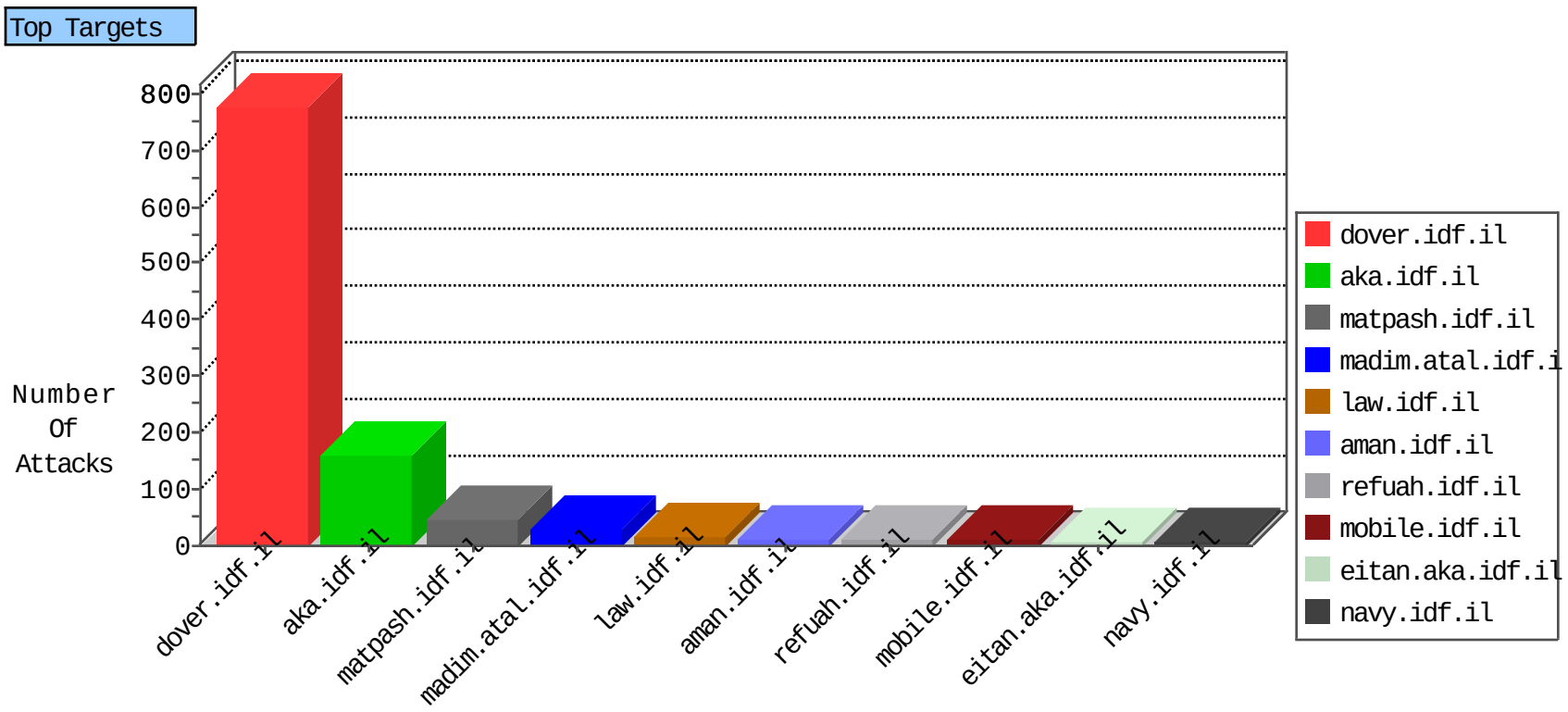
04-22-2016-22:04:00 to 04-22-2016-23:04:00

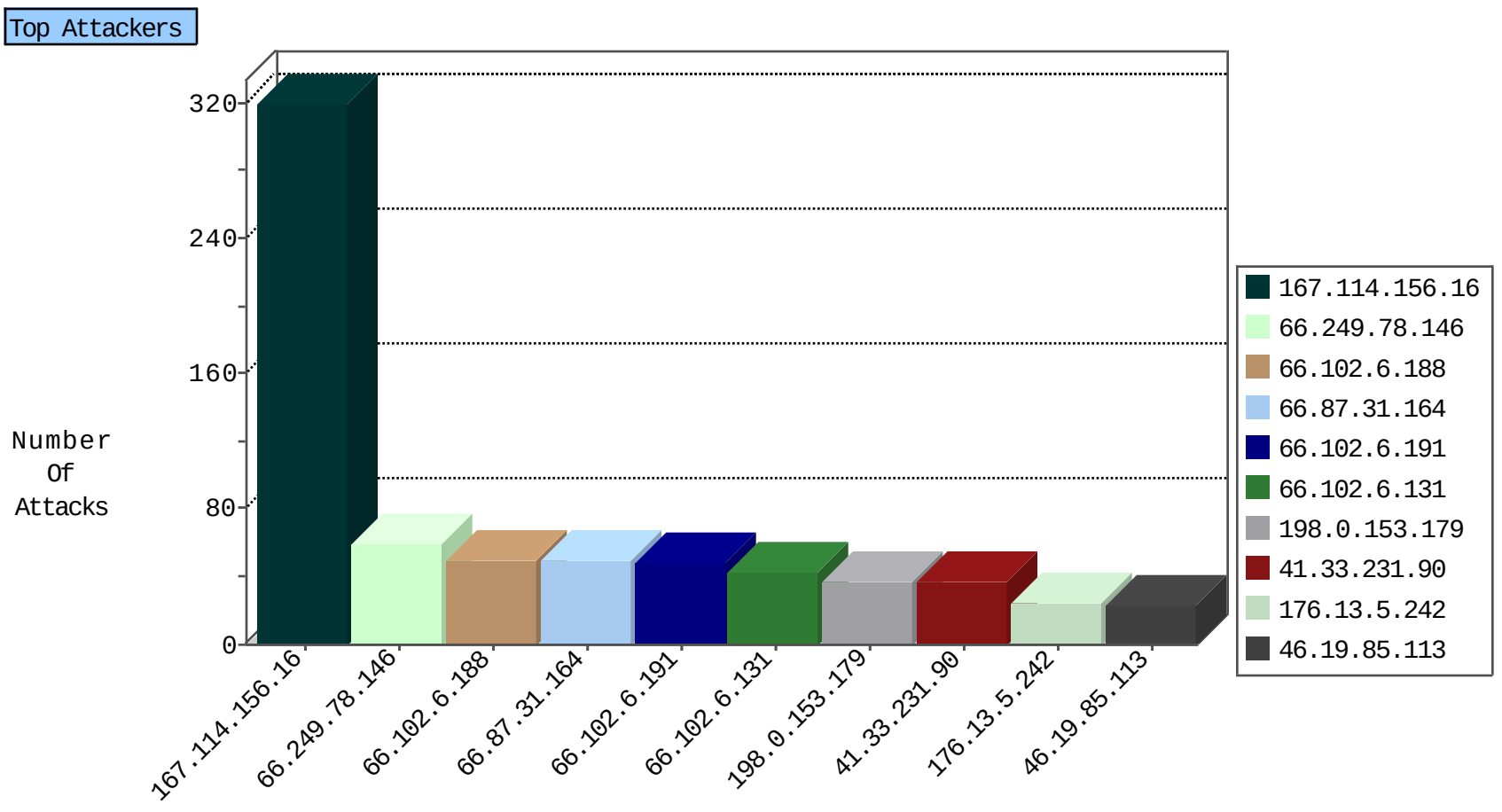
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-22-2016-22:04:00 to 04-22-2016-23:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	12428
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3772
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3301
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
174.27.31.101	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
37.26.146.133	Israel	147.237.76.31	nakchal.idf.il	TCP handshake violation, first packet not syn	drop	2
62.138.2.213	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
62.138.2.213	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
62.138.2.213	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
62.138.2.213	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
62.138.2.213	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-22-2016-22:04:00 to 04-22-2016-23:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.225.135	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-22-2016-22:04:00 to 04-22-2016-23:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.225.135	147.237.77.74	France	law.idf.il	SQL Injection - Select From	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.64.26	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
173.65.154.27	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
109.235.254.181	147.237.0.19	Turkey	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
220.231.195.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
213.8.204.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.86	147.237.77.226	Lithuania	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
109.235.254.181	147.237.0.19	Turkey	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
220.231.195.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1

04-22-2016-22:04:00 to 04-22-2016-23:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
66.102.6.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
66.87.31.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.102.6.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.102.6.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
198.0.153.179	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
176.13.5.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
86.177.7.188	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.113	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.43.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
69.127.100.226	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
93.43.249.11	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
8.37.227.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
8.37.227.68	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.113	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
68.228.83.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
92.114.44.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.49	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
131.253.25.240	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
192.0.113.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.55.143.37	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
65.55.210.94	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.1	Russian Federation	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
23.101.61.176	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.15.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
178.154.189.202	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.48.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.82	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.64.94.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.44.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.204.53.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.174	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.93.21	Europe	147.237.76.42	refuah.idf.il	Directory Traversal	directory traversal overflow	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.200.12.85	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
91.200.12.85	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	5
80.246.137.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.253.224.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
89.238.188.119	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.238.188.119	Block	3
80.246.136.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.139.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.224.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.224.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.224.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.139.21	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
104.162.132.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
185.88.24.151	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.87.31.164	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.idf.il/1038-en/dover.aspx	Block	1
109.253.224.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
141.212.122.161	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
2.55.1.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
199.30.24.248	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nakha	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
157.55.12.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.19	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/news/news.asp	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
109.253.224.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.93.21	Israel	147.237.76.42	refuah.idf.il	Distributed URL is Above Root Directory	Block	1
182.191.179.62	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
46.121.137.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.224.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
80.246.138.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	1
207.46.13.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/info.aspx	Block	1
91.200.12.85	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
185.3.144.30	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
82.81.71.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/עונות	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19754-he/dover.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1