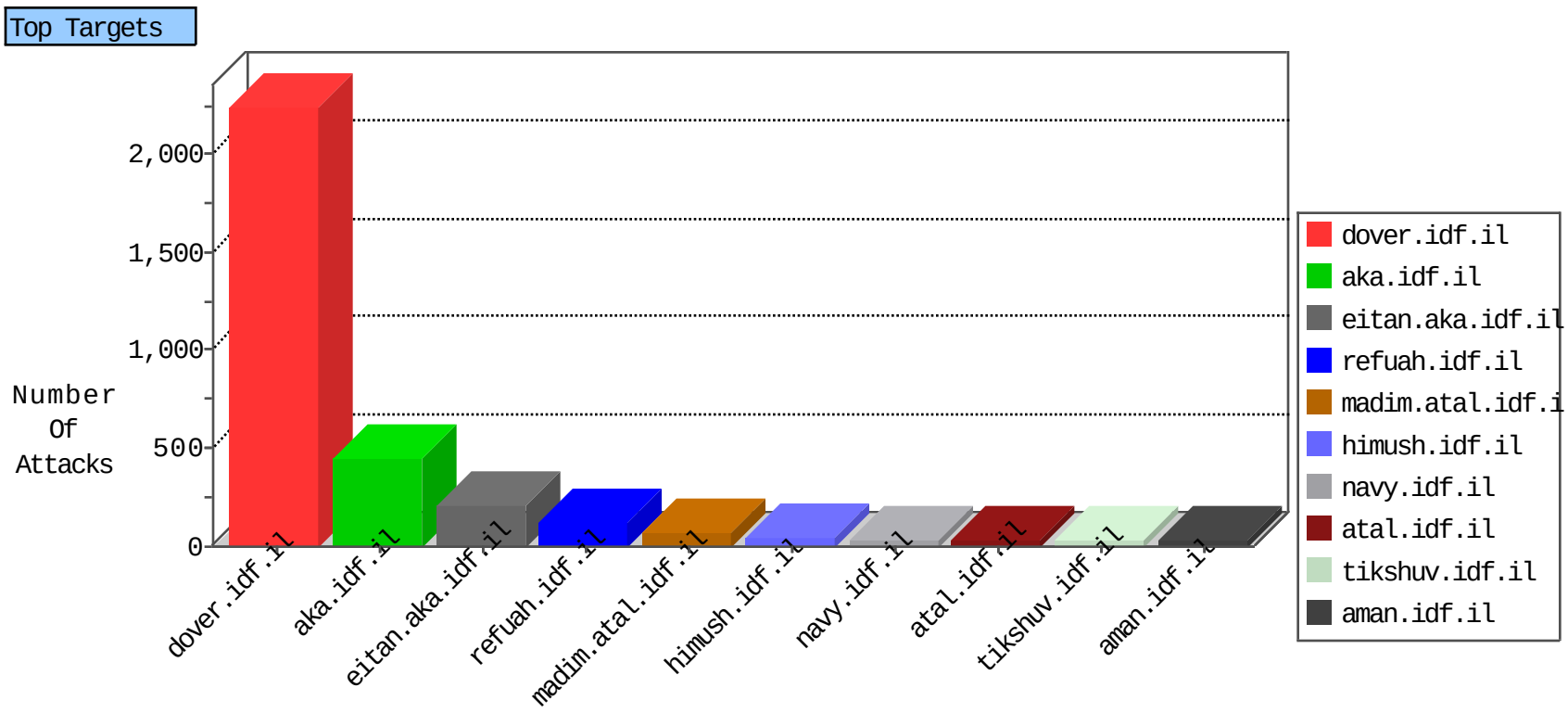
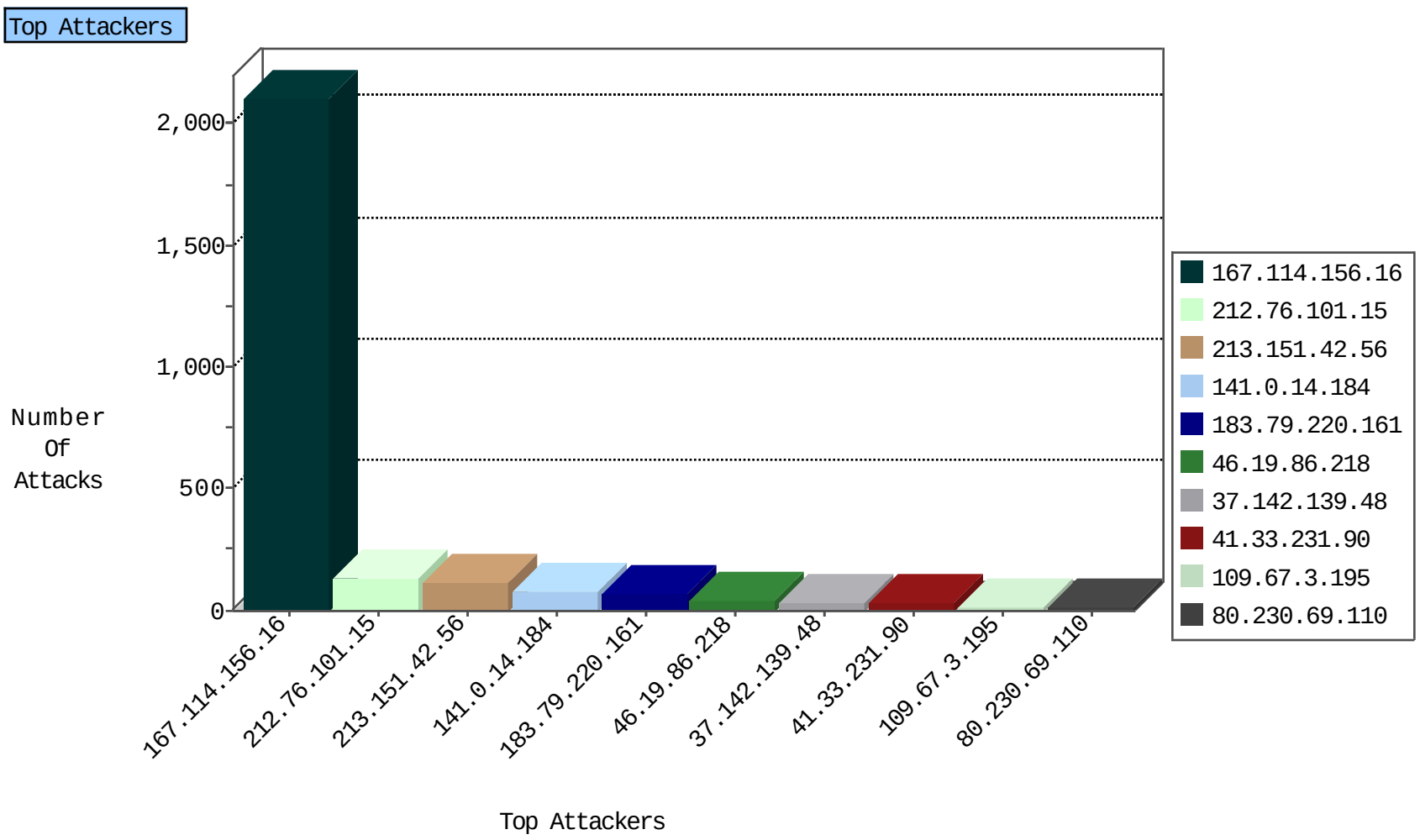
12-14-2015-20:04:09 to 12-14-2015-21:04:09

IDF Under Attack Daily Report





12-14-2015-20:04:09 to 12-14-2015-21:04:09

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	3262
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
79.181.133.131	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1

12-14-2015-20:04:09 to 12-14-2015-21:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-14-2015-20:04:09 to 12-14-2015-21:04:09

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
31.210.186.138	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
31.210.186.138	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
98.119.105.221	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
31.14.252.194	147.237.76.39	Romania	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
31.14.252.194	147.237.76.30	Romania	himush.idf.il	ET SCAN Potential SSH Scan	1
5.102.254.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
212.199.57.194	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
2.54.141.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
149.78.182.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.229.53.89	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.208.239.24	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
31.14.252.194	147.237.76.34	Romania	yohalan.idf.il	ET SCAN Potential SSH Scan	1
84.108.70.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.97.172.218	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
221.231.6.246	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.28.178.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
162.252.240.179	147.237.77.205	Canada	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
149.78.81.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-14-2015-20:04:09 to 12-14-2015-21:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.0.14.184	Europe	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	74
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	48
212.76.101.15	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
80.230.69.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
199.190.224.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.67.3.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
213.57.137.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.54.15.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
132.66.237.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.98	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.64.188.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.100	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.186.156	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.126.185.53	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
2.54.153.131	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.186.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.138.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.78.181.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.126.185.53	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.142.126.168	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.129.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
188.120.148.151	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.32.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.151.37.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.219.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.129.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.160.150.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.121.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.113.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.206.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.42.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.187.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.213	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.27.105.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.56.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.46.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.172.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.149.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.120.219.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
176.13.6.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

12-14-2015-20:04:09 to 12-14-2015-21:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.42.56	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.151.42.56	Block	118
212.76.101.15	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
149.88.180.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.220.161	Block	9
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Illegal HTTP Version from 183.79.220.161	Block	9
176.13.3.147	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	8
185.120.125.5		147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	7
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
149.88.23.102	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	5
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
79.183.60.197	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	3
85.64.201.39	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.125.5		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
176.13.0.206	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
46.117.134.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.141.140	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
71.65.240.113	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 37.142.139.48	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 37.142.139.48	Block	2
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	2
71.65.240.113	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 37.142.139.48	Block	2
176.12.143.88	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
81.218.140.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.52.147.131	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
77.127.22.245	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 37.142.139.48	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 37.142.139.48	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 37.142.139.48	Block	2
85.250.78.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
79.182.49.142	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
77.125.2.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
37.142.144.14	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
2.54.57.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 37.142.139.48	Block	2
24.184.33.244	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 37.142.139.48	Block	2
157.55.39.88	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
84.229.192.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 112 cookies	Block	1
79.180.113.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
40.77.167.61	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
124.218.68.149	Taiwan	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1

12-14-2015-20:04:09 to 12-14-2015-21:04:09