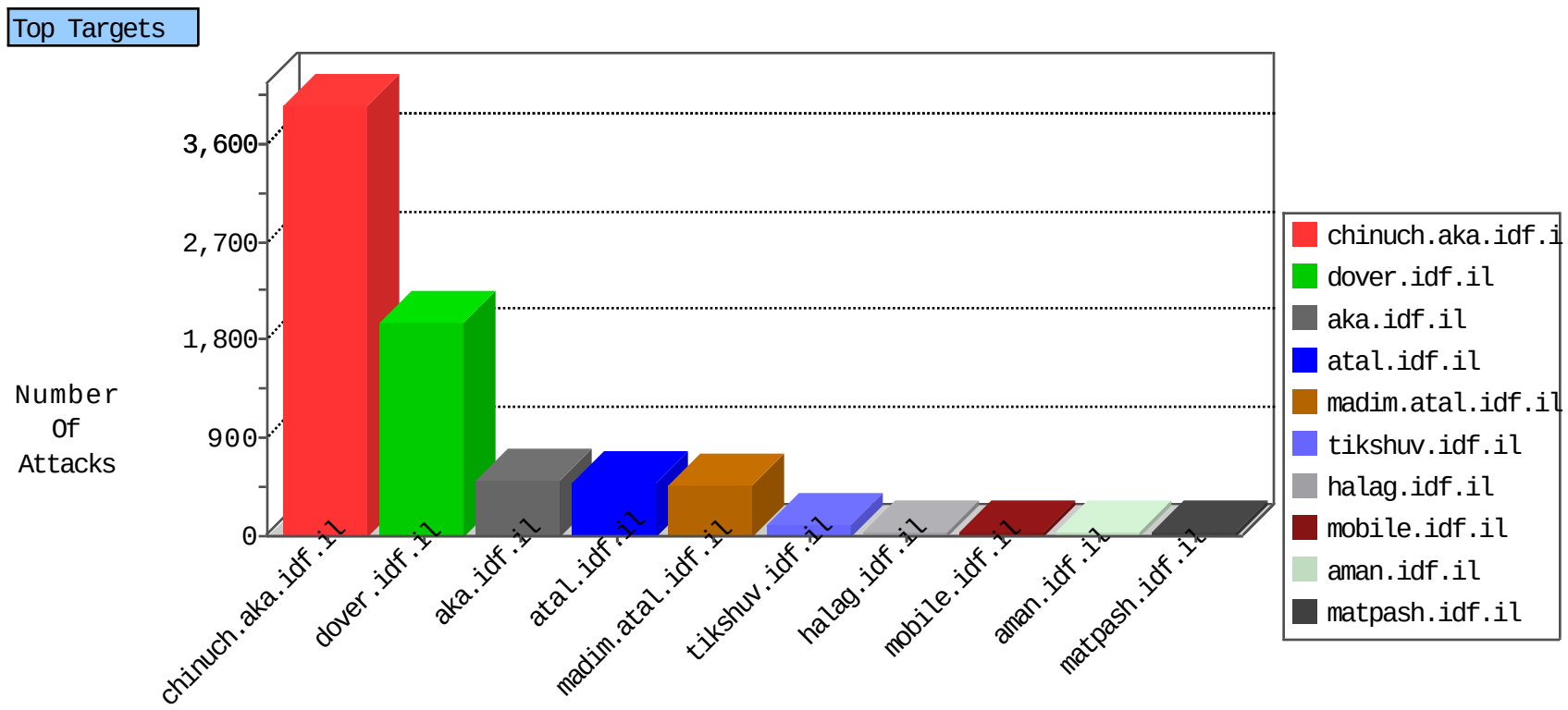
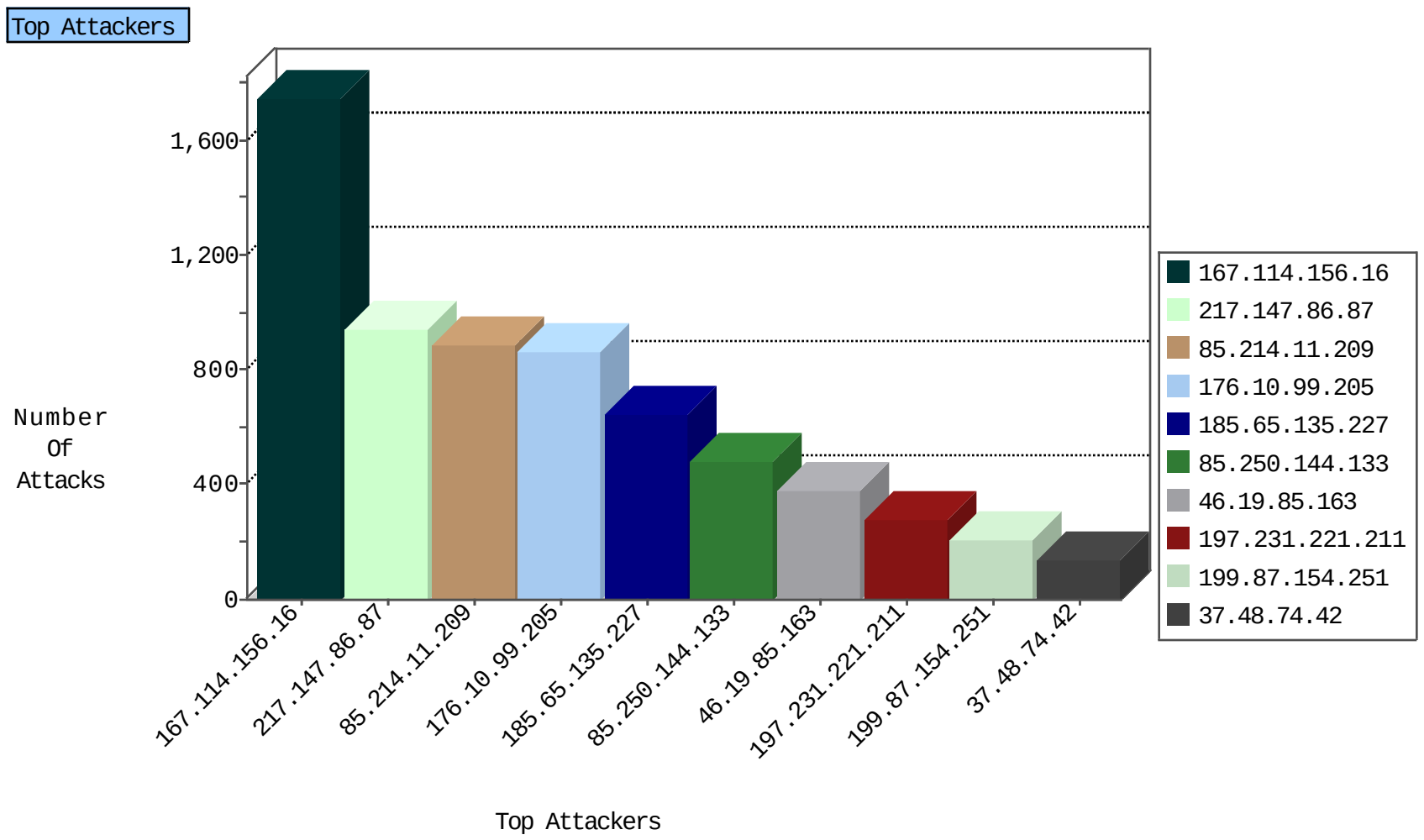
01-11-2016-12:04:02 to 01-11-2016-13:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-11-2016-12:04:02 to 01-11-2016-13:04:02

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	3133
66.249.73.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	265
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
37.29.108.204	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	L4 Source or Dest Port Zero	drop	1
107.150.60.74	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
168.235.197.60	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
107.150.60.246	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
23.95.248.111	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.158	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.213	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
37.29.108.204	Russian Federation	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	1
107.150.55.212	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1

01-11-2016-12:04:02 to 01-11-2016-13:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-11-2016-12:04:02 to 01-11-2016-13:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
84.108.66.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.73.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.121.135.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.15.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.43.246.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.98.200.238	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
109.253.206.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.111.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.234	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
62.219.54.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.118.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.58.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
172.98.200.238	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.77.74	Italy	law.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.162.131	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1

01-11-2016-12:04:02 to 01-11-2016-13:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.250.144.133	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	463
37.48.74.42	Netherlands	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	68
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
155.250.255.143	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
5.102.254.140	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	20
5.102.254.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
192.116.190.206	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
85.250.144.133	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
155.250.255.143	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
141.0.14.218	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
2.54.151.240	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.213.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
147.235.8.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
37.48.74.42	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
147.235.8.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.114.91.245	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.114.91.245	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.149.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.223	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.0.244.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.32	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.220.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
62.0.219.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
192.114.91.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.150.82.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.201.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.114.91.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.32	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.127.201.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.3.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.135.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.223	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.0.208.1	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.64.82.209	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.219.151.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.130.234	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.219.151.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

01-11-2016-12:04:02 to 01-11-2016-13:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.147.86.87	United Kingdom	147.237.76.147	chinuch.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	939
85.214.11.209	Germany	147.237.76.147	chinuch.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	887
176.10.99.205	Switzerland	147.237.76.147	chinuch.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	833
185.65.135.227	Sweden	147.237.76.147	chinuch.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	644
197.231.221.211	Liberia	147.237.76.147	chinuch.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	279
199.87.154.251	Canada	147.237.76.147	chinuch.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	210
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	193
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	189
176.13.6.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.198.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.19.86.167	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.19.86.167	Block	12
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	4
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	4
109.253.211.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.82.209	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.82.209	Block	3
95.35.83.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.45.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.226.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.120.126.115		147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 185.120.126.115	Block	2
2.54.53.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	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
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
2.54.5.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.193.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.115		147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 185.120.126.115	Block	2
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
77.125.79.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.120.126.115		147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 185.120.126.115	Block	2
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
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	1
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.17.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.126.115		147.237.77.216	dover.idf.il	Unknown HTTP Request Method Ã¿Ã»[[#31]]Ã¿Ã» in URL	Block	1
5.102.254.140	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
176.13.0.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.232.54	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
132.70.66.12	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.25.67.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.113	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.146.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.43.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.126.115		147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL	Block	1

01-11-2016-12:04:02 to 01-11-2016-13:04:02