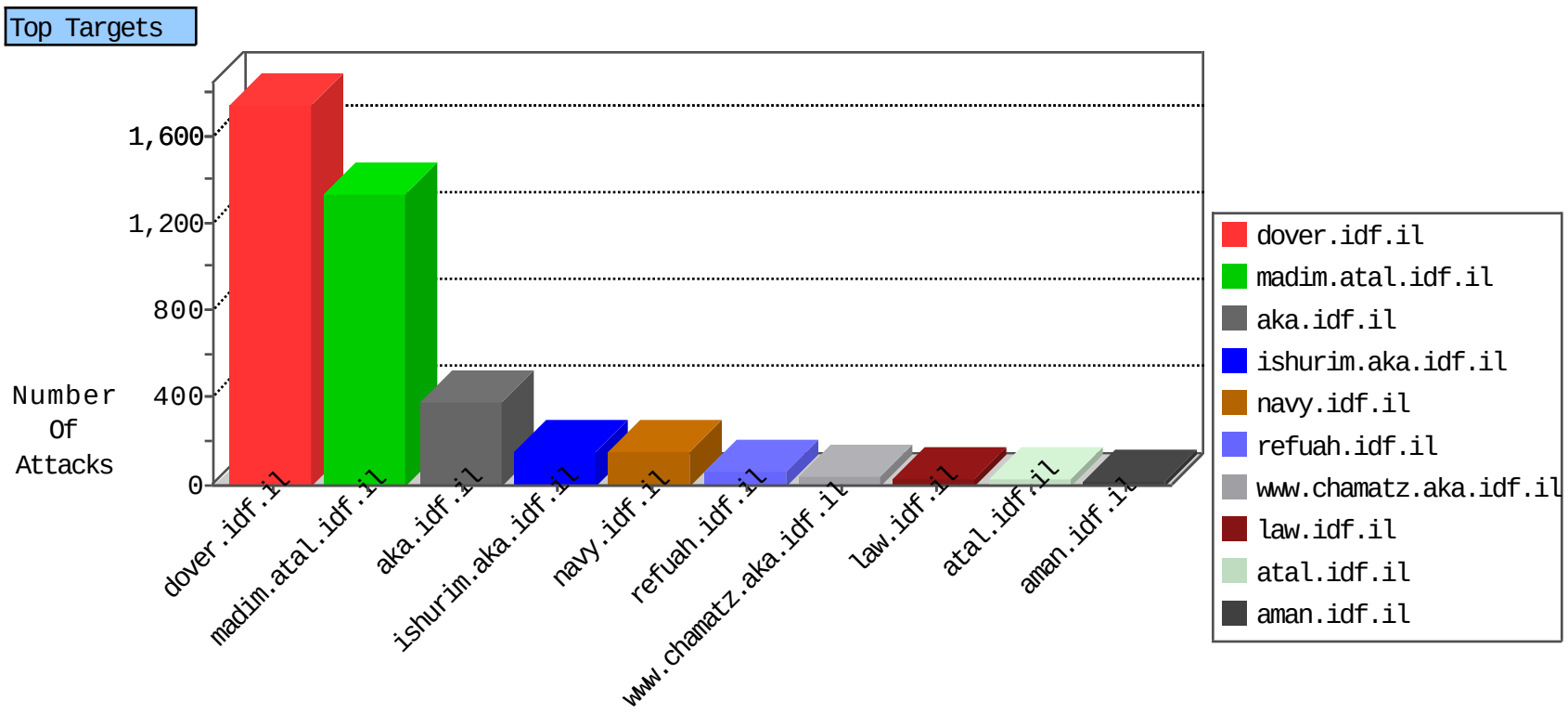
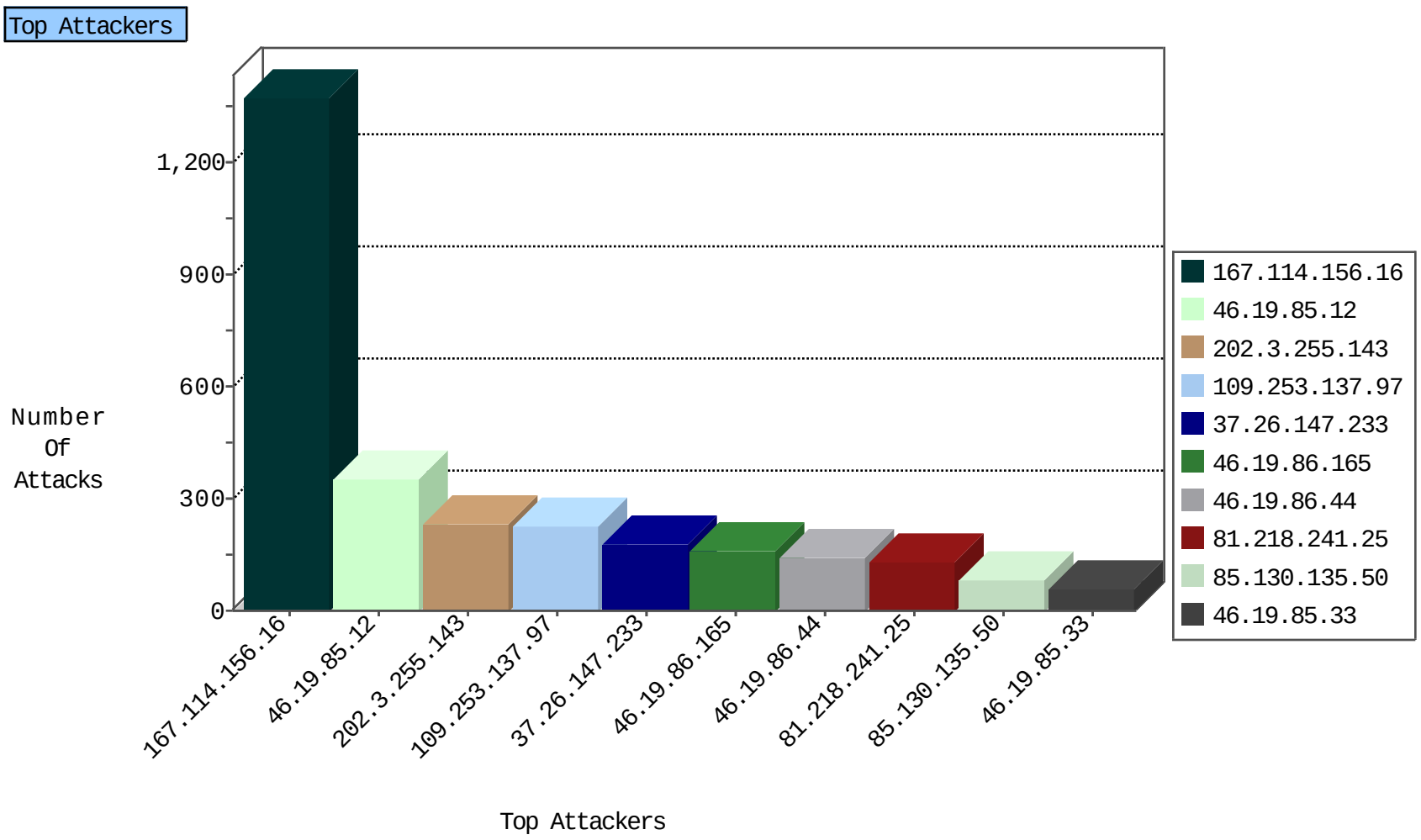
01-17-2016-08:04:02 to 01-17-2016-09:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-17-2016-08:04:02 to 01-17-2016-09:04:02

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	3374
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	419
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	87
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	37
109.67.127.174	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
185.130.5.228		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
156.201.94.22		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
88.254.254.3	Turkey	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
156.201.94.22		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1

01-17-2016-08:04:02 to 01-17-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-17-2016-08:04:02 to 01-17-2016-09:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	194
87.69.74.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.17.69.169	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
14.17.69.169	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.2.12	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
101.108.105.207	147.237.77.74	Thailand	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.64.62.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.17.69.169	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
2.52.151.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
105.226.112.224	147.237.0.16	South Africa	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

01-17-2016-08:04:02 to 01-17-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.135.50	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	40
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
148.177.129.212	Europe	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	24
79.183.113.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
82.166.53.161	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	24
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
185.89.217.226		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
185.89.217.233		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
85.130.223.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
185.89.217.230		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
85.130.223.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.86.233	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.254	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
185.89.217.228		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
109.253.215.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.227		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
185.89.217.231		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
185.89.217.232		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
185.89.217.229		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
185.89.217.225		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
185.89.217.235		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
85.130.135.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
72.9.148.10	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
85.130.135.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.109.82.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
149.88.12.13	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.19.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.234		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.108.219.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.135.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
93.157.84.34	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
37.142.188.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.143	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.43.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

01-17-2016-08:04:02 to 01-17-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.137.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	192
46.19.85.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	175
46.19.85.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
37.26.147.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
37.26.147.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
46.19.85.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
37.26.146.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
80.246.136.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	37
109.253.137.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
46.19.86.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	22
109.253.143.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
109.253.145.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.131.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.215.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.102.193.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.153.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed 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/1133-22461-he/dover.aspx.	Block	2
176.13.16.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
149.78.23.72	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 149.78.23.72	Block	2
2.52.140.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.166.190.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
40.77.167.96	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
184.105.247.196	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.102.9.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
213.151.36.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1783-he/refuah.aspx&sa=u&ved=0ahukewjj6fbyobdkahuflhokhxbtcfsqfgglmae&sig2=vpsqkul75cftlisu0t58qq&usg=afqjcneg6rddoj0zlogbaqalfvydqhveca	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.246.136.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.115.94.2	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	1
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
149.202.74.134	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
46.121.220.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
207.46.13.24	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmiluim/templates/www.behazdaa.org	Block	1
85.64.241.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-17-2016-08:04:02 to 01-17-2016-09:04:02