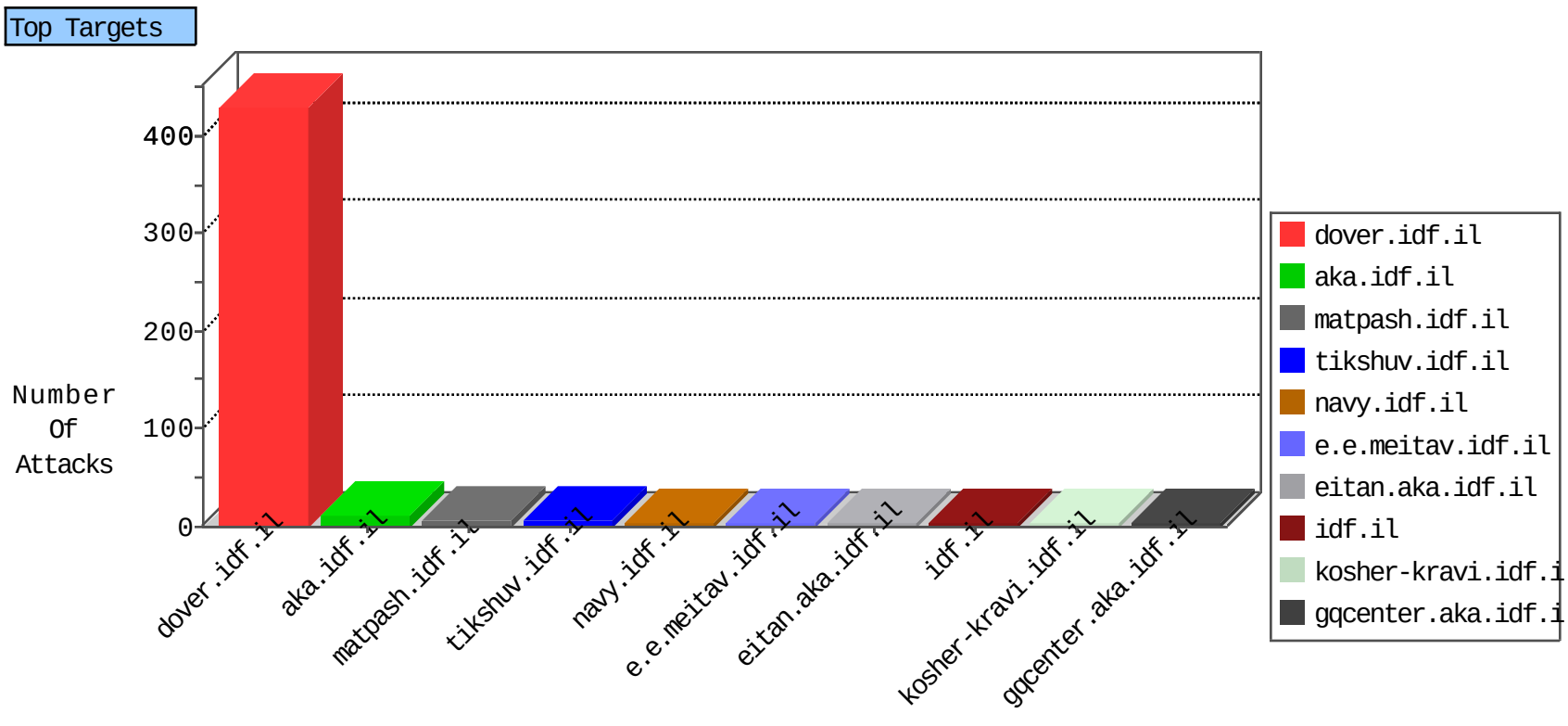
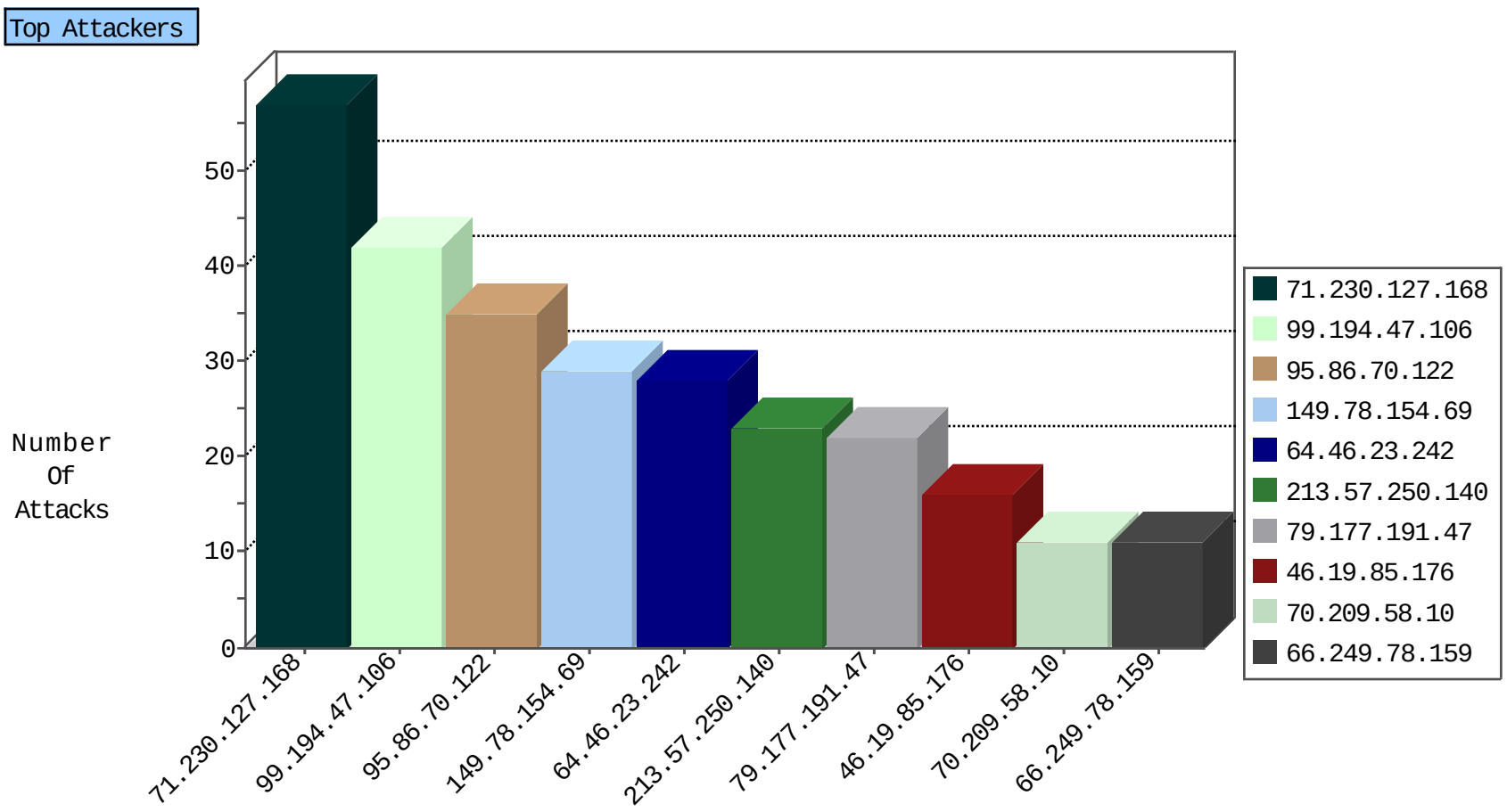
05-08-2015-02:03:06 to 05-08-2015-03:03:06

IDF Under Attack
05-08-2015-02:03:06

Top Targets



Top Attackers



05-08-2015-02:03:06 to 05-08-2015-03:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.160	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	464
213.57.250.140	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
220.181.108.101	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	97
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
108.41.61.61	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
223.176.129.11	India	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
146.185.239.100	Russian Federation	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
46.183.220.250	Latvia	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
192.3.207.66	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

05-08-2015-02:03:06 to 05-08-2015-03:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	2
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.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	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.216	dover.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
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
122.59.2.124	New Zealand	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
122.107.249.146	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.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
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1

05-08-2015-02:03:06 to 05-08-2015-03:03:06

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
89.248.160.215	Netherlands	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.0.33	idf.il	ET SCAN NMAP -f -sS	1
24.155.160.204	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
178.19.107.114	Poland	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
24.155.160.204	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
144.0.0.60	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.160.215	Netherlands	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.160.215	Netherlands	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
61.240.144.65	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
24.155.160.204	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
144.0.0.60	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
144.0.0.60	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.215	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.160.215	Netherlands	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

05-08-2015-02:03:06 to 05-08-2015-03:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
71.230.127.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
99.194.47.106	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
95.86.70.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
64.46.23.242	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
79.177.191.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.85.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
70.209.58.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
220.237.123.63	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.29.208.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
73.138.51.185	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
213.57.250.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
87.68.63.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.90	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
151.252.99.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.182.60.3	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	4
71.100.21.203	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.64.20.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
197.35.208.55	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
24.183.147.16	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
108.41.61.61	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
132.72.168.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
98.233.113.255	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.25.78.159	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
84.109.155.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.25.78.159	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.244.68.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.157.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
94.230.86.128	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	2
162.243.210.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
199.119.124.41	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.178	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.190.112.130	Russian Federation	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.75	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

05-08-2015-02:03:06 to 05-08-2015-03:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	3
87.69.0.81	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.67.23	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
188.138.17.205	France	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
151.252.99.95	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/undefined	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/idnew.stm	Block	1
77.127.157.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
2.52.42.100	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1540-13036-he/dover.aspx target=	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
174.129.237.157	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 174.129.237.157	Block	1
79.177.206.138	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/french/doctrine/doctrine.stm	Block	1
157.55.39.122	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/departmentslobby/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
174.129.237.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/main.stm	Block	1
79.180.203.201	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.78.222	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
178.137.19.143	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1

05-08-2015-02:03:06 to 05-08-2015-03:03:06