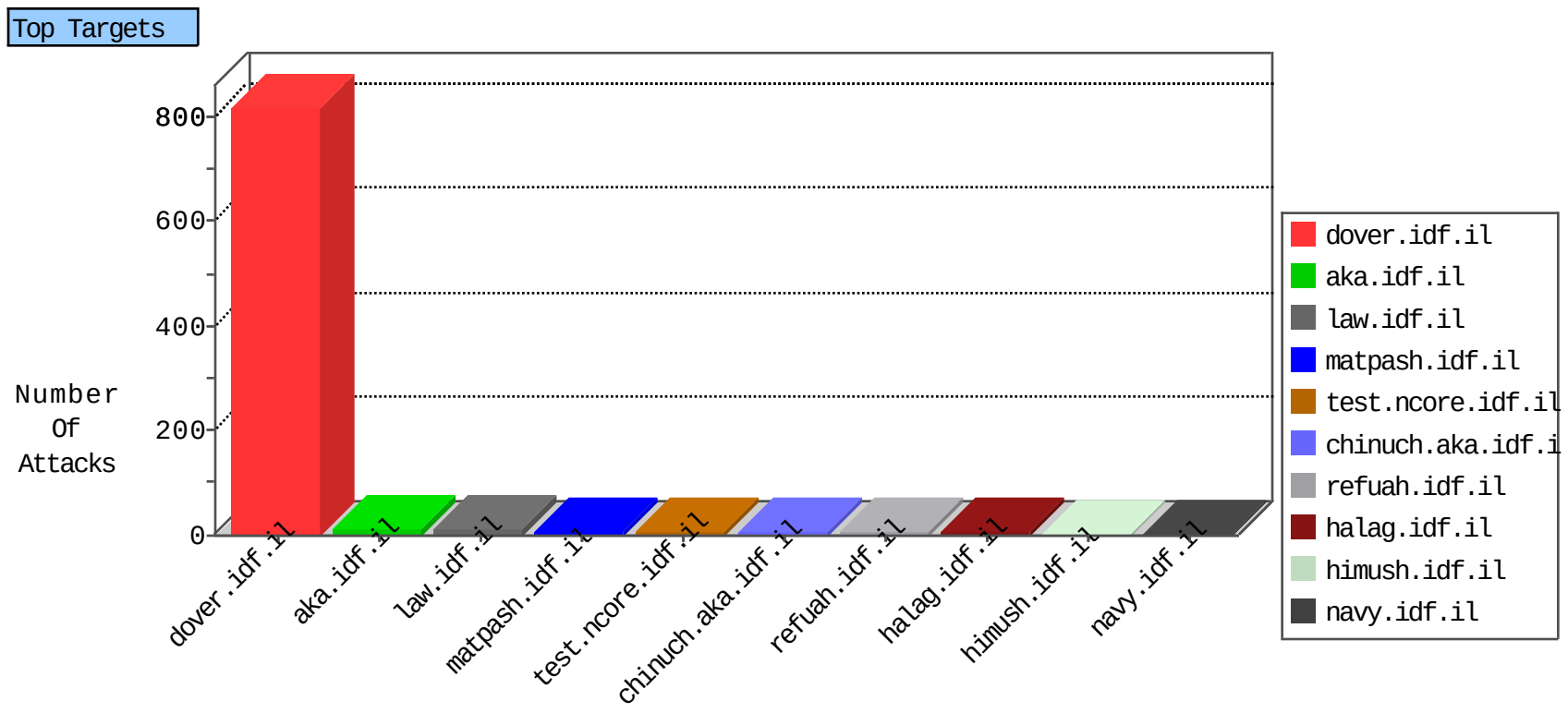
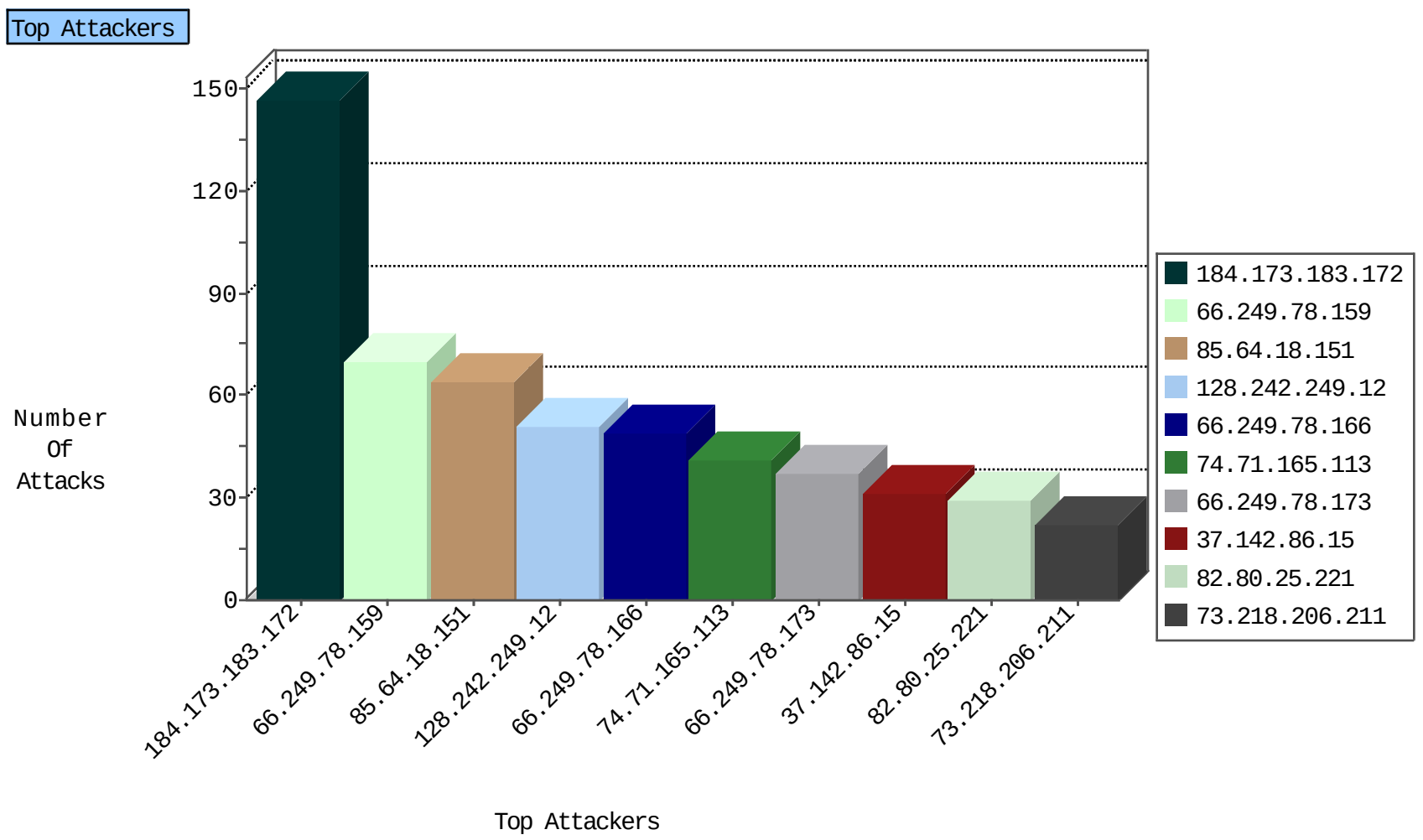
04-20-2015-04:03:05 to 04-20-2015-05:03:05

IDF Under Attack
04-20-2015-04:03:05

Top Targets



Top Attackers



04-20-2015-04:03:05 to 04-20-2015-05:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
68.41.116.68	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	220
85.64.18.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
101.143.72.34	Japan	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
197.41.28.158	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
68.41.116.68	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
112.218.150.106	Korea, Republic of	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-20-2015-04:03:05 to 04-20-2015-05:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	145
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	51
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.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
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.227	e.hamaz.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	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1

04-20-2015-04:03:05 to 04-20-2015-05:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
176.12.138.63	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.31	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.162	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.251	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.49	Ukraine	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.251	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	ET DROP Dshield Block Listed Source	1
58.20.54.249	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
186.218.133.107	Brazil	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.27	Netherlands	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1

04-20-2015-04:03:05 to 04-20-2015-05:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	64
85.64.18.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	62
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
74.71.165.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
37.142.86.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
73.218.206.211	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
79.183.5.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
98.188.248.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
76.29.63.40	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	11
207.46.13.35	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
73.36.44.175	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
192.187.115.90	United States	147.237.77.176	matpash.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	6
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
174.6.36.154	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
81.218.176.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.172.81.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
190.43.37.176	Peru	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
152.23.184.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
217.132.70.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.151.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
95.49.107.102	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.187.129.181	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.67.104	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
86.147.152.222	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
177.226.3.127	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
45.36.22.74		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
17.142.145.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.67.112	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
65.19.138.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

04-20-2015-04:03:05 to 04-20-2015-05:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.173.160.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	2
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
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
66.249.65.153	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15982-he/dover	Block	1
77.237.146.28	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18775-he/dover.aspx	Block	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
216.218.206.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0407-2.stm	Block	1
82.80.148.177	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19915-he/dover.aspx	Block	1
180.76.4.154	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
69.30.240.46	United States	147.237.76.30	himush.idf.il	Illegal HTTP Version	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
46.119.113.155	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	1
66.249.64.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
192.187.115.90	United States	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/4.asp	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
109.186.52.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/history.stm	Block	1
66.249.65.30	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
206.174.81.229	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
76.4.163.202	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19538-he/dover.aspx	Block	1
66.249.64.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1

04-20-2015-04:03:05 to 04-20-2015-05:03:05