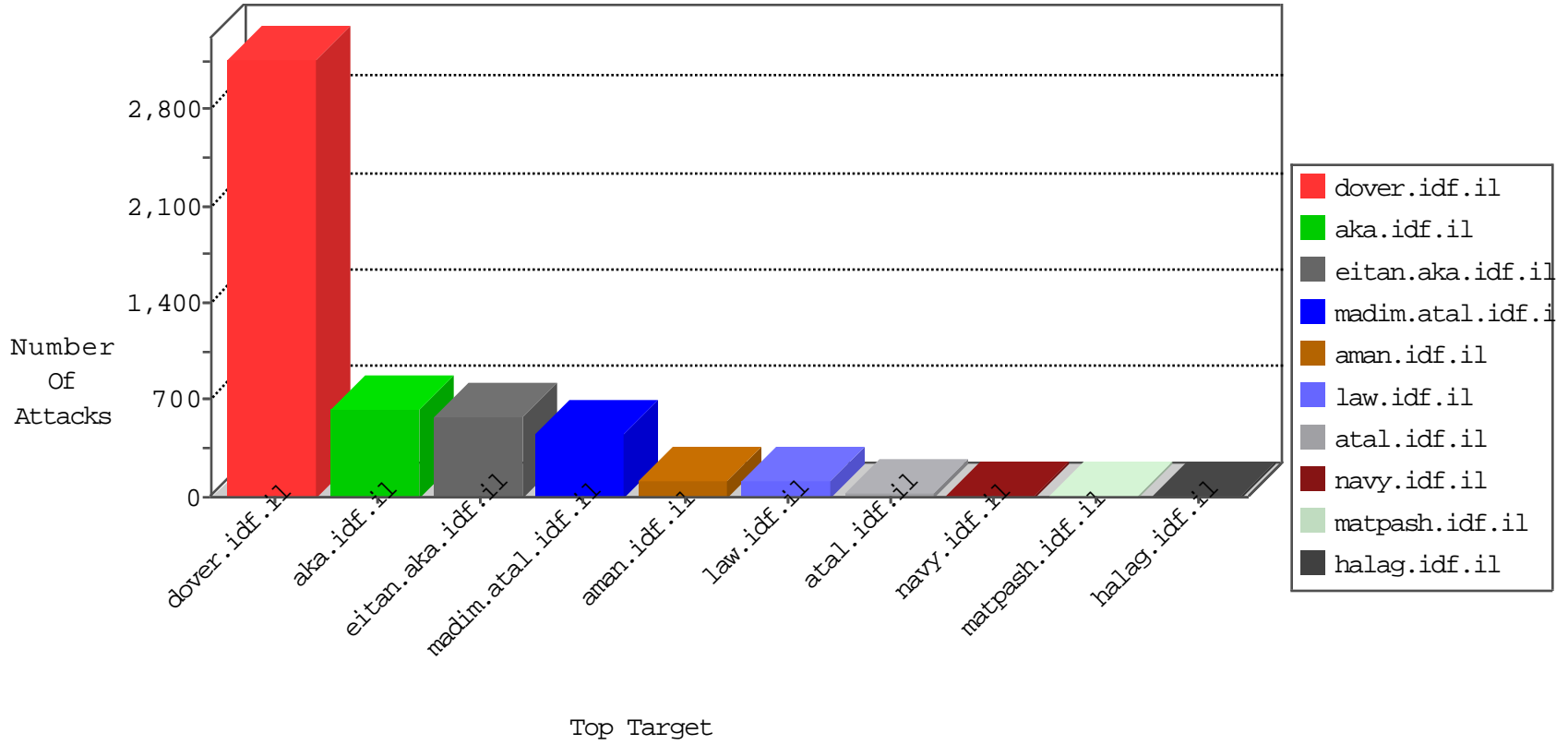


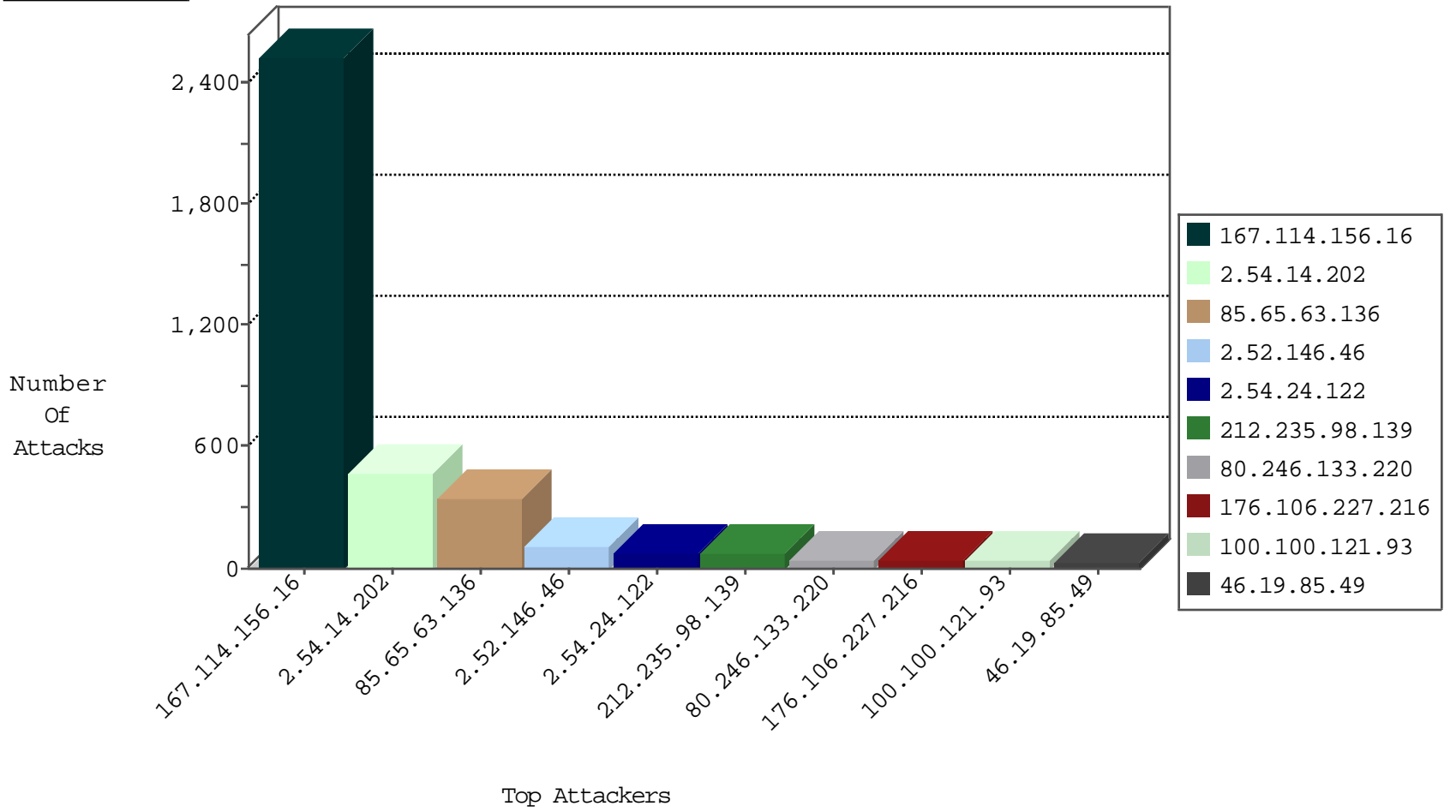
IDF Under Attack Daily Report



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	3567
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
192.3.170.124	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

12-01-2015-18:04:06 to 12-01-2015-19:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	3
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
84.109.240.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.185.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.218.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
176.12.141.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.25.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.206.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.14.202	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	429
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	73
2.52.146.46	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	63
100.100.121.93		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	23
93.172.25.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
176.13.14.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.176.198.68	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
100.100.1.138		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.149.171	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.52.146.46	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.52.146.46	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.125.145.18	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.146.46	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.60.172	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
62.0.197.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.3.126	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.50	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
109.65.52.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.140.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
213.57.130.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.138	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.52.146.46	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
100.100.56.63		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
79.181.190.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.134.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.106.227.216	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.63.136	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.63.136	Block	176
85.65.63.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
2.54.24.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
85.65.63.136	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 85.65.63.136	Block	54
80.246.133.220	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
176.106.227.216	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
2.54.14.202	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.14.202	Block	38
37.26.148.181	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	14
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.52.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.0.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.136.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.66.25	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
168.61.42.209	United States	147.237.77.216	doover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/doover.aspx	Block	5
212.179.21.194	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	4
195.62.28.15	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.250.97.59	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
176.13.10.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.48.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	3
176.13.11.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.75.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
176.12.142.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
194.100.58.154	Finland	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
176.13.10.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.100.58.154	Finland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/index.php	Block	2
195.62.28.15	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/index.php	Block	2
83.37.210.47	Spain	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
77.125.75.129	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.75.129	Block	2
194.100.58.154	Finland	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
37.26.146.205	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
46.120.99.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Å	Block	2
176.13.0.167	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.52.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.143.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.36.174.122	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
93.173.161.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.62.28.15	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.62.28.15	Block	1
66.249.66.43	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20315-he/doover.aspx	Block	1
164.138.113.248	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ahukewjvznabjrvjahxgthqkhsxvncqfvggnmaa&usg=afqjcnhcdsh5ryhkeugapxlds7fowjwnw	Block	1
46.120.206.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.168.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
2.54.27.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.188	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
185.120.126.44		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.34	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
107.178.194.83	United States	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/doover.aspx.	Block	1
79.178.61.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1