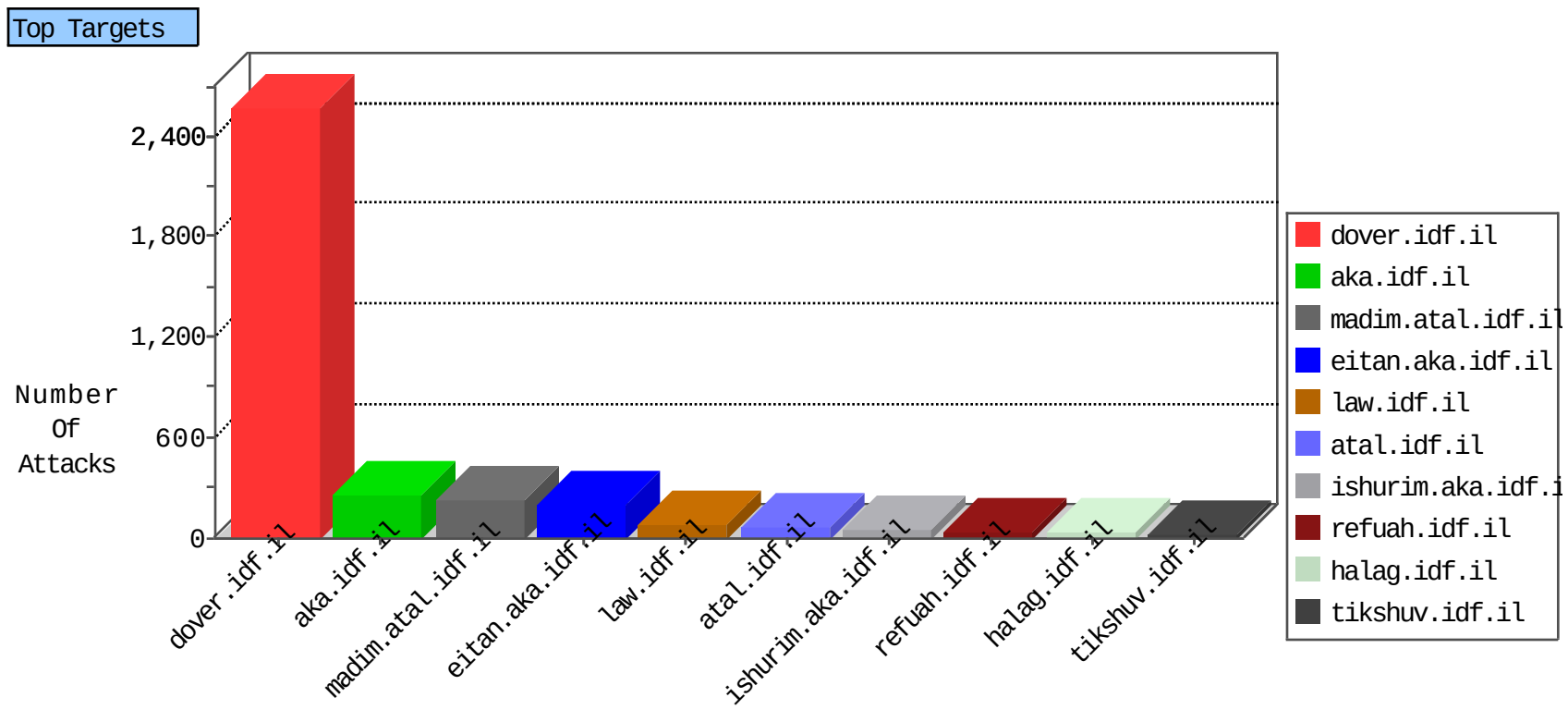
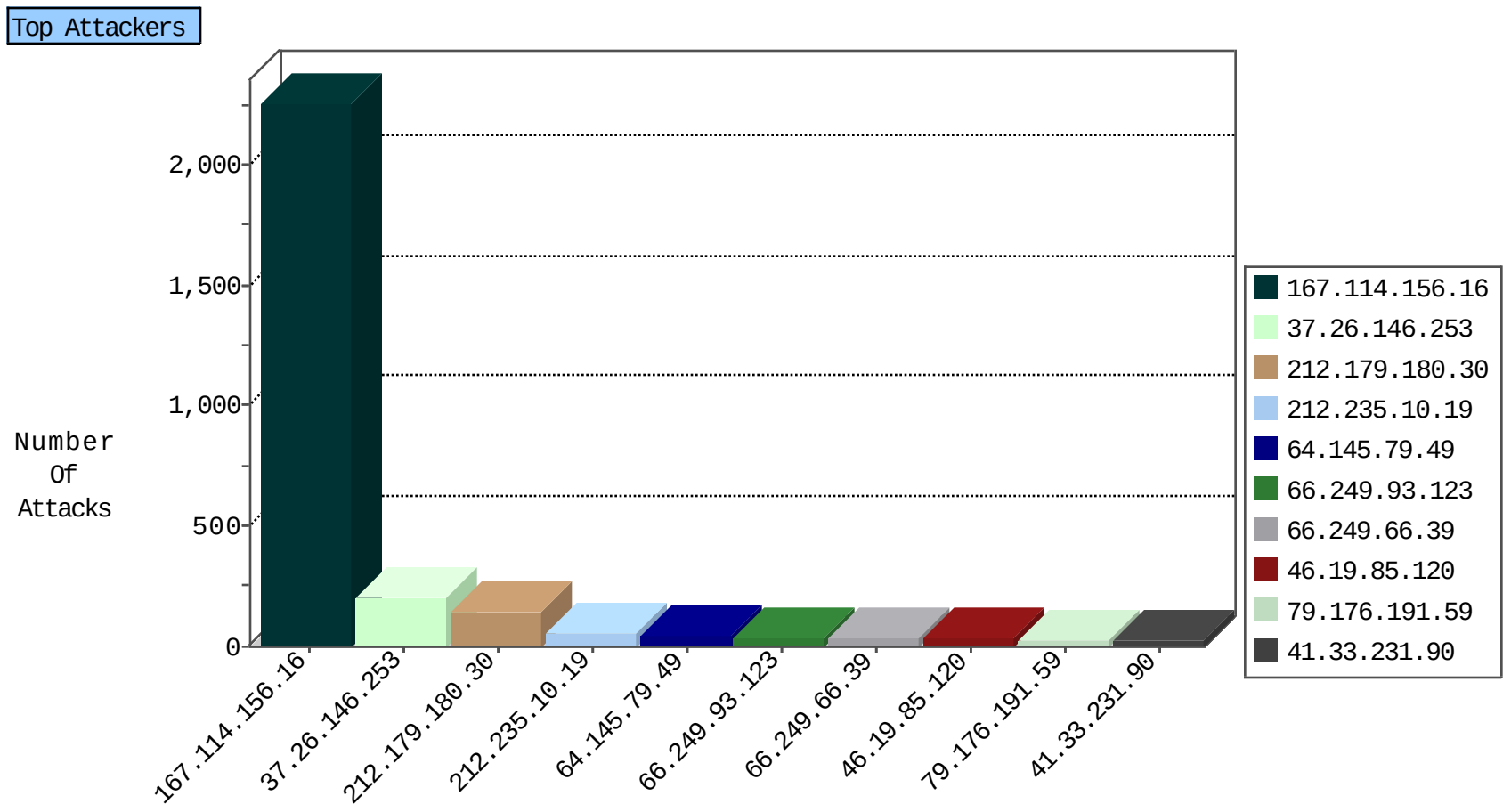
12-22-2015-12:04:01 to 12-22-2015-13:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-22-2015-12:04:01 to 12-22-2015-13:04:01

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	3176
64.145.79.49	United States	147.237.77.74	law.idf.il	SQL-Inj-Pang-NonUn1	dest-reset	41
66.249.64.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
185.3.146.123	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
195.211.116.254	Ukraine	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
79.177.101.223	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.86.101	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
212.179.28.34	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
195.211.116.252	Ukraine	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
192.35.35.35	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.96.201.142	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
192.96.201.142	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

12-22-2015-12:04:01 to 12-22-2015-13:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
138.128.170.124	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
5.34.160.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	12618: HTTP: WebCruiser Vulnerability Scanner	Block	1
31.13.160.217	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	3798: HTTP: SQL Injection (Boolean Identity)	Block	1
89.163.148.58	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-22-2015-12:04:01 to 12-22-2015-13:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.52.185.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.17.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.235.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.191.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.120.191.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.176.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.148	United States	gqcenter.aka.idf.il	ET DROP Dshield Block Listed Source	1
2.54.14.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.75.6.126	147.237.72.166	India	aka.idf.il	ET SCAN NMAP -sS window 1024	1
173.252.74.100	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.76.86	Ukraine	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.181.31.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.127	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
66.249.81.135	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
46.120.157.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.253.157	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1

12-22-2015-12:04:01 to 12-22-2015-13:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.10.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
212.179.180.30	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.85.120	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	19
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.83.161	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.153	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.176.191.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.176.191.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
64.233.172.206	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.150	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
95.86.85.143	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.168.11.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
46.19.86.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.32.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.228	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.120	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.159.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.32.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.172	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.83.167	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
105.196.58.221	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.228	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
194.90.125.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.52.48.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
37.46.39.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.52.48.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
199.203.215.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.241	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.48.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.114.105.254	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.15.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
223.30.72.254	India	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
208.115.111.68	United States	147.237.77.74	law.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
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

12-22-2015-12:04:01 to 12-22-2015-13:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
212.179.180.30	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.180.30	Block	88
37.26.146.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
176.13.1.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
37.26.146.253	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.146.253	Block	17
81.218.176.160	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.176.160	Block	3
46.19.86.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
128.127.107.81	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.139.187	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.13.15.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
39.158.152.60	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
5.22.131.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
221.178.182.132	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
31.13.160.217	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.13.160.217	Block	2
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	2
46.116.193.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.189.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.194.180.34	Ireland	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
124.120.240.43	Thailand	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/sendtofriend	Block	1
80.14.226.112	France	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
195.200.205.35	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
37.26.148.176	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
91.231.193.150	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 91.231.193.150	Block	1
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.20.9	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
23.94.115.65	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
85.130.240.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.190.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
218.205.17.204	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	1
50.31.26.42	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
150.70.172.231	Japan	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
79.176.7.194	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/login.aspx?x™x•x¨	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.1.183	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
89.139.148.212	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
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
62.102.148.67	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.13.5.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.81.46.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.178.204.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.199.104.146	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
197.38.206.237	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
37.26.148.213	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
91.231.193.150	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1

12-22-2015-12:04:01 to 12-22-2015-13:04:01