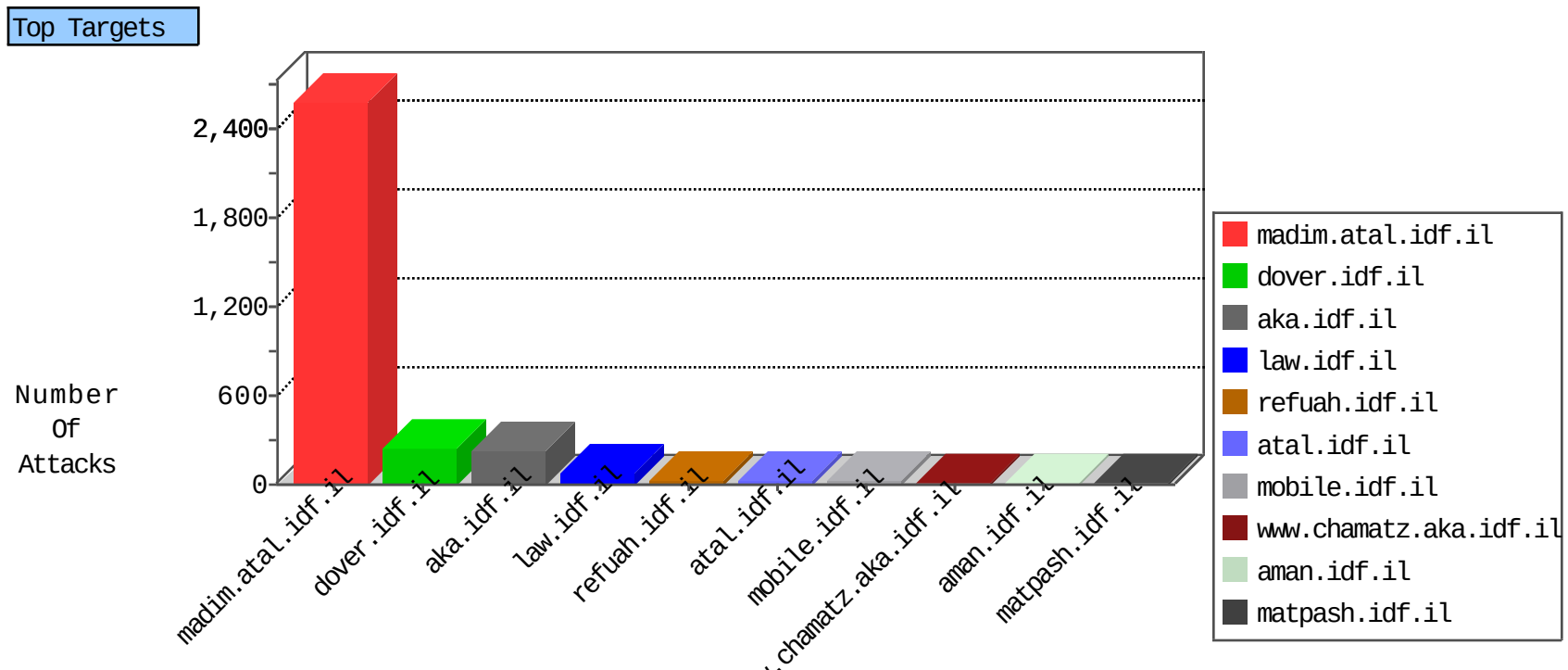
01-27-2016-22:04:07 to 01-27-2016-23:04:07

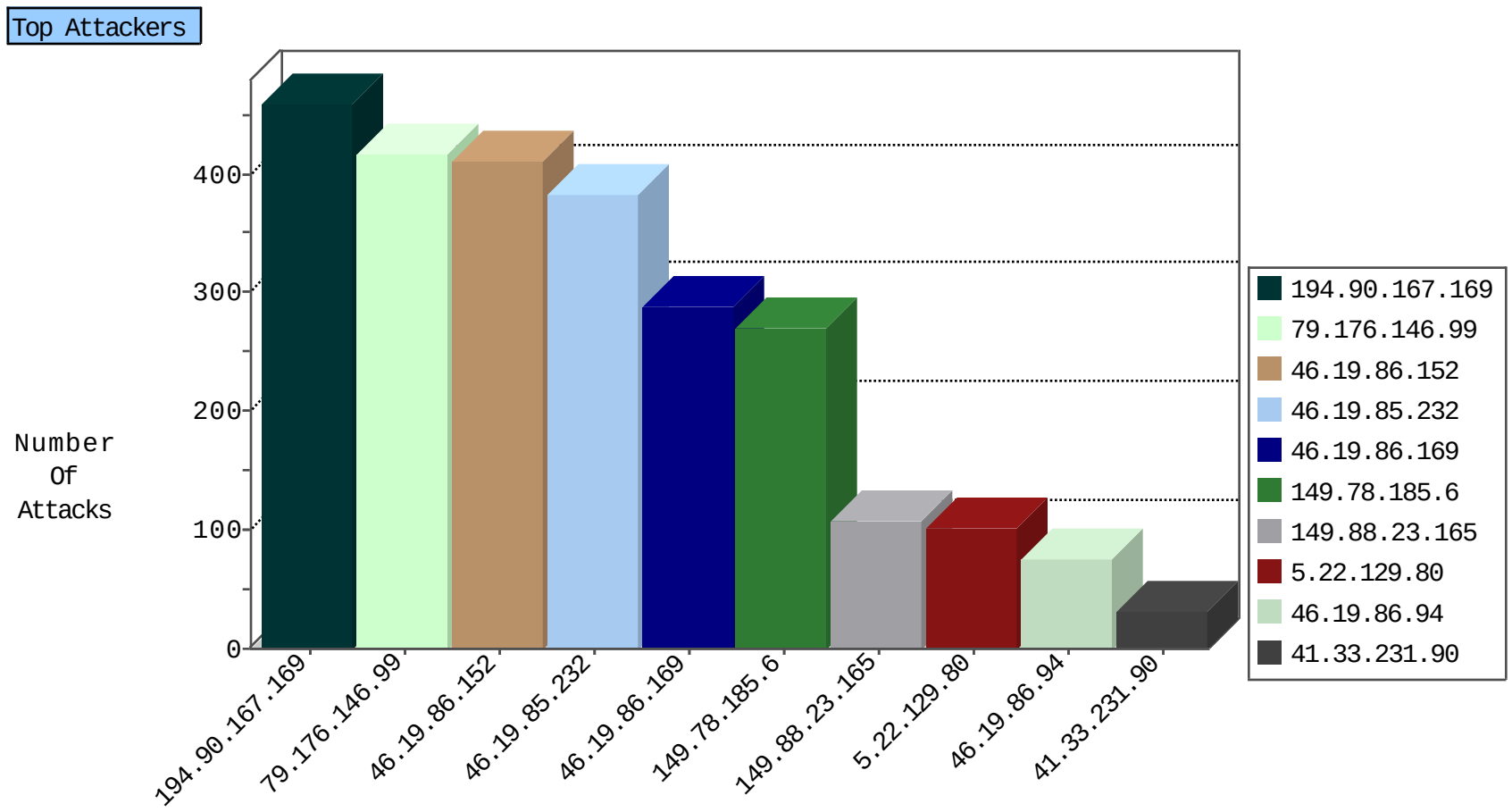
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-27-2016-22:04:07 to 01-27-2016-23:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.67.38.74	United States	147.237.76.31	nakchal.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
208.73.206.244		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

01-27-2016-22:04:07 to 01-27-2016-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.196.151	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-27-2016-22:04:07 to 01-27-2016-23:04:07

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
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.179	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.197	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1

01-27-2016-22:04:07 to 01-27-2016-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
149.88.20.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
77.127.192.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.246	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	12
194.90.167.169	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
130.193.50.7	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.10.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.188.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.24	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
93.158.152.46	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
66.249.81.174	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.242	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
188.120.148.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.170	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.22.135.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.183.224.89	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
130.193.37.18	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
185.84.71.86		147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.145.222.108	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.177.205.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
178.154.189.26	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
87.69.31.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.16.190	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.130.143	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.239	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.102.202.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
98.7.65.105	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

01-27-2016-22:04:07 to 01-27-2016-23:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.90.167.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	259
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	225
79.176.146.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	214
194.90.167.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	189
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	186
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	153
46.19.86.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	140
149.78.185.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	136
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
149.78.185.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	130
79.176.146.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
79.176.146.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	96
5.22.129.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
149.88.23.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	50
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	44
46.19.86.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	44
149.88.23.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
46.19.86.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	44
149.88.23.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
176.13.13.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
5.22.129.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	25
95.86.92.8	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.92.8	Block	9
80.246.139.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
185.32.179.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.111.233.25	Block	5
109.66.175.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
188.120.148.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.173.199	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.176.173.199	Block	2
84.228.177.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.183.3.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
37.26.148.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.138.171.95	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
109.253.201.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.136.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.176.173.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	2
207.46.13.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	2
176.13.22.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
91.200.12.5	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
84.110.144.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.230.86.170	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.35.170	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
84.94.32.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
5.29.171.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1

01-27-2016-22:04:07 to 01-27-2016-23:04:07