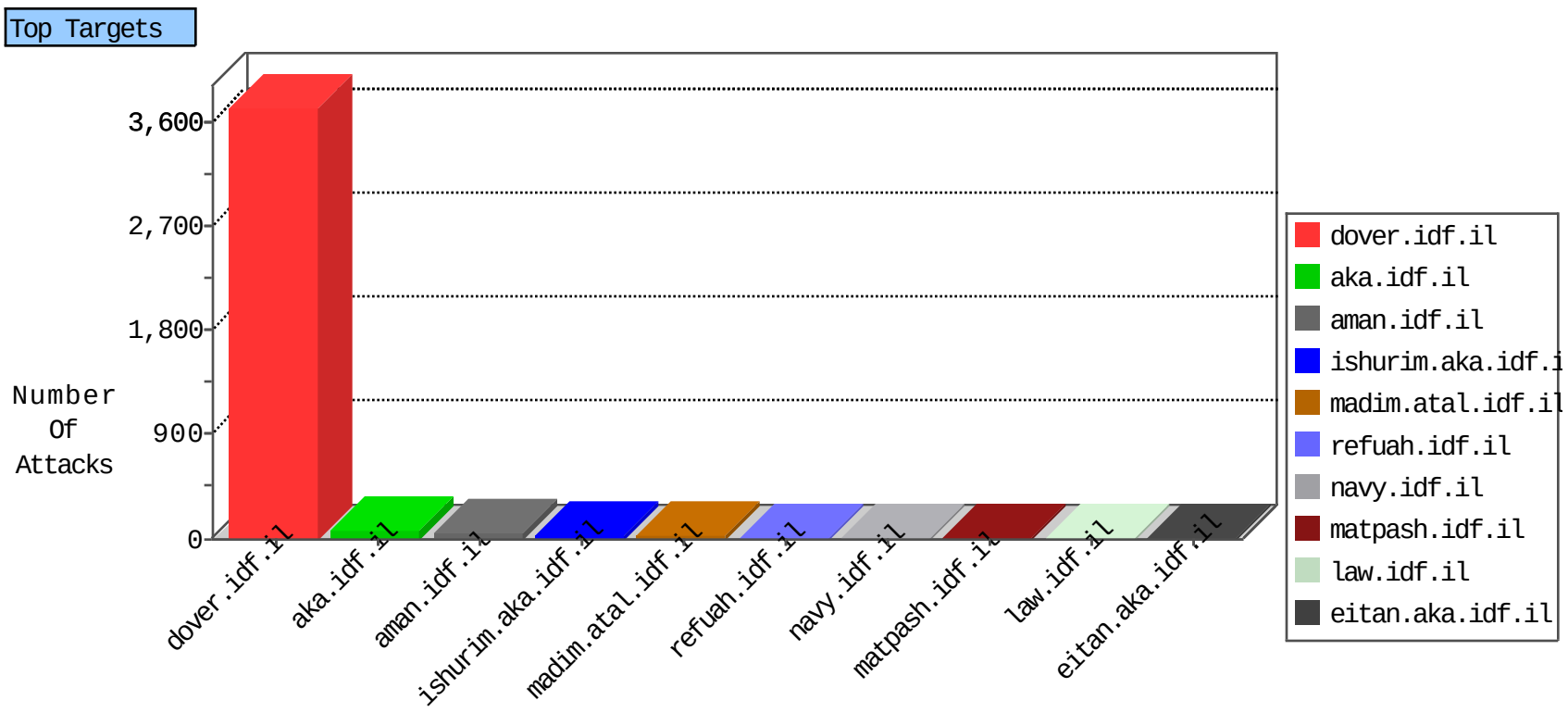
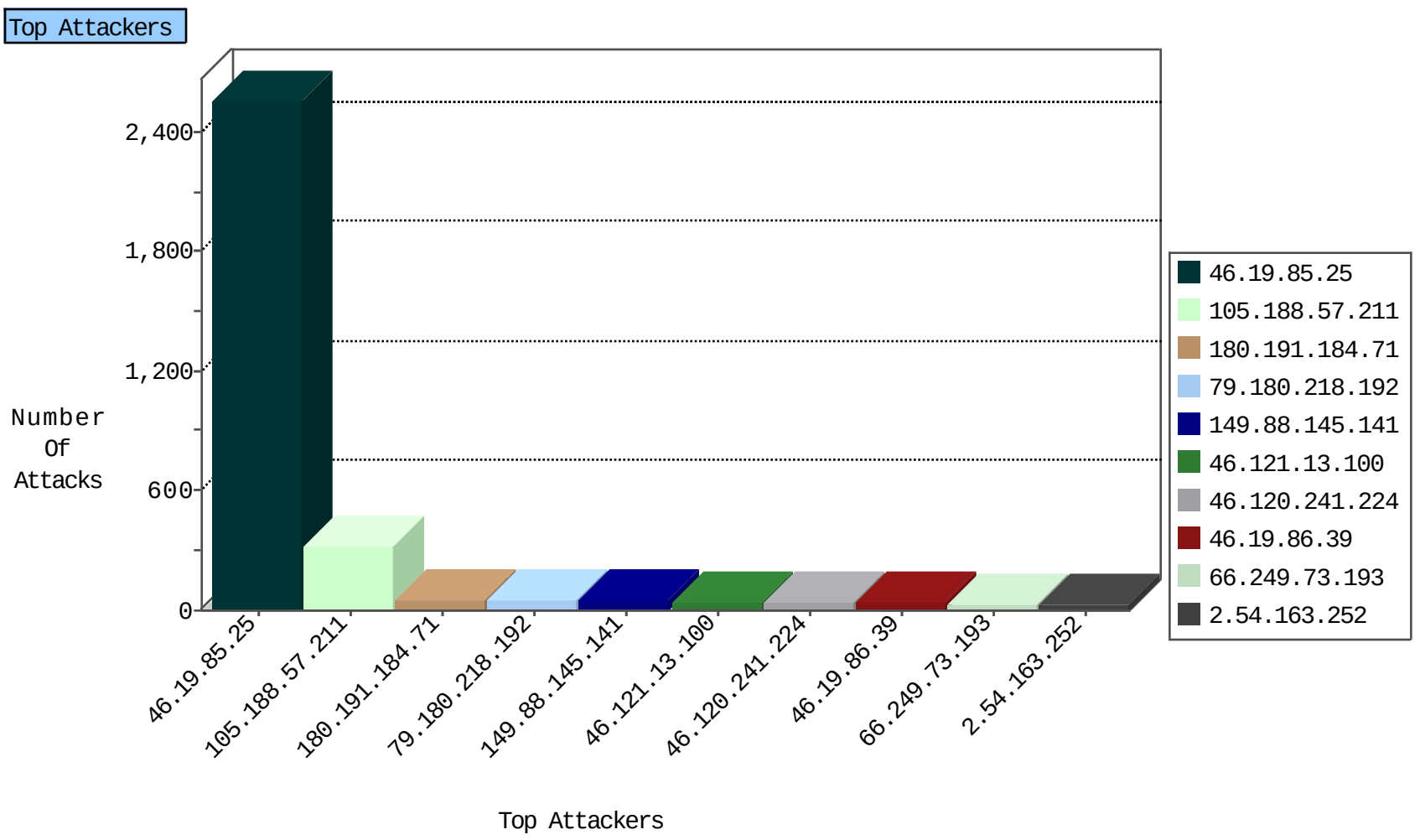
05-09-2015-18:03:08 to 05-09-2015-19:03:08

IDF Under Attack
05-09-2015-18:03:08

Top Targets



Top Attackers



05-09-2015-18:03:08 to 05-09-2015-19:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.121.13.100	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	405
87.68.53.235	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
109.67.71.12	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
220.181.108.81	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	96
89.138.237.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
37.142.65.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	48
192.168.14.183		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
79.181.152.77	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.121.108.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
180.191.184.71	Philippines	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.86.39	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.228.148.211	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.183.220.250	Latvia	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
31.154.92.157	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-09-2015-18:03:08 to 05-09-2015-19:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
185.32.178.164	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.i	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
79.178.98.221	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.116.81.215	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
80.178.2.62	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
176.67.124.121	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-18:03:08 to 05-09-2015-19:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
192.151.147.94	United States	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
192.151.147.94	United States	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
192.151.147.94	United States	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
192.151.147.94	United States	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.151.147.94	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
192.151.147.94	United States	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
212.18.232.63	United Kingdom	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
192.151.147.94	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
203.170.75.2	Pakistan	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
192.151.147.94	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
203.170.75.2	Pakistan	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
188.138.9.51	Germany	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.151.147.94	United States	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
139.192.193.87	Indonesia	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
192.151.147.94	United States	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.151.147.94	United States	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
5.9.1.16	Germany	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
192.151.147.94	United States	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.89.137.3	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.18.232.63	United Kingdom	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
192.151.147.94	United States	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
203.170.75.2	Pakistan	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
192.151.147.94	United States	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
139.192.193.87	Indonesia	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
192.151.147.94	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
82.221.47.101	Iceland	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1

05-09-2015-18:03:08 to 05-09-2015-19:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2556
105.188.57.211		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	262
180.191.184.71	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
79.180.218.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
149.88.145.141	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
46.120.241.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
46.19.86.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
105.188.57.211		147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	28
105.188.57.211		147.237.77.216	dover.idf.i	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	28
66.249.73.193	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
2.52.149.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
66.249.73.201	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
79.176.150.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
84.111.110.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
2.52.153.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
203.133.170.144	Korea, Republic of	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
46.19.86.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
46.116.81.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
62.128.62.1	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.210.180.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
87.68.71.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
99.27.126.151	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
94.153.9.66	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.191	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
208.54.90.255	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
79.176.20.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.19.86.98	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.19.86.33	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
93.172.35.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.120.103.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
176.63.13.204	Hungary	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
82.126.28.37	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
46.19.86.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
105.188.57.211		147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	5
46.19.85.80	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
31.168.148.67	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
77.126.24.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
149.88.104.174	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4

05-09-2015-18:03:08 to 05-09-2015-19:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.163.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
176.12.137.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	12
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	4
79.183.205.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
84.108.46.180	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
180.76.4.215	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
157.55.39.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
69.30.240.46	United States	147.237.72.156	aman.idf.il	Illegal HTTP Version	Block	1
84.228.234.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/halochamim	Block	1
188.138.17.205	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
46.120.165.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.93.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11677en/dover.aspx	Block	1
85.64.216.71	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.176	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	1
46.121.13.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.145.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.233.87	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
46.121.108.84	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.80.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
176.67.124.121	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
5.29.59.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.142	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/faq.aspx	Block	1

05-09-2015-18:03:08 to 05-09-2015-19:03:08