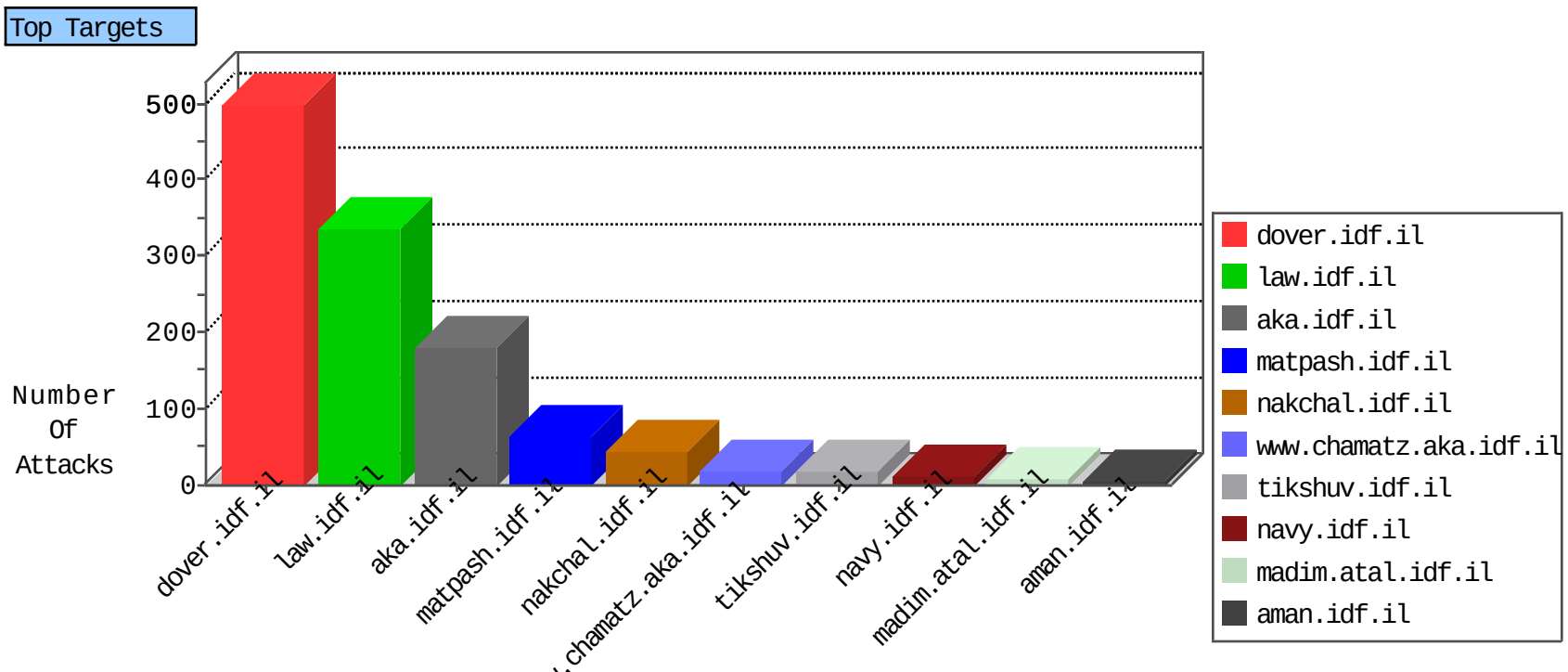
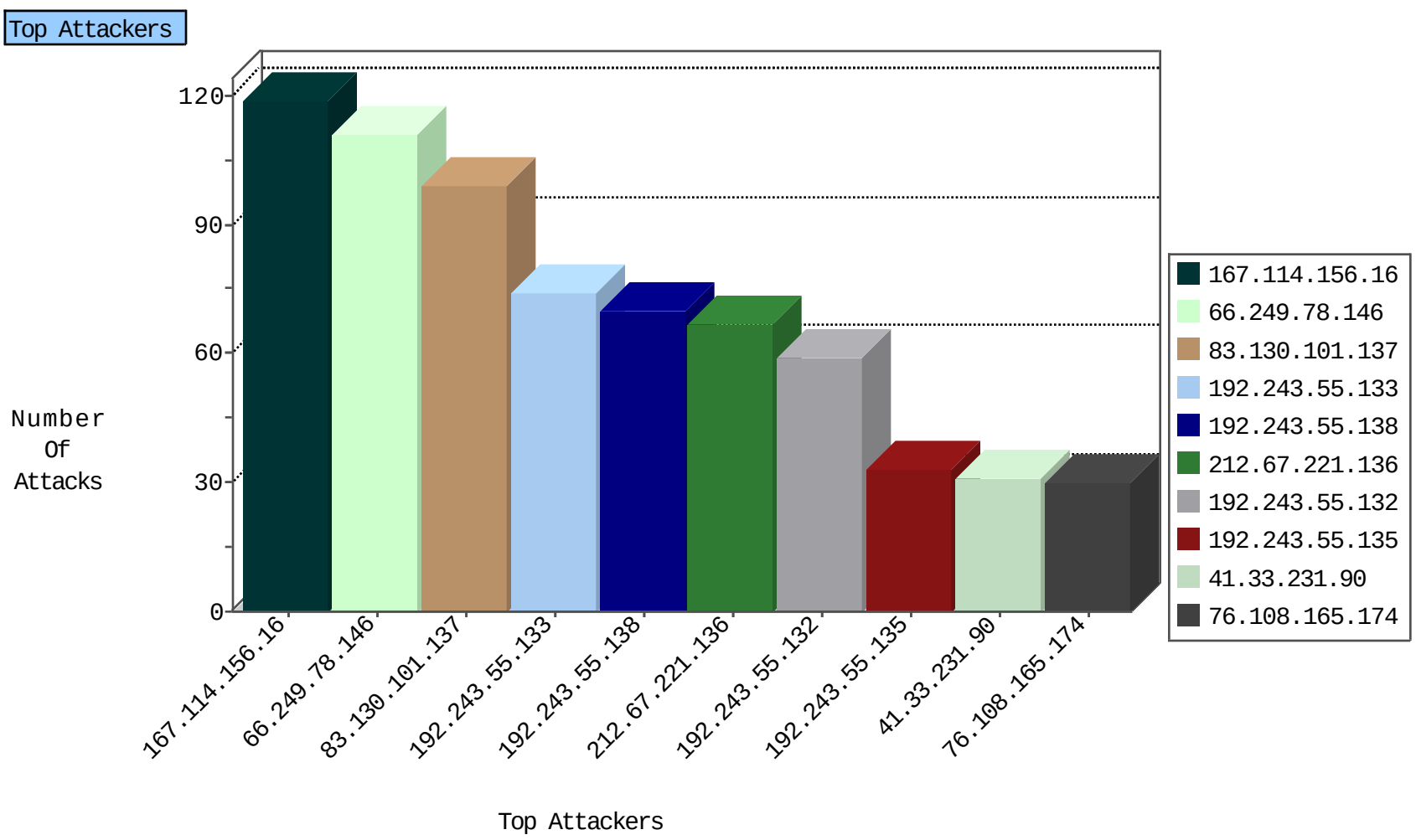
04-24-2016-03:04:03 to 04-24-2016-04:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-24-2016-03:04:03 to 04-24-2016-04:04:03

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	9536
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4184
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	13
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
74.91.23.108	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
173.208.197.251	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

04-24-2016-03:04:03 to 04-24-2016-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.106.179.116	Germany	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.106.179.116	Germany	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
204.12.168.26	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
37.205.0.49	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.145.99	Israel	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
82.165.24.123	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-24-2016-03:04:03 to 04-24-2016-04:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.8.145.99	147.237.77.74	Israel	law.idf.il	SQL Injection - Select From	12
212.67.221.136	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	10
87.106.179.116	147.237.77.226	Germany	www.chamatz.aka.idf.il	SQL Injection - Select From	10
212.67.221.136	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	10
82.165.24.123	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	6
204.12.168.26	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	6
37.205.0.49	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.99	147.237.76.147	Lithuania	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.8.46	Lithuania	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
112.124.10.141	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
111.68.104.195	147.237.77.179	Pakistan	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
23.96.109.87	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.122.143	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.99	147.237.77.212	Lithuania	e.dover.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.44	Lithuania	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.34	Lithuania	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
111.68.104.195	147.237.77.179	Pakistan	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
23.102.168.255	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
23.96.109.87	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

04-24-2016-03:04:03 to 04-24-2016-04:04:03

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	108
83.130.101.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
83.130.101.137	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
76.108.165.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
141.0.15.35	Norway	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	28
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
181.141.72.35	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
70.199.225.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop		drop	8
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.177.100.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.69.88	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop		drop	6
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
197.34.13.132	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.119	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.67.221.136	United Kingdom	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 212.67.221.136	Block	12
212.67.221.136	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.67.221.136	Block	11
212.67.221.136	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	10
212.67.221.136	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	10
157.55.39.69	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.69	Block	2
199.30.24.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.27	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
66.249.78.154	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/16838.jpg	Block	1
5.151.198.27	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
66.249.78.137	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/iturim/iturim.aspx	None	1
157.55.39.215	United States	147.237.72.166	aka.idf.il	Unknown Parameter cat_id in aka.idf.il/iturim/asp/wars.asp	None	1
83.130.101.137	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in aka.idf.il/giyus/main/	None	1
37.48.81.27	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
157.55.39.69	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/kiosk/general.aspx	Block	1
66.249.78.147	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/popups/popup.aspx	None	1
157.55.39.215	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/news/	None	1
94.154.239.69	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dover.aspx	Block	1
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/skira/default.asp	None	1
157.55.39.215	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.215	Block	1
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/chinuch/gallery/	None	1
5.29.150.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/faq/mobile	Block	1
157.55.39.215	United States	147.237.72.166	aka.idf.il	Unknown Parameter catld in aka.idf.il/yohalan/main/main.asp	None	1
109.167.200.251	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
66.249.64.254	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
207.46.13.164	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
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/eitan/mesiratmeida/	None	1
157.55.39.215	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/general	Block	1
66.249.78.161	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/kamlar/gallery/	None	1
192.243.55.133	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
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
157.55.2.147	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.130	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation DocID in www.navy.idf.il/navy/general.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/giyus/giyus/general.aspx	None	1
157.55.39.215	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in aka.idf.il/rights/asp/info.asp	None	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
40.77.167.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/tizmoret/gallery/	None	1