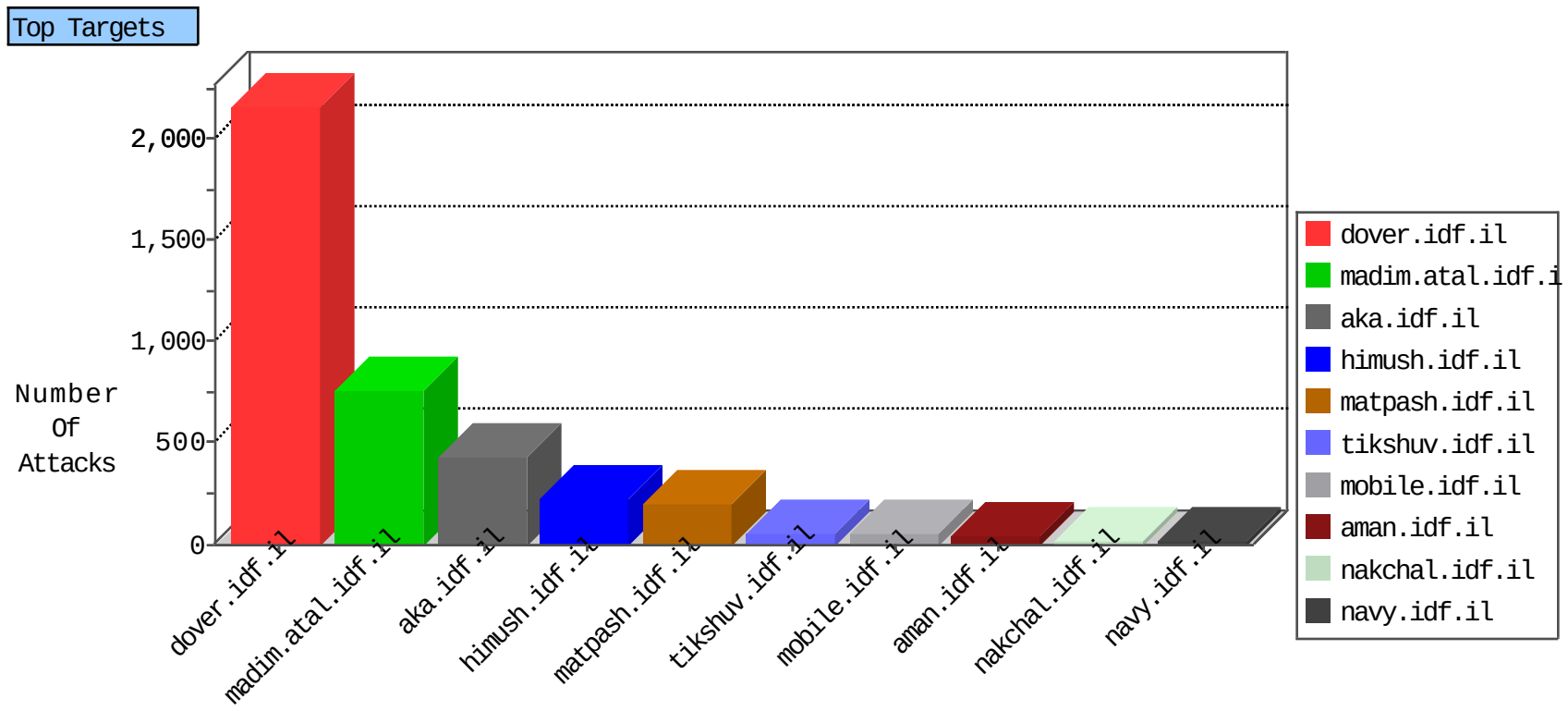
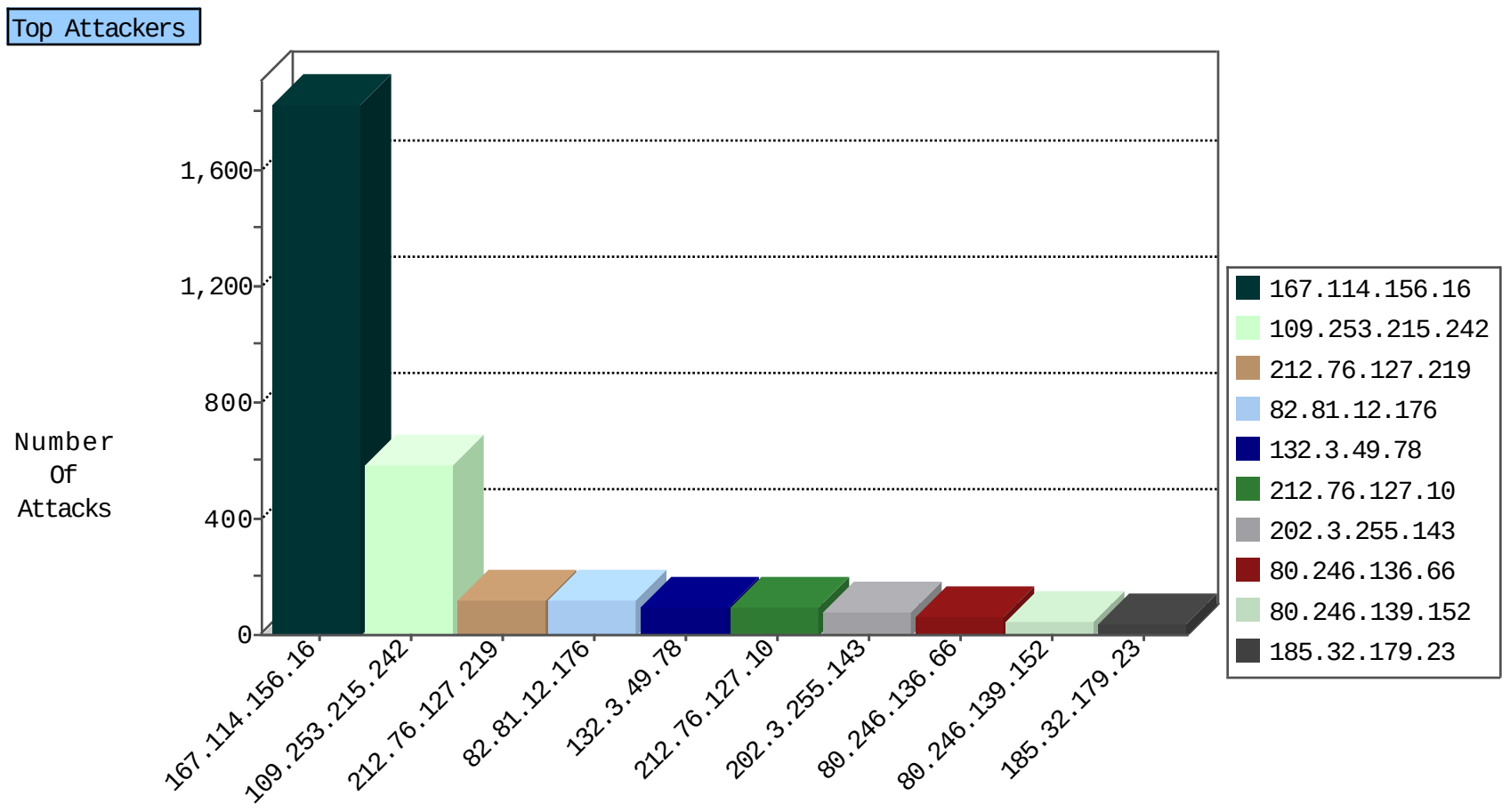
01-19-2016-19:04:04 to 01-19-2016-20:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-19-2016-19:04:04 to 01-19-2016-20:04:04

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	3004
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	118
157.55.39.161	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.46.102.242	Romania	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
119.244.207.6	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

01-19-2016-19:04:04 to 01-19-2016-20:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.178.197	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	30
77.127.59.212	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
136.243.5.215	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	4
109.64.162.50	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
89.139.148.131	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
84.109.212.72	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
46.119.121.146	Ukraine	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
199.30.24.180	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-19-2016-19:04:04 to 01-19-2016-20:04:04

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.i	GPL SCAN nmap TCP	43
177.185.192.77	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	4
46.120.81.127	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
66.249.78.165	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

01-19-2016-19:04:04 to 01-19-2016-20:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	120
132.3.49.78	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	97
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	93
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.178.36.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
132.3.49.81	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	22
75.145.80.5	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
132.3.49.80	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
132.3.49.79	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
75.145.80.5	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.176.138.214	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
79.176.138.214	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.180.33.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.98.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
132.3.49.82	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
176.13.15.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.117.163.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.243.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.73.222.143	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.64.166.224	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.191.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.11.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.213.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.7.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.176.106.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.73.222.143	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
72.186.5.22	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.73.222.143	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
212.76.127.111	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
31.210.187.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.126.13.26	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
176.77.96.18	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.43.109.21	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
109.64.2.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
109.64.2.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
80.178.187.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
144.76.182.149	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.62.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence 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
82.102.136.65	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
104.34.82.252	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
185.3.147.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

01-19-2016-19:04:04 to 01-19-2016-20:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	408
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.215.242	Block	63
80.246.136.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
80.246.139.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
185.32.179.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected ********** ********** ********** *, Observed ********** ********** **********	None	30
176.13.2.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
213.57.165.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
105.108.208.34	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/'	Block	3
176.13.18.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
144.76.182.149	Germany	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 144.76.182.149	Block	3
176.13.6.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.250.180.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
37.142.243.3	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
93.172.175.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.88.7.35	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
79.180.33.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.181.98.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
93.173.189.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.180.100.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.84	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.15.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.147.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.86.124.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.109.12.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.66.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1726	Block	1
149.88.85.150	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
79.180.209.103	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.29.127.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.204.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.13.26	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
185.24.233.96	Ireland	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
87.69.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sahar	Block	1
46.119.121.146	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
149.88.7.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
79.177.155.76	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
207.46.13.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ahukewj-ienfrp_jahvdtbqkhd8_cw0qfggnmaa&sig2=fknsk6ifabc6y15_vmmf7g&usg=afqjcnhcdsh5ryhkeugapxldsq7fowjwnw	Block	1
37.142.243.3	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	1
109.253.205.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
2.54.30.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
84.111.208.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.17	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
157.55.39.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ses.20.8afc=*	Block	1

01-19-2016-19:04:04 to 01-19-2016-20:04:04