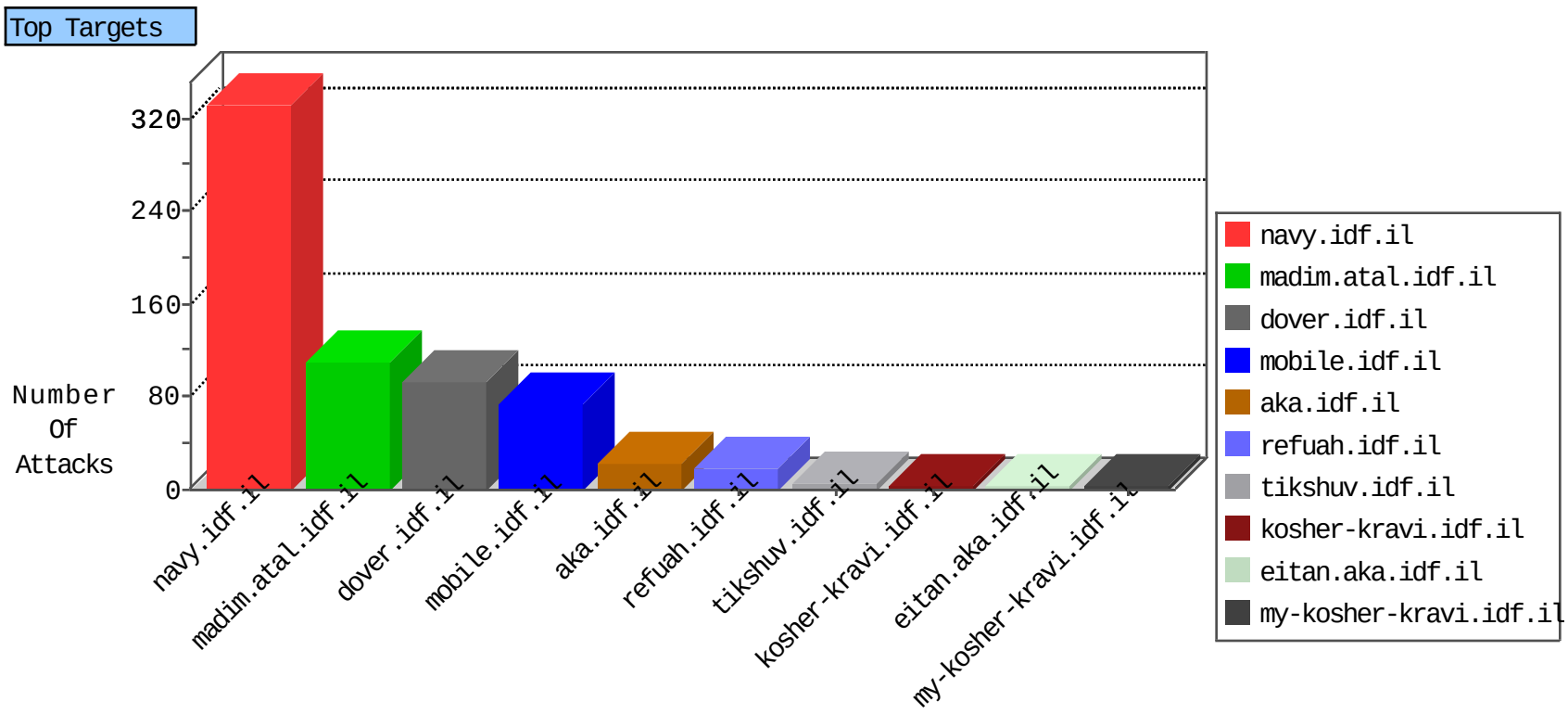
09-22-2016-06:04:06 to 09-22-2016-07:04:06

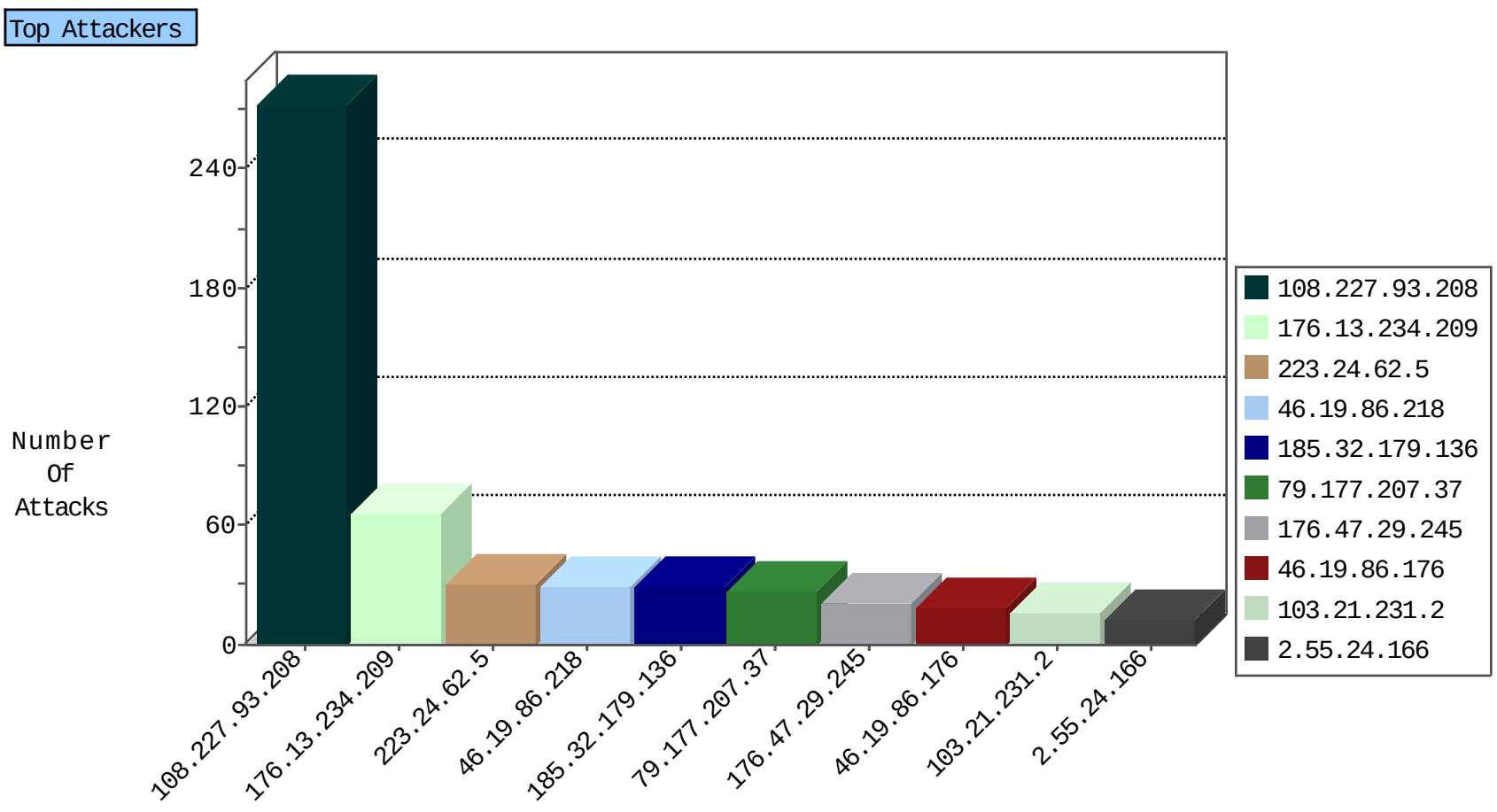
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-22-2016-06:04:06 to 09-22-2016-07:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.248.172.16	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
31.220.43.189	Netherlands	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
45.32.196.8	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
82.221.105.7	Iceland	147.237.76.197	e.himush.idf.il	Black List	drop	1

09-22-2016-06:04:06 to 09-22-2016-07:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.49.112.67	United States	147.237.0.34	tikshuv.idf.il	4807: HTTP: PHP File Include Exploit	Block	2
109.74.3.83	Sweden	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
219.94.227.72	Japan	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
69.60.103.162	United States	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
111.67.201.232	China	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
5.200.9.12	Netherlands	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
88.151.130.66	United Kingdom	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
185.76.64.30	Sweden	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
50.87.248.103	United States	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
91.216.107.211	France	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
198.20.99.130	Netherlands	147.237.76.201	e.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
69.49.112.67	United States	147.237.0.34	tikshuv.idf.il	3885: HTTP: PHP File Include Exploit	Block	1
108.58.150.82	United States	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
202.92.134.3	Philippines	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

09-22-2016-06:04:06 to 09-22-2016-07:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
206.246.150.226	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.70.44.28	147.237.76.42	Hungary	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
195.70.44.28	147.237.0.33	Hungary	idf.il	ET SCAN NMAP -sS window 1024	1
125.65.83.162	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
100.13.130.4	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.231.57	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.70.44.28	147.237.76.177	Hungary	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
195.70.44.28	147.237.76.31	Hungary	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.29.245	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
123.31.41.199	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

09-22-2016-06:04:06 to 09-22-2016-07:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.227.93.208	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	270
223.24.62.5	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.177.207.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
176.47.29.245	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
103.21.231.2	Solomon Islands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.55.24.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
89.138.163.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
93.172.136.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
79.176.31.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.176	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.151.59.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
202.1.174.191	Solomon Islands	147.237.77.216	dover.idf.il	SYN Attack		monitor	4
46.19.86.176	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
172.56.16.113	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
141.226.218.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.213.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
207.46.13.80	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
71.218.180.15	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
202.1.174.191	Solomon Islands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
139.162.37.147	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.23	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
191.241.242.96	Brazil	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
180.97.106.37	China	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
31.220.43.189	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
85.130.187.253	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
202.1.174.191	Solomon Islands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.162	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
46.19.85.157	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
100.13.130.4	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.40	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.99.130	Netherlands	147.237.76.201	e.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
31.220.43.189	Netherlands	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
206.246.150.226	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
184.105.139.104	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.176	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.55.48.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
100.13.130.4	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.86	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.55	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
31.220.43.189	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-22-2016-06:04:06 to 09-22-2016-07:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.234.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
185.32.179.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
185.76.64.30	Sweden	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	3
46.116.122.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
148.72.232.32	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	2
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.74.3.83	Sweden	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	1
88.151.130.66	United Kingdom	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
184.168.200.73	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
66.249.66.249	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
5.196.79.214	France	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
157.55.39.108	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
91.216.107.211	France	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
69.60.103.162	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
46.39.230.150	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	1
180.97.106.161	China	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
109.74.3.83	Sweden	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
88.151.130.66	United Kingdom	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
184.168.200.73	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	1
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
5.200.9.12	Netherlands	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
157.55.39.226	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main/main.as...291&docid=66297	Block	1
91.216.107.211	France	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
69.60.103.162	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	1
185.76.64.30	Sweden	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
180.97.106.161	China	147.237.0.15	kosher-kravi.idf.il	NULL Character in Method	Block	1
141.226.218.79	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
88.151.130.66	United Kingdom	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
184.168.200.73	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
66.249.79.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
14.137.192.71	Australia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
172.56.12.159	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
108.58.150.82	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
69.60.103.162	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
219.94.227.72	Japan	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
180.97.106.161	China	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.161	Block	1
50.87.248.103	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	1
89.138.163.34	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.229.103	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
176.13.15.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18287-he/dover.aspx	Block	1
109.74.3.83	Sweden	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
79.176.9.185	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
219.94.227.72	Japan	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
180.97.106.161	China	147.237.77.170	maarachot.idf.il	Multiple NULL Character in Method from 180.97.106.161	Block	1
50.87.248.103	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
157.55.39.37	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
91.216.107.211	France	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1925-he/cogat.aspx	Block	1
185.32.179.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-22-2016-06:04:06 to 09-22-2016-07:04:06