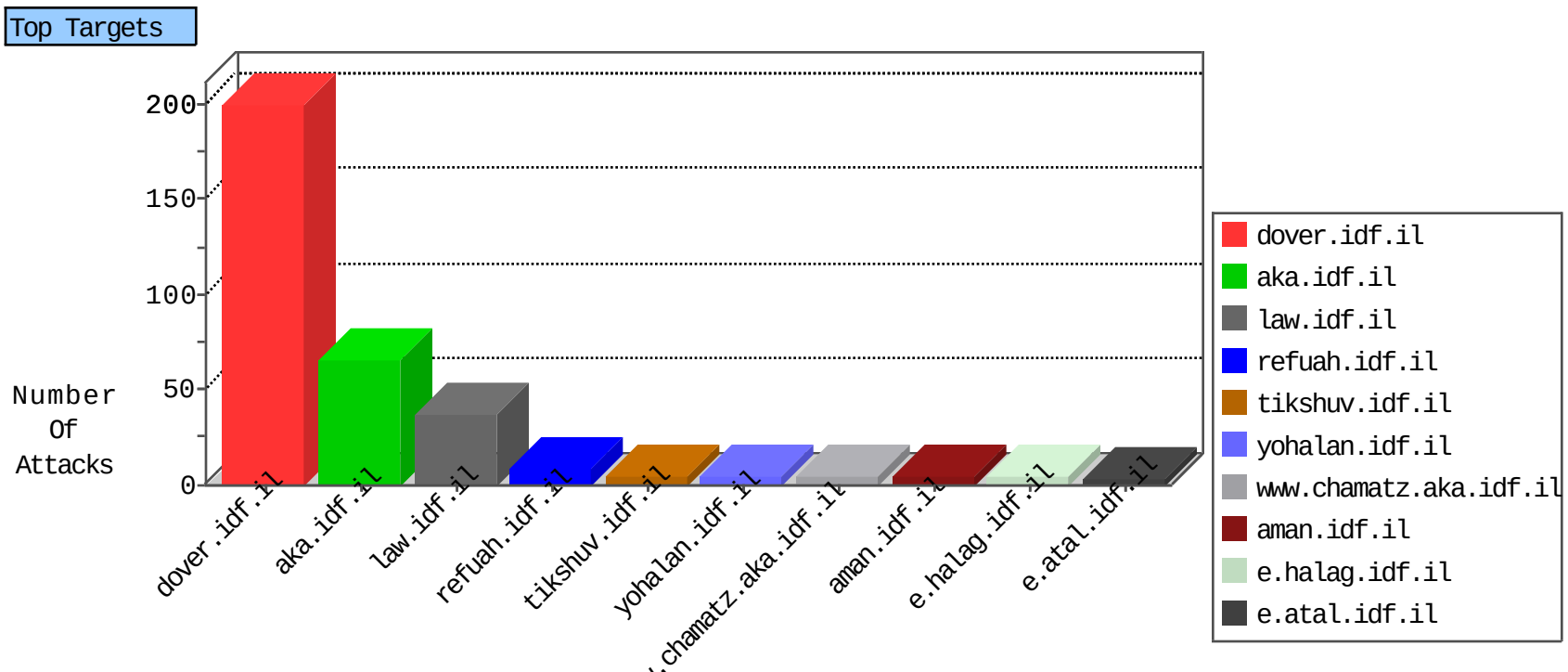
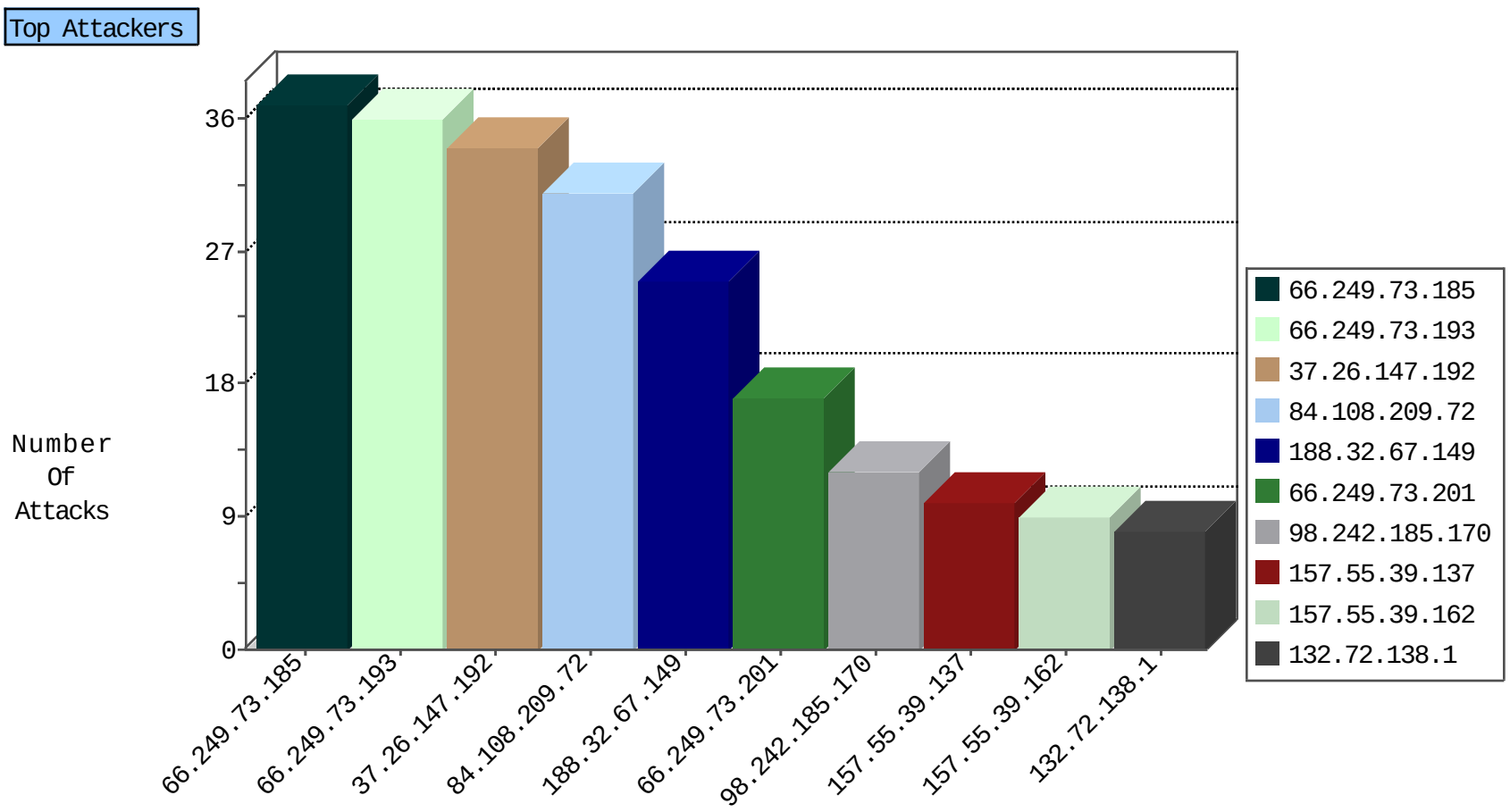
05-10-2015-04:03:08 to 05-10-2015-05:03:08

IDF Under Attack
05-10-2015-04:03:08

Top Targets



Top Attackers



05-10-2015-04:03:08 to 05-10-2015-05:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.152	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2553
220.181.108.87	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	103
98.242.185.170	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	63
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
70.55.225.19	Canada	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

05-10-2015-04:03:08 to 05-10-2015-05:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
132.72.138.1	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.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
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1

05-10-2015-04:03:08 to 05-10-2015-05:03:08

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
66.249.67.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
218.77.79.43	China	147.237.76.201	e.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
178.19.107.114	Poland	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
74.59.142.119	Canada	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.236.220.17	Iran, Islamic Republic of	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.255.174.84	Vietnam	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 2048	1
222.69.94.13	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -f -sS	1
91.238.134.92	Poland	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
222.255.174.84	Vietnam	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
222.255.174.84	Vietnam	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
222.69.94.13	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1

05-10-2015-04:03:08 to 05-10-2015-05:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
37.26.147.192	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
84.108.209.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
188.32.67.149	Russian Federation	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	25
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
37.140.141.37	Russian Federation	147.237.77.74	law.idf.il	SAM rule	drop	drop	7
97.74.24.188	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
98.242.185.170	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
157.55.39.137	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.191	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
76.194.231.193	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
190.226.73.163	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
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
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
107.178.209.181	United States	147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	2
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
58.96.48.248	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
136.243.36.97	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
70.196.70.5	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
174.138.201.61	Canada	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
72.69.237.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
184.105.139.91	United States	147.237.76.34	yohalan.idf.il		drop	drop	2
218.22.211.69	China	147.237.76.34	yohalan.idf.il		drop	drop	1
174.138.201.61	Canada	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
74.82.47.30	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
184.105.247.219	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
174.138.201.61	Canada	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
176.12.146.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
174.138.201.61	Canada	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
31.3.230.138	United Kingdom	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
180.76.5.191	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.138.17.205	France	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
174.138.201.61	Canada	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
180.76.6.130	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
95.211.168.135	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

05-10-2015-04:03:08 to 05-10-2015-05:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.162	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
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	2
136.243.36.97	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.97	Block	1
66.249.67.78	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71811-he/maarachot.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-13341-en/dover.aspx forcerecrawl: 0	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/templates/inner.asp	Block	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
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
136.243.36.97	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	1
176.9.3.89	Germany	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 176.9.3.89	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
37.26.147.192	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
199.180.114.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17436-en/dover.aspx/trackback/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.9.3.89	Germany	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
157.55.39.124	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
74.82.47.4	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
61.135.190.200	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
207.46.13.26	United States	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	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
157.55.39.7	United States	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/fr.au	Block	1
176.9.3.89	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&amp	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
112.83.32.29	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.249.64.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.7	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
176.12.141.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1

05-10-2015-04:03:08 to 05-10-2015-05:03:08