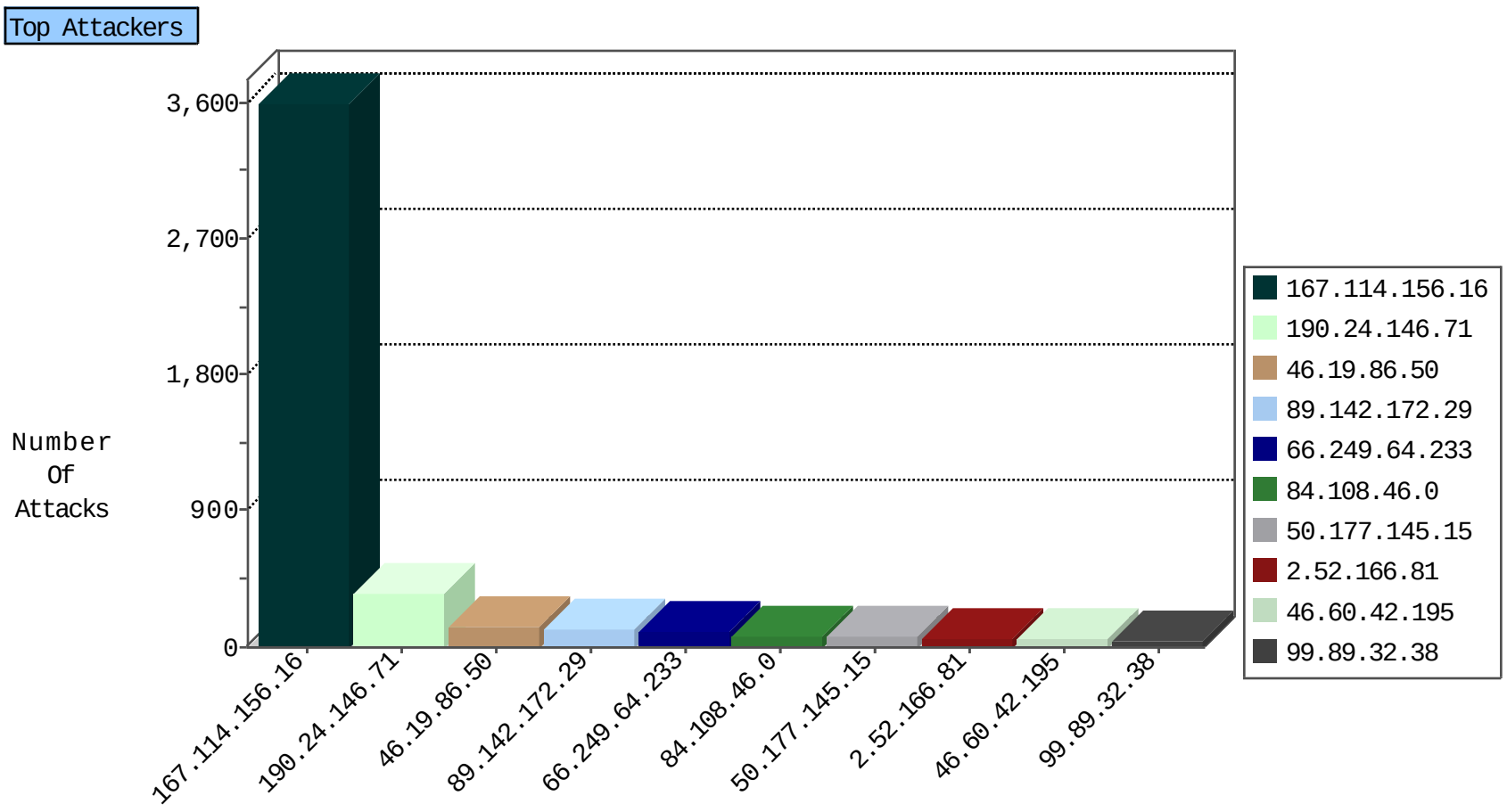
11-25-2015-00:04:02 to 11-25-2015-01:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-25-2015-00:04:02 to 11-25-2015-01:04:02

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	2832
82.166.118.110	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	4
115.231.222.40	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2

11-25-2015-00:04:02 to 11-25-2015-01:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-25-2015-00:04:02 to 11-25-2015-01:04:02

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
169.54.233.117	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.16.132	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.117	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.16.132	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.117	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.16.132	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.117	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.16.132	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.117	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.117	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.60.175	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.60.175	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.117	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.176.8.76	147.237.0.34	Israel	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
169.54.233.117	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.16.132	147.237.77.234		halag.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.117	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.16.132	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.117	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.63.16.132	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.117	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.117	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.73.228.130	147.237.76.147	Singapore	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
220.241.81.245	147.237.0.17	Hong Kong	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.175	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.117	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.166.118.110	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 1024	1

11-25-2015-00:04:02 to 11-25-2015-01:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1494
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	360
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	106
89.142.172.29	Slovenia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	86
50.177.145.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
2.52.166.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
46.60.42.195	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	SAM rule	drop	44
99.89.32.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
174.53.35.232	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
82.145.209.73	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
159.53.174.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
89.142.172.29	Slovenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
52.68.136.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.10.159.213	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
188.120.148.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
38.107.91.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
173.252.88.244	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.100.92.98		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
78.43.195.176	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.86.70.254	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.8.255		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
173.252.88.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
173.252.88.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.25.1	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
182.250.253.234	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.60.42.195	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop		drop	4
173.252.88.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.118.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.60.42.195	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
217.132.229.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.176.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.205.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
89.142.172.29	Slovenia	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

11-25-2015-00:04:02 to 11-25-2015-01:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
84.108.46.0	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.108.46.0	Block	72
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.50	Block	31
85.250.228.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
2.52.166.81	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.52.166.81	Block	6
84.108.79.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.148.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.28.178.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.4.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.166.81	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1678	Block	2
157.55.39.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
2.54.1.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.223.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.183.226.86	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	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
109.186.8.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.200.12.5	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
37.142.242.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.67.204	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 85.250.67.204	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/forgotpassword.aspx	Block	1
109.201.135.182	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
54.145.50.68	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.66.210.43	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed PHP Attempt	Block	1
37.142.68.105	Israel	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	1
212.179.152.234	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
46.121.208.233	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.183.226.86	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
176.12.151.122	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.125.156.188	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
157.55.39.55	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.200.12.5	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.200.12.5	Block	1
85.164.206.87	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
212.199.104.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2422.jpg	Block	1
109.66.210.43	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.142.188.69	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
31.210.187.167	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
84.108.74.63	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.121.208.233	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
109.64.7.124	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
46.121.208.233	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
99.1.240.226	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	1
5.28.172.177	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.180.206.22	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.180.206.22	Block	1

11-25-2015-00:04:02 to 11-25-2015-01:04:02