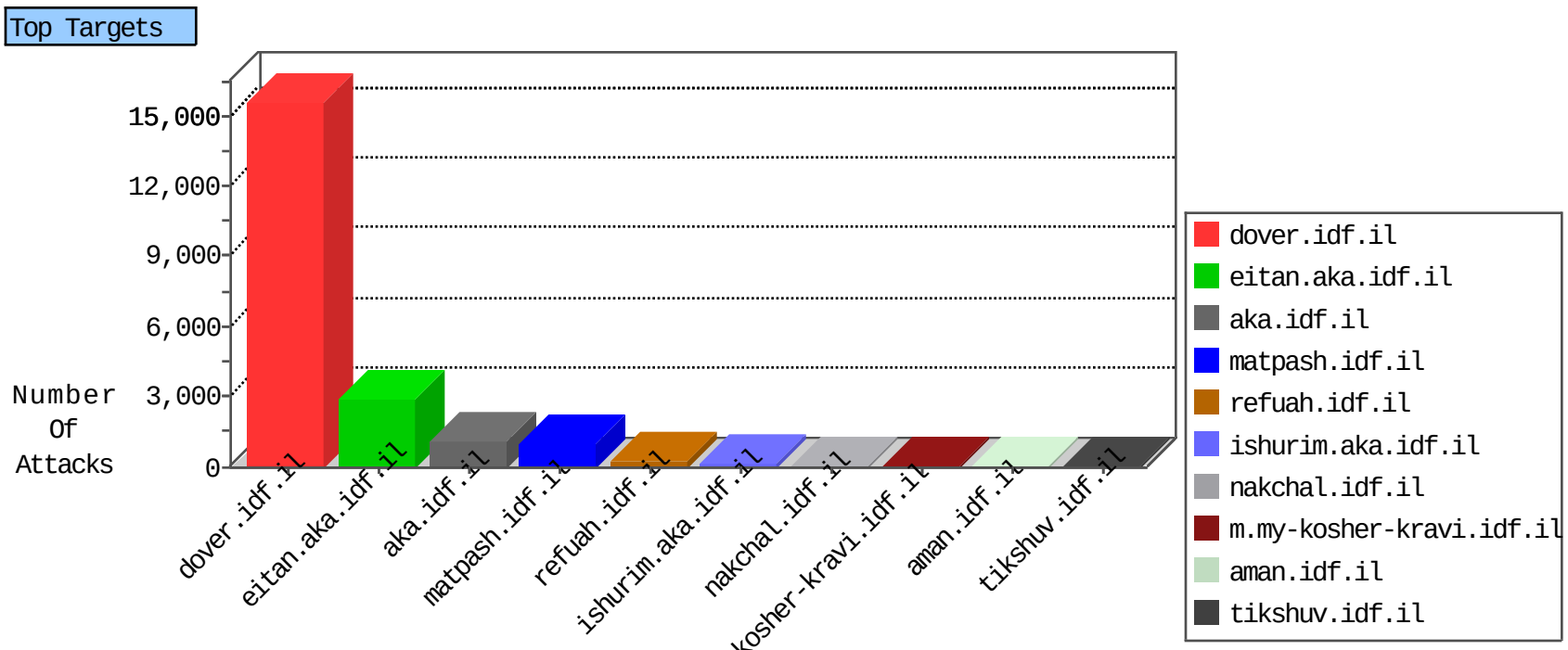
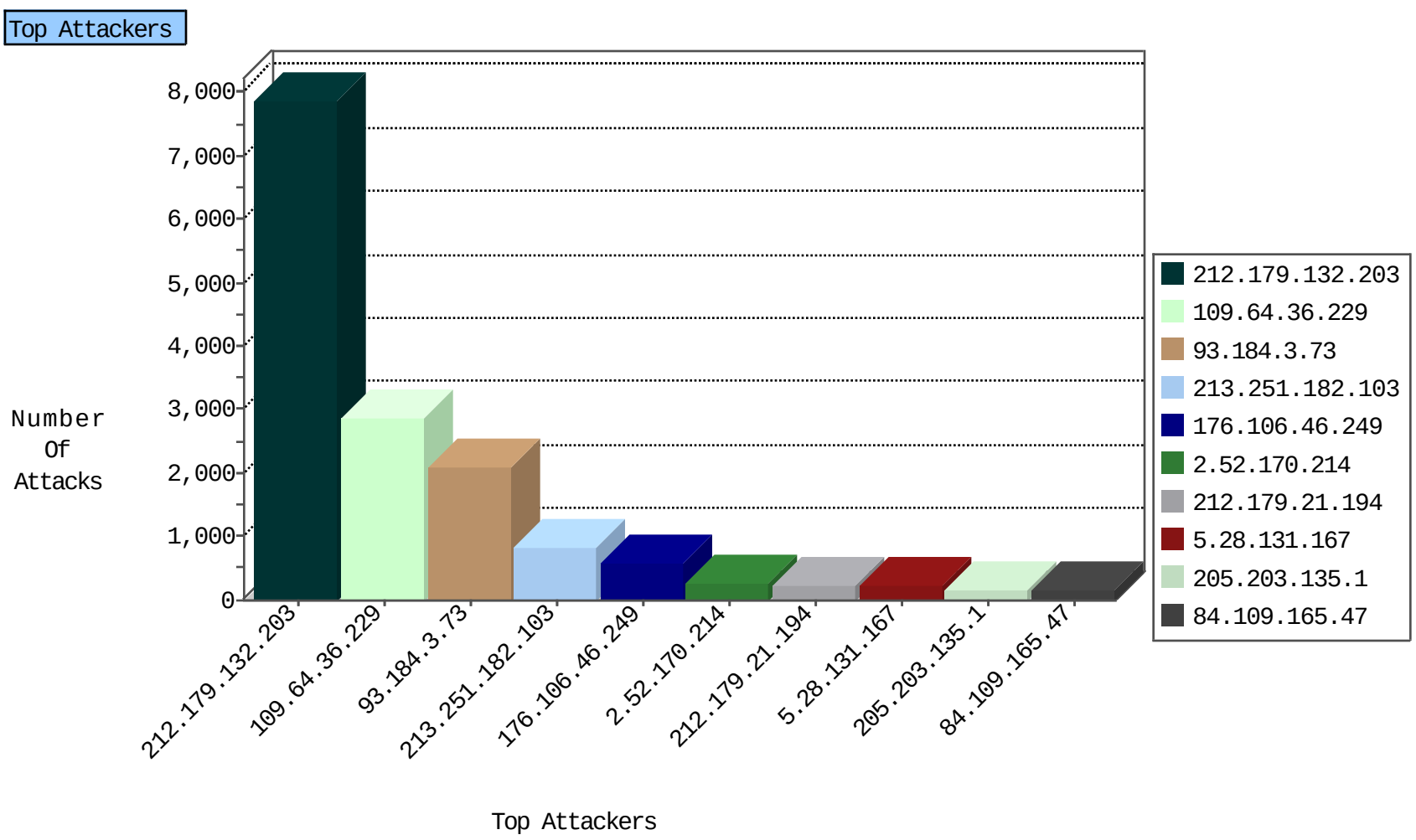
10-27-2015-13:04:03 to 10-27-2015-14:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-27-2015-13:04:03 to 10-27-2015-14:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6324
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	265
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	170
212.25.84.200	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	114
37.26.148.243	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	93
176.13.15.156	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	68
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	57
194.90.128.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
87.69.220.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
82.81.33.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
77.125.130.132	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
2.54.136.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
2.54.22.145	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	11
80.246.136.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.15.156	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
46.19.86.66	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	10
212.150.249.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
31.168.19.190	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
199.67.203.141	Europe	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6
46.19.86.39	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.36	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
31.210.186.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.71.132	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
31.210.186.247	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
147.236.28.31	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.80.198.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.149.132	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.188.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.162.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
78.95.82.29	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.64.162	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
46.98.247.191	Ukraine	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.88.183.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
46.19.86.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
31.168.136.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.69.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.114.91.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.179.132.203	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.228.46.187	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.136.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.136.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.52.42.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

10-27-2015-13:04:03 to 10-27-2015-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.29.124.83	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1

10-27-2015-13:04:03 to 10-27-2015-14:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
109.66.12.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.31.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.173.194.101	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.158.53.18	147.237.76.201	China	e.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.199.57.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
186.231.99.62	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.162.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.101.79.240	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.67.12.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.138	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.0.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.252.197.194	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
46.19.85.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.53.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.204.115.66	147.237.77.216	Russian Federation	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
212.179.102.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.138.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
140.118.122.7	147.237.77.170	Taiwan	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1

10-27-2015-13:04:03 to 10-27-2015-14:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.132.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7876
93.184.3.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2091
109.64.36.229	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	774
176.106.46.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	581
2.52.170.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	262
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	203
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
84.109.165.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	145
46.120.24.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	142
78.146.103.67	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
46.98.247.191	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
80.179.196.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
176.13.14.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
100.100.107.138		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	57
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
149.78.216.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
79.181.130.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
87.68.76.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
145.53.149.178	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
220.227.112.205	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
87.68.68.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
89.187.221.12	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.34.202.0	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.150.249.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.166.22.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
176.12.142.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
93.172.0.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
2.54.35.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
2.54.16.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
37.142.191.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
46.121.209.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
37.142.165.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
193.61.54.39	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
77.125.130.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
188.161.183.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
37.26.146.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
31.168.147.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
62.90.210.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.36.229	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.36.229	Block	2086
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	840
5.28.131.167	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.28.131.167	Block	209
31.154.135.45	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	98
2.52.12.74	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	95
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	84
46.19.85.4	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.85.4	None	70
81.218.56.171	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	56
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	55
62.219.248.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	42
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	28
52.88.3.64	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
109.65.211.30	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
37.142.64.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
178.78.148.39	Armenia	147.237.77.216	dover.idf.il	Parameter Type Violation __viewstategenerator in www.idf.il/1283-18521-en/dover.aspx	Block	14
94.159.244.155	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
80.178.195.147	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
5.29.119.39	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
54.169.222.155	Singapore	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	14
149.78.49.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
45.63.49.95		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	14
84.108.0.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
2.54.51.28	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	14
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	14
66.249.64.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
95.128.67.20	Belarus	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.142	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.19.86.142	Block	14
5.79.74.89	Netherlands	147.237.77.74	law.idf.il	Suspicious Response Code	Block	14
80.179.255.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
157.55.39.93	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/links/	Block	14
46.19.85.4	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding x5yS-z/q7R(T]C_* in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
84.228.205.110	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
77.126.186.141	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.186.141	Block	14
2.54.160.6	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
185.32.179.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.34	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1880	Block	14
207.46.13.143	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	14
62.219.248.97	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.248.97	Block	14
176.12.144.49	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	14
87.68.76.130	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
77.126.186.141	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9841-he/refuah.aspx	Block	14