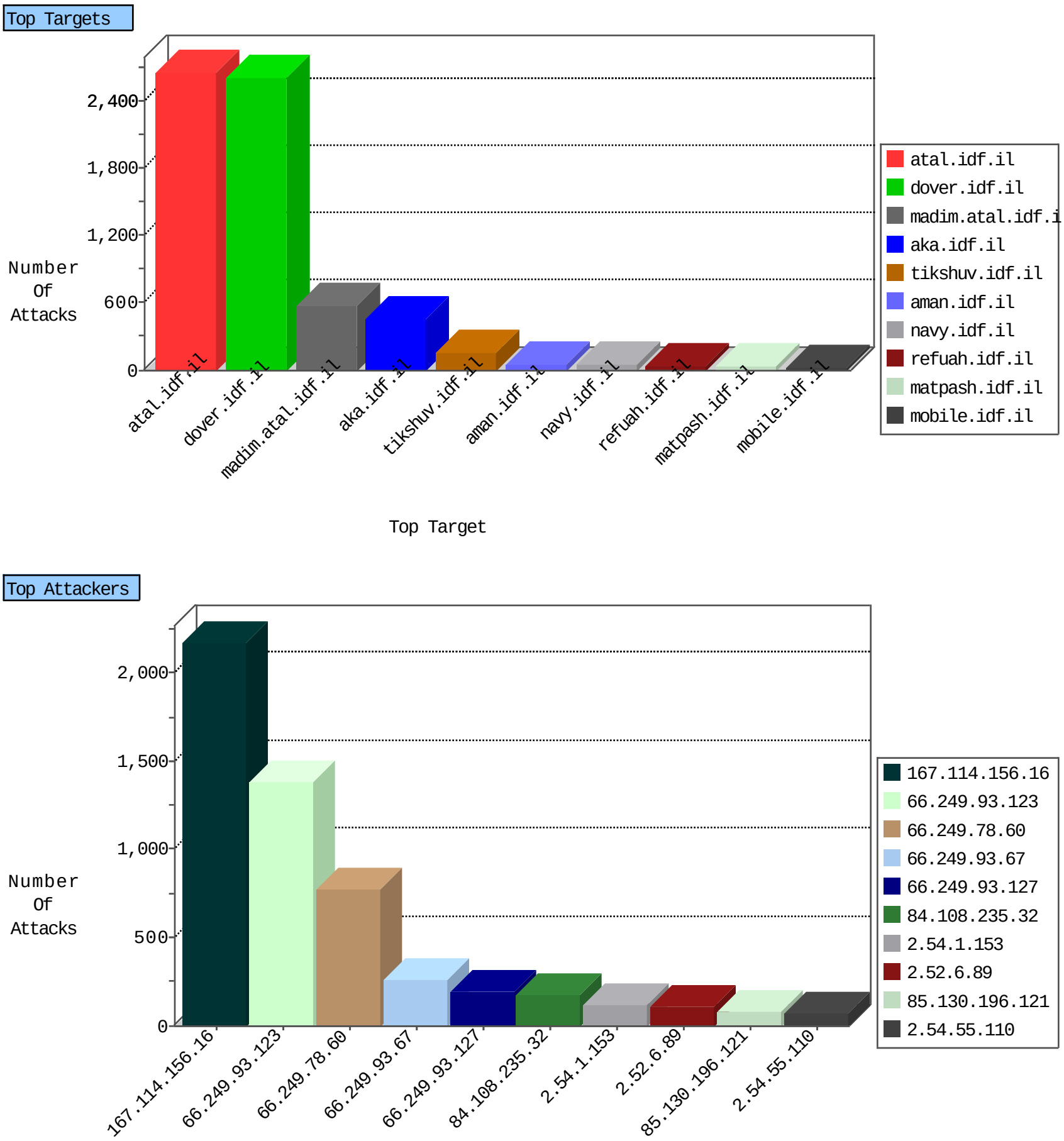
01-25-2016-18:04:04 to 01-25-2016-19:04:04

IDF Under Attack Daily Report



01-25-2016-18:04:04 to 01-25-2016-19:04:04

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	3035
109.67.165.217	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
14.105.246.213	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	1
81.218.56.125	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

01-25-2016-18:04:04 to 01-25-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.200.200	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-25-2016-18:04:04 to 01-25-2016-19:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.60	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	778
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
84.228.57.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.68	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.52.5.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
201.201.110.218	147.237.72.166	Costa Rica	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.159.147.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.206.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.108.21.7	147.237.77.216	Austria	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
213.8.204.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.188.22	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.172.144.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-25-2016-18:04:04 to 01-25-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	653
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop		drop	364
66.249.93.123	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	145
66.249.93.123	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	144
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	117
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	77
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop		drop	59
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	40
66.249.93.67	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
66.249.93.67	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop		drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
31.25.78.49	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	28
85.130.196.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
85.130.196.121	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
85.130.196.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.54.166.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
66.249.93.127	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
66.249.93.127	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.117.175.126	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	18
176.13.1.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
176.13.13.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.86.39	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.93.67	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
109.160.160.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
68.180.230.244	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
109.160.160.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
79.176.129.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.93.123	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
184.6.137.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
66.249.93.123	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
213.8.204.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.93.123	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
79.182.162.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.93.127	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
213.8.204.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.3.144.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
94.159.147.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	7
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.159.147.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
46.19.86.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.102.254.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

01-25-2016-18:04:04 to 01-25-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.235.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
2.52.6.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
2.54.1.153	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
79.183.204.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
2.54.55.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
185.32.179.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
84.108.235.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
46.19.86.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.54.1.153	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.1.153	Block	39
168.235.207.191	United States	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
31.168.101.163	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.101.163	Block	9
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
217.132.115.55	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
2.52.34.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.52.167.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
213.133.133.76	United Kingdom	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
109.253.132.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.128.117	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	5
46.19.86.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.185.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.55.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
149.88.91.157	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 149.88.91.157	Block	4
93.172.238.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
77.125.15.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.167.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.101.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
85.64.179.132	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	3
2.52.6.89	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
77.127.151.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.134.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.134.210	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
87.69.247.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.223.222	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
95.86.117.13	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/1/71101.pdf&sa=u&ved=0ahukewizhoq_t8xkahxi1hokhyr7c9wqfgghmaa&usg=afqjcneftvyqb05mfz2siw7lzfh88warbw	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
46.19.86.17	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
85.64.179.132	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/	Block	2
2.52.6.89	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method .aspx?&l=he&f=1133&d=23119 in URL	Block	1
79.180.52.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
210.172.183.48	Japan	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
94.249.68.87	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.121.74.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.179.132	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.64.179.132	Block	1
2.54.52.92	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
80.82.64.68	Netherlands	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to qassam.ps/prisoner-52-murid_salim_al_akhras.html	Block	1

01-25-2016-18:04:04 to 01-25-2016-19:04:04