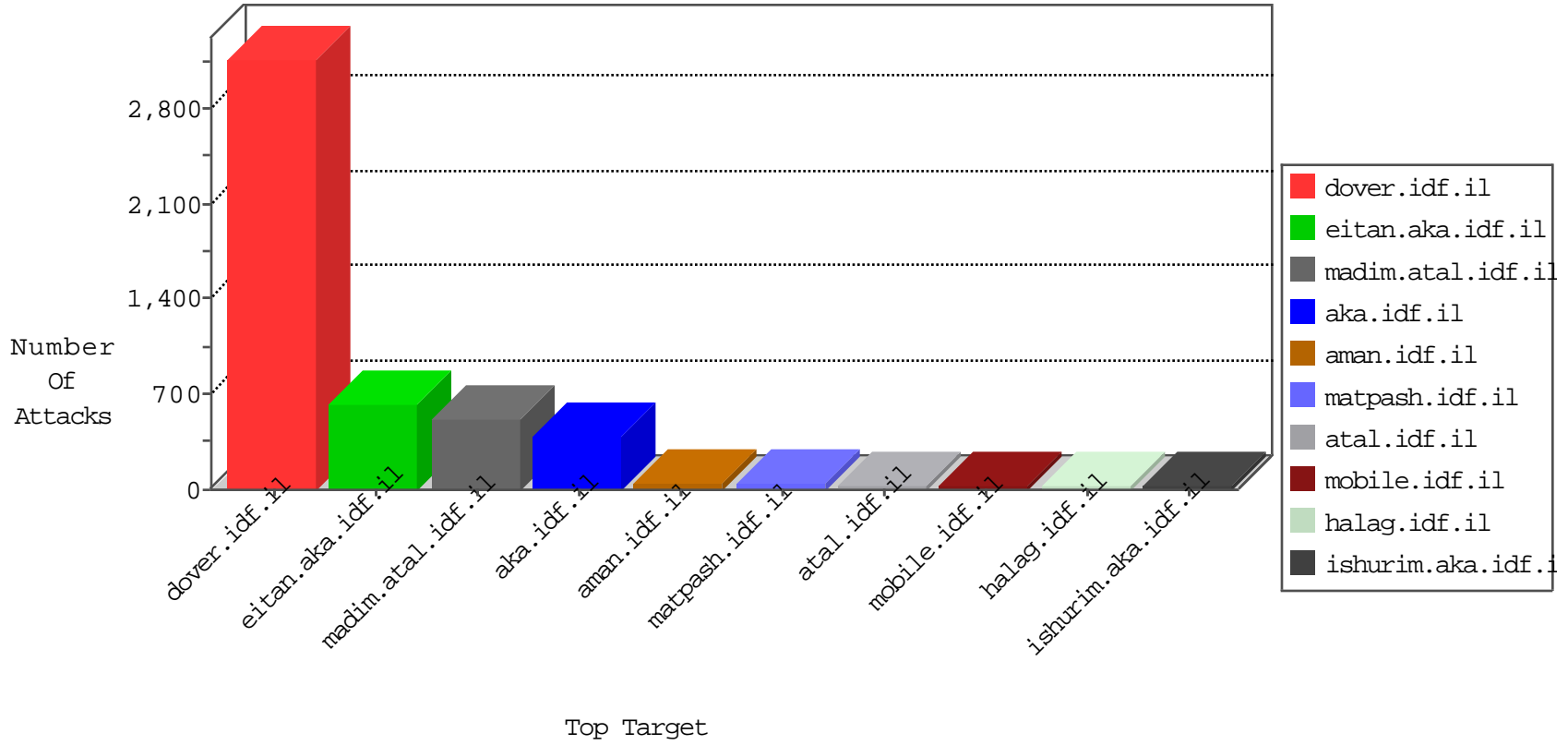


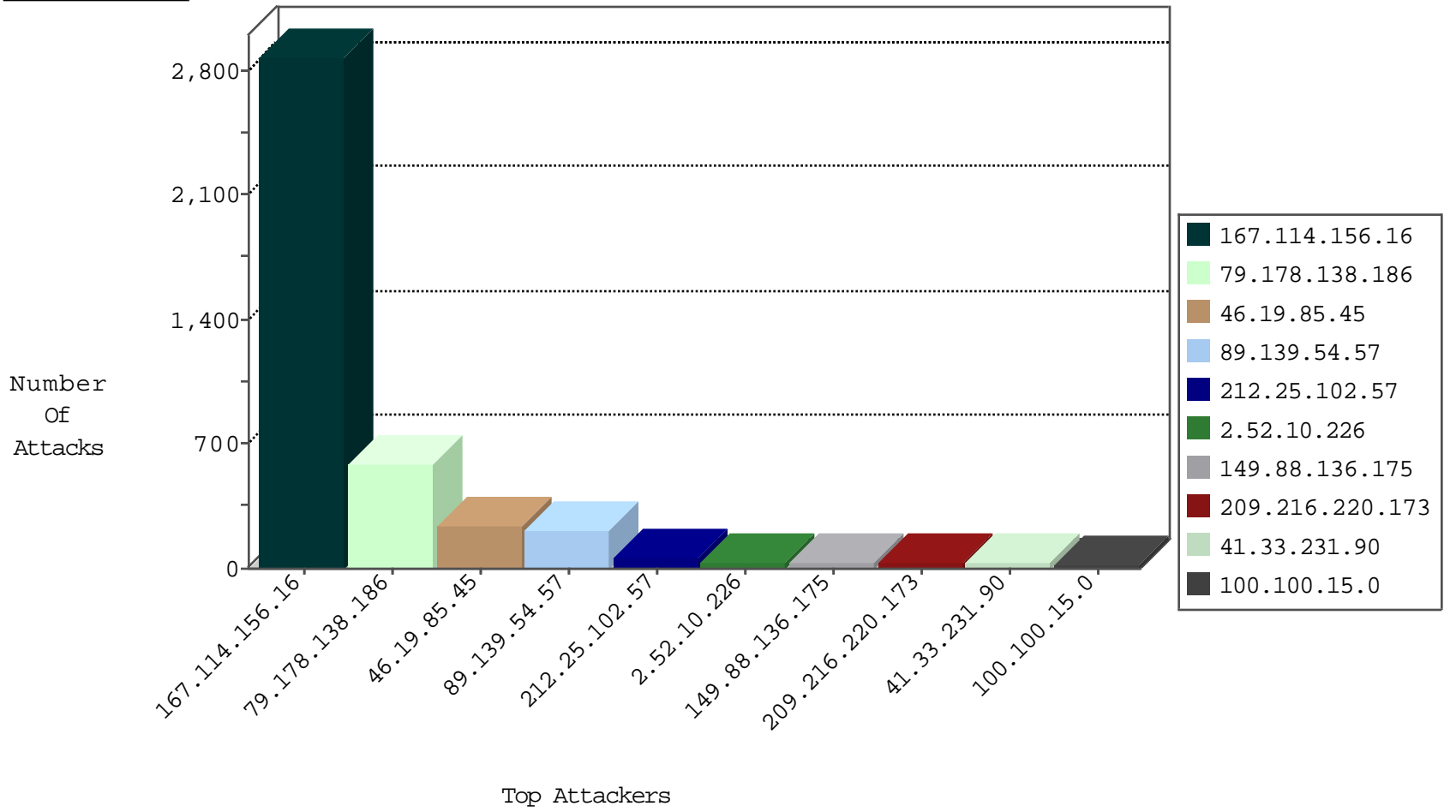
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3535
94.102.56.238	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

12-03-2015-19:04:04 to 12-03-2015-20:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

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
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
212.199.57.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.7.124.245	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
187.35.143.28	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.27.105.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.25.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.152.66	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	1
79.183.15.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.137.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.161.81.221	147.237.0.35	Mexico	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.52.10.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.46	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
183.179.171.73	147.237.76.31	Hong Kong	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.49.102	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
85.250.241.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.194.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.121.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.138.186	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	519
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
209.216.220.173	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	30
107.167.107.131	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
192.114.23.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
212.25.102.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
149.78.227.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
87.69.38.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
80.179.22.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.15.0		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.15.0		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.52.10.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
95.35.252.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
109.64.61.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.85.254	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
5.102.254.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.176.18.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.90.147.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
100.100.111.81		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.52.10.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.10.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.0.64		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.9.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.0.64		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.179.182.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.10.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.10.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.32.179.181	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.111.14.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.143.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.29.156.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.61.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.109.152.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.144.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.136.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.253	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.152.105	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.6.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.29.62.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
81.218.55.253	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.176.120.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
89.139.54.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
79.178.138.186	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
89.139.54.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.25.102.57	Block	41
89.139.54.57	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.54.57	Block	25
149.88.136.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
84.108.45.164	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.45.164	Block	9
2.52.131.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
87.228.117.183	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
176.13.12.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
87.228.117.183	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.228.117.183	Block	5
176.13.23.146	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
2.54.158.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
82.220.34.22	Switzerland	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
87.69.40.64	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
46.19.85.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.81	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.81	Block	3
5.29.34.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/sachar	Block	3
84.108.45.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
79.177.63.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
82.220.34.22	Switzerland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	2
37.142.233.109	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.233.109	Block	2
193.201.224.186	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
79.177.63.31	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.63.31	Block	2
31.210.186.143	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.210.186.143	Block	2
79.181.58.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
37.142.68.73	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/xmlrpc.php	Block	1
66.249.66.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
176.106.226.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/30/	Block	1
150.70.173.59	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
5.29.62.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.152.66	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.120.76.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.23.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
80.179.223.31	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
213.8.174.25	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
193.201.224.186	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
46.19.85.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/rabanut/general.aspx	Block	1
176.13.3.96	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
31.210.186.143	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
87.69.38.135	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 87.69.38.135	Block	1
2.54.150.219	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
66.249.66.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/rabanut/general.aspx	Block	1