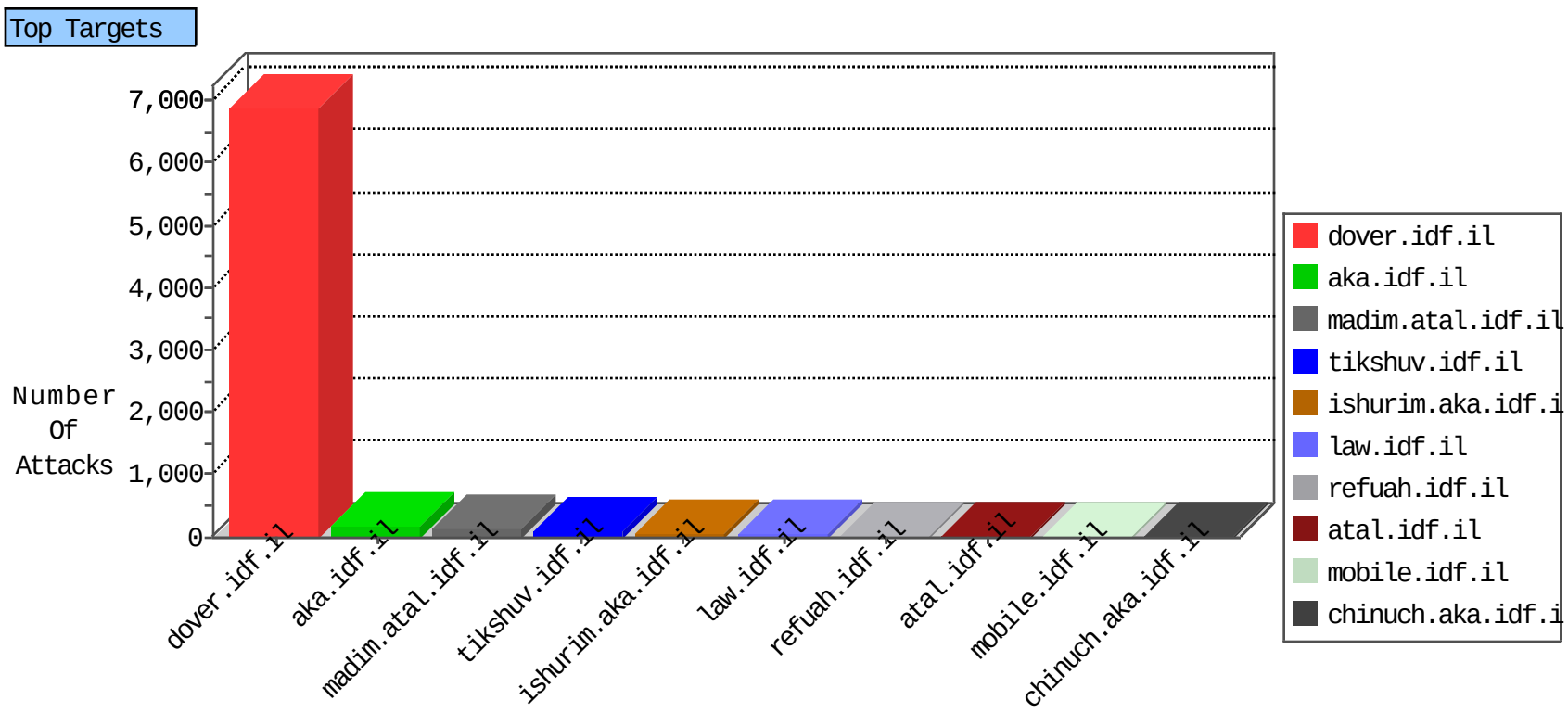
01-14-2016-22:04:03 to 01-14-2016-23:04:03

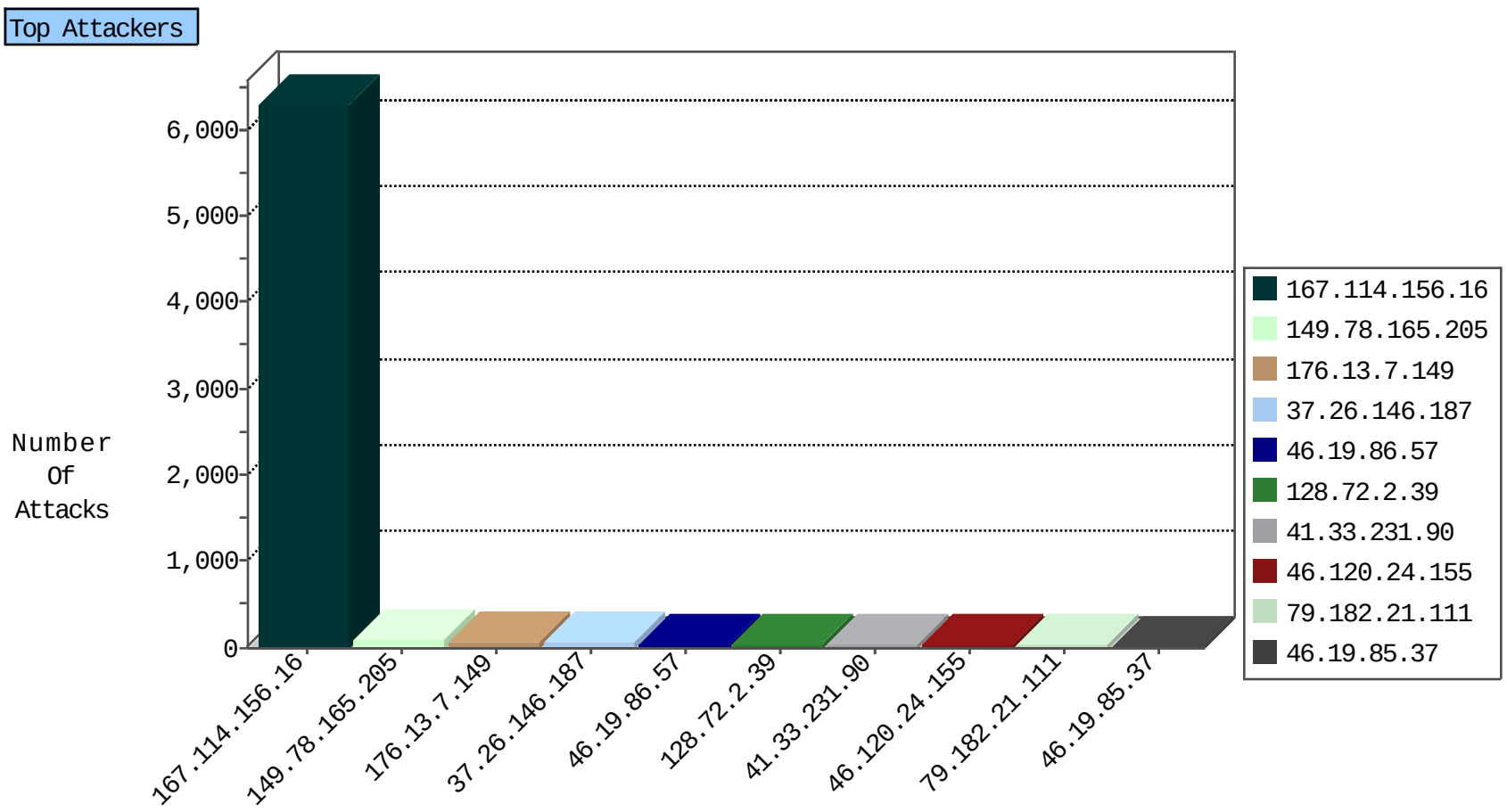
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-14-2016-22:04:03 to 01-14-2016-23:04:03

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	3499
37.26.146.187	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
31.25.76.152	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
37.26.146.187	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
66.249.65.224	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
66.249.65.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.109.130.231	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
157.55.39.53	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
157.55.39.168	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
157.55.39.169	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
181.51.71.15	Colombia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
157.55.12.89	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
157.55.39.167	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3
157.55.39.52	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
40.77.167.42	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
173.252.90.249	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
115.238.231.71	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
188.103.124.129	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
157.55.39.53	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
188.103.124.129	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
157.55.39.53	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
173.252.90.249	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
115.238.231.71	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
198.154.60.27	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
173.252.74.118	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
66.220.156.105	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
173.252.90.83	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
115.238.231.71	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
186.150.253.154	Dominican Republic	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-14-2016-22:04:03 to 01-14-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-14-2016-22:04:03 to 01-14-2016-23:04:03

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
84.108.111.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.252.90.249	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
92.124.149.244	147.237.8.27	Russian Federation	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.183.23.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

01-14-2016-22:04:03 to 01-14-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2781
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2247
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop		drop	860
46.19.86.57	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
128.72.2.39	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	42
46.120.24.155	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
84.94.96.73	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.146.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
213.8.204.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
2.54.42.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
99.95.213.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.147.176	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.210.186.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
191.37.159.68	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.130.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.99	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.198	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.253.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
191.37.159.68	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
212.179.210.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.15.199	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.179.210.200	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.177.15.199	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.103.124.129	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.180.145.247	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.120.24.155	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
93.172.246.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.179.210.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.25.16	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
40.77.167.42	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.78.248.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.104.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-14-2016-22:04:03 to 01-14-2016-23:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.165.205	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 149.78.165.205	Block	107
176.13.7.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
79.182.21.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
77.126.151.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
5.29.92.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.52.131.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.169.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.145.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.156.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
5.102.253.4	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.158.139.107	United Kingdom	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
2.54.174.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.159.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.94.84.124	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 84.94.84.124 (Open Mode)	None	1
157.55.39.50	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/61998	Block	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Language: in URL he-il,he	Block	1
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.168.115	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
85.158.137.195	Europe	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 85.158.137.195 (Unknown SSL Session)	None	1
207.46.13.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
79.181.69.129	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
2.54.42.25	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.54.42.25	Block	1
128.232.110.29	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
62.141.39.119	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Malformed URL he-il,he;q=0.8,en-us;q=0.6,en;q=0.4	Block	1
213.8.204.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
95.86.92.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.253.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.116.166.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.77.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.15.199	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
157.55.39.169	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/3/	Block	1
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.118.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/home.aspx	Block	1
85.158.137.195	Europe	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
37.142.252.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.140.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.19.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.99.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.165.205	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
66.216.170.29	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.111	Block	1
213.8.204.55	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
193.81.143.124	Austria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
84.109.32.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-14-2016-22:04:03 to 01-14-2016-23:04:03