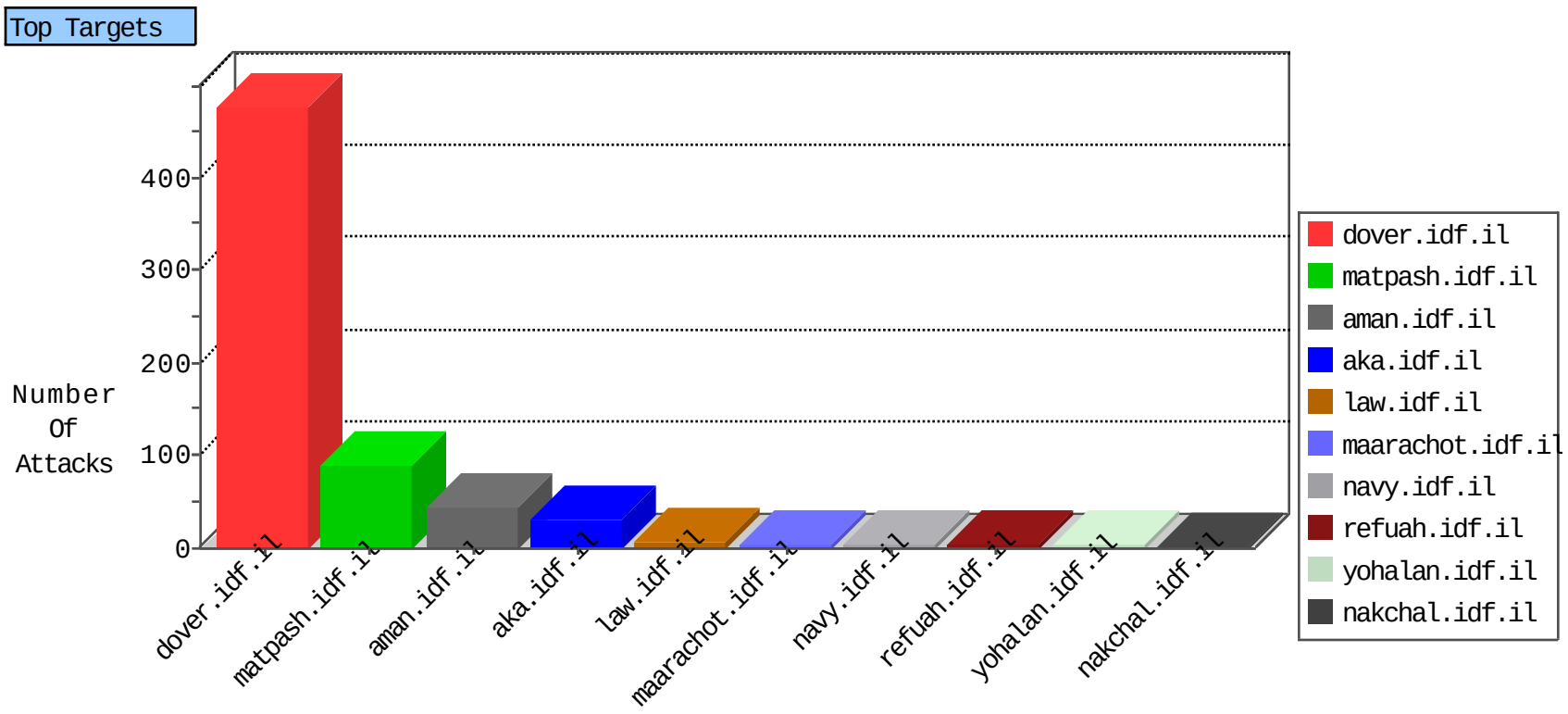
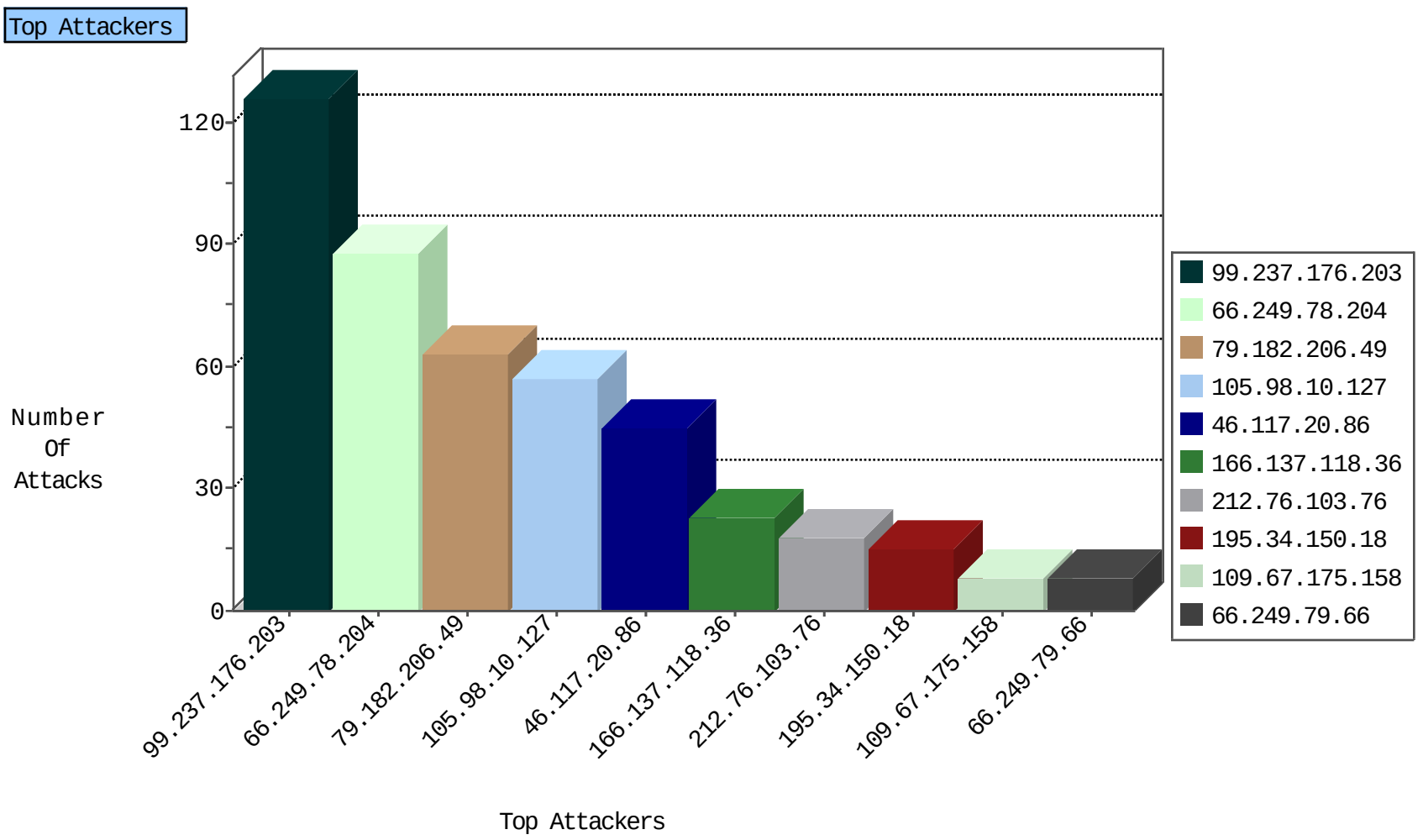
04-24-2015-01:03:02 to 04-24-2015-02:03:02

IDF Under Attack
04-24-2015-01:03:02

Top Targets



Top Attackers



04-24-2015-01:03:02 to 04-24-2015-02:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
72.219.191.21	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2017
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	434
220.181.108.81	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	410
220.181.108.148	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	86
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
85.250.221.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
109.253.145.57	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
41.234.159.72	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
149.88.156.140	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
95.86.80.47	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-24-2015-01:03:02 to 04-24-2015-02:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
105.98.10.127	Algeria	147.237.77.216	dover.idf.il	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.177	ncore.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
84.108.240.70	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.i	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-01:03:02 to 04-24-2015-02:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	88
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
105.98.10.127	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
85.104.233.220	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	3
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
58.124.173.155	Korea, Republic of	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.39.68.33	United States	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -f -sS	1
178.239.176.25	Italy	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	1
91.224.132.118	Russian Federation	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.200.188.213	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
218.200.188.213	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
85.104.233.220	Turkey	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	1
218.200.188.213	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
218.200.188.213	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1

04-24-2015-01:03:02 to 04-24-2015-02:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
99.237.176.203	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	126
79.182.206.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
105.98.10.127	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
166.137.118.36	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
212.76.103.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
109.67.175.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.210.178.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
71.104.87.43	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
93.172.10.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
199.30.24.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.210.225.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
80.179.62.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.116.161.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.160.191.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
149.88.156.140	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.29.164.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.79.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.65.99.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.173.186.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
2.52.170.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
209.52.0.111	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.102.250.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.127.114.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
193.164.156.110	France	147.237.76.200	eitan.aka.idf.i		drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.157.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
176.12.149.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.116.237.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.181.211.179	Israel	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
84.229.198.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.42	Israel	147.237.72.166	aka.idf.il	illegal header format detected: Malformed HTTP protocol name in response	Block HTTP Non Compliant	monitor	2
109.66.159.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.29.135.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
70.210.228.86	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.178.146.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.79.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
89.138.73.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
80.179.62.162	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
109.253.128.197	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.11.47.196	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.99.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
79.181.34.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
46.19.85.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	2
77.126.151.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
157.55.39.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
5.28.137.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.228.253.112	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Â¾Â¶rÂ°ÃŸ@Â™Ã‹ [[#2]]e+Ã±[[#21]]gÂŽÃ–[[#25]]ZÃ‰[[#24]][[#4]]n[[#27]]zh[[#19]]Ã©ÃŠÃ¸Â¨SÂ¾uÃŠÂ“Ãƒâ‰0Â€*Ã¦sÃ–SyÂ¥ÃƒÃº3Ã–Â¸Â³*Â¶	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
106.184.1.4	Japan	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.73.158	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
157.55.39.127	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/×œ×›×ª×‘×” ×”×žœ×?×”	Block	1
5.255.253.16	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 5.255.253.16	Block	1
84.228.253.112	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL [[#25]]×˜	Block	1
61.135.190.200	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
109.66.3.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chamatz/miktzo...95&docid=39561	Block	1
80.246.130.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/bamachane/	Block	1
5.255.253.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
84.228.253.112	Israel	147.237.72.166	aka.idf.il	Malformed URL [[#25]]×˜	Block	1
77.93.58.250	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.11	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
109.188.124.26	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
84.109.48.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2003/july/16z.stm	Block	1
176.12.148.82	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.117.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.253.112	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.125.30.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.65.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
157.55.39.54	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
84.228.253.112	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	1
180.76.5.26	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
37.236.11.135	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
84.228.253.112	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Â¾Â¶rÂ°ÃŸ@Â™Ã‹[[#2]]e+Ã±[[#21]]gÂŽÃ–[[#25]]ZÃ‰[[#24]][[#4]]n[[#27]]zh[[#19]]Ã©ÃŠÃ¸Â¨SÂ¾uÃŠÂ“Ãƒâ‰0Â€*Ã¦sÃ–SyÂ¥ÃƒÃº3Ã–Â¸Â³*Â¶ in URL	Block	1
66.249.65.74	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1