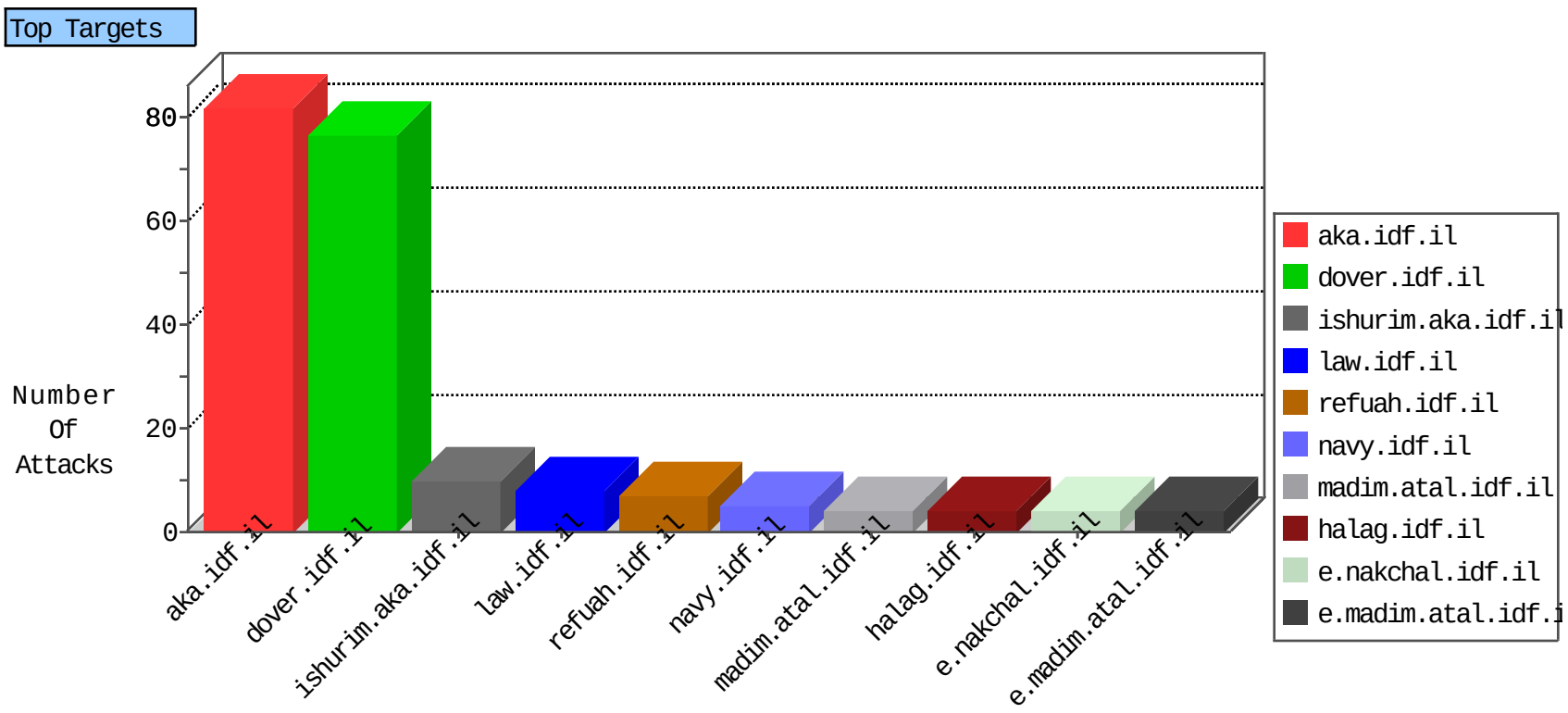
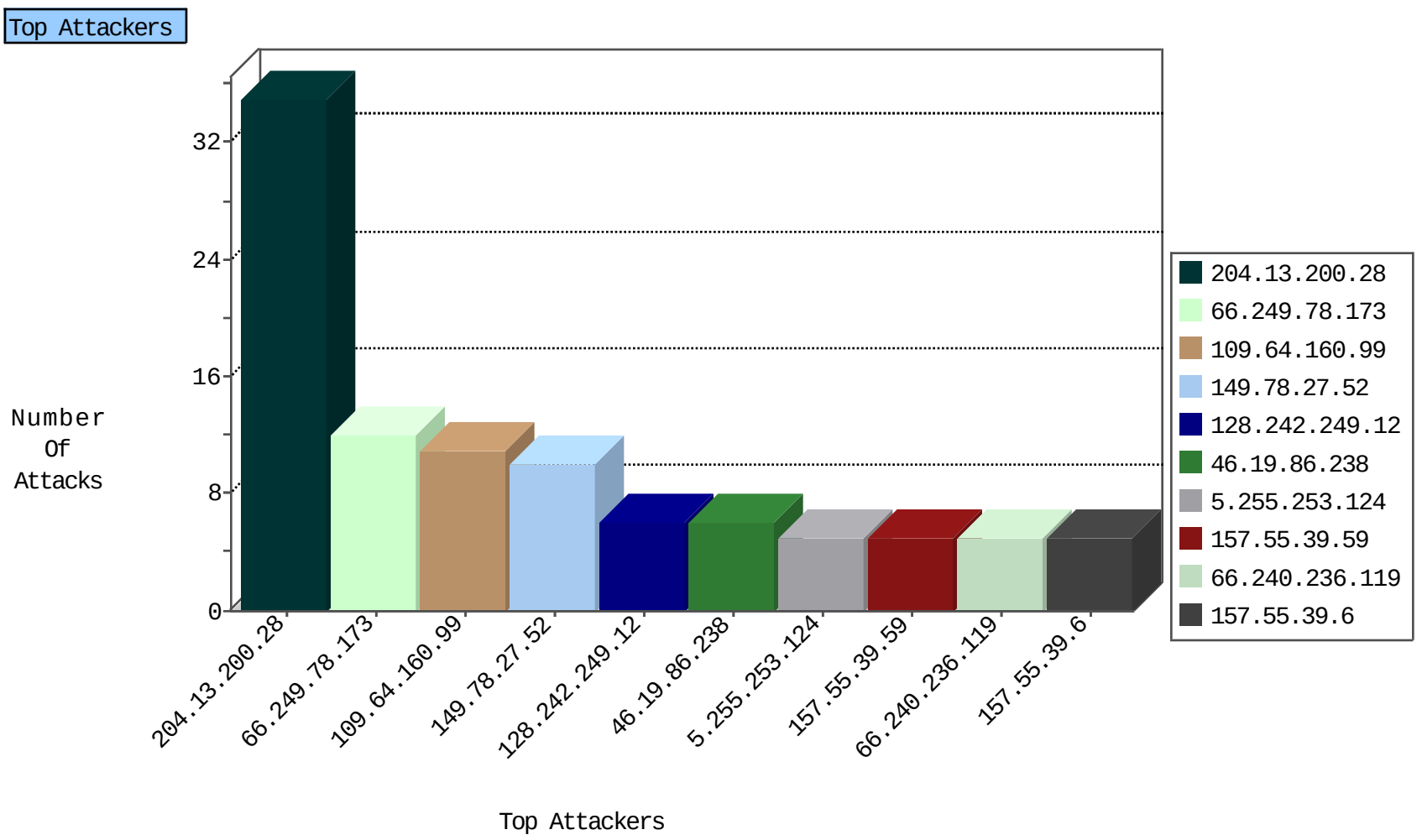
04-26-2015-07:03:03 to 04-26-2015-08:03:03

IDF Under Attack
04-26-2015-07:03:03

Top Targets



Top Attackers



04-26-2015-07:03:03 to 04-26-2015-08:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3118
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	179
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	172
220.181.108.110	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	90
149.78.27.52	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	45
122.102.204.59	Japan	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	4
204.13.200.28	United States	147.237.72.166	aka.idf.il	Frk_Under_Attack_Con_Https	drop	2
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
110.174.10.142	Australia	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-26-2015-07:03:03 to 04-26-2015-08:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
46.19.85.82	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1

04-26-2015-07:03:03 to 04-26-2015-08:03:03

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	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.64	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
109.186.70.28	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
91.243.126.2	Iran, Islamic Republic of	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1
2.52.13.160	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
125.39.116.219	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.243.126.2	Iran, Islamic Republic of	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.64	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
125.39.116.219	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1

04-26-2015-07:03:03 to 04-26-2015-08:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
204.13.200.28	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.238	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.86.238	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
213.57.158.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.158.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.133.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
194.90.125.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
100.2.28.93	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
89.27.138.50	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.92.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
216.223.27.22	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
65.55.210.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.52.25.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
128.242.249.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
74.82.47.43	United States	147.237.77.212	e.dover.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
185.32.179.202	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.67.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
128.242.249.14	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
80.246.130.65	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
185.32.179.202	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
94.230.86.169	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.32	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.35	United States	147.237.77.61	e.cogat.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1

04-26-2015-07:03:03 to 04-26-2015-08:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.160.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
80.179.91.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	3
37.26.147.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
37.142.131.100	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
79.176.136.228	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
212.117.136.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/webresource.axd	None	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
31.13.98.113	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/902-8184-he	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.147.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
184.105.139.68	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
84.108.213.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
61.135.190.199	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
31.193.51.84	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/givati/givati.stm	Block	1
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
5.29.42.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
65.101.234.159	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.208	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
80.246.130.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//newsite/english/main.stm	Block	1
208.115.125.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
52.4.217.78	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/60042.pdf	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.64.160.99	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.160.99	Block	1
77.75.77.32	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/18/	Block	1
66.249.67.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/giyus/faq.aspx	None	1
176.12.150.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
80.246.133.19	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
212.117.136.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
54.166.122.69	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/january/11.stm and january/11.stm	Block	1
31.13.98.112	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/902-8183-he	Block	1
66.249.78.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
184.73.81.214	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
46.19.85.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1

04-26-2015-07:03:03 to 04-26-2015-08:03:03