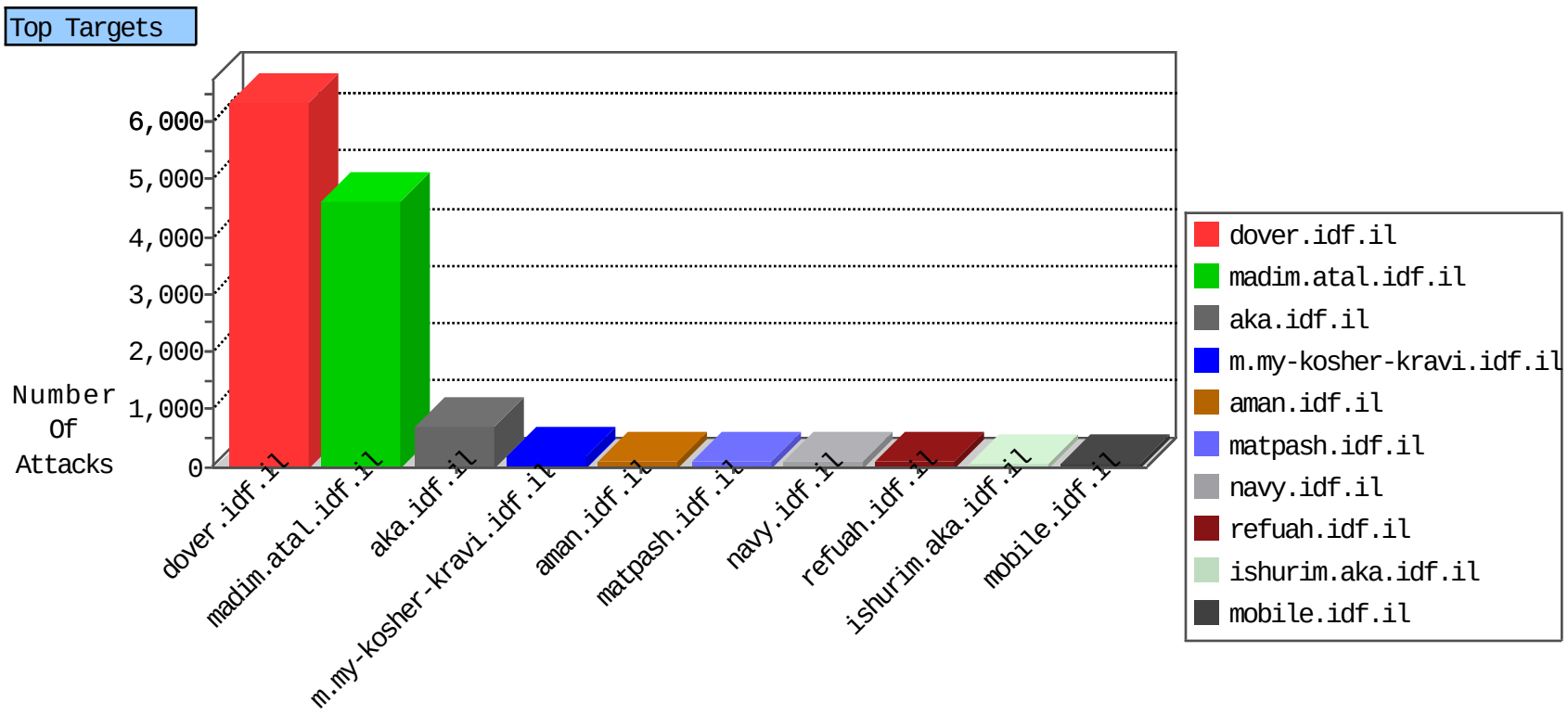
10-27-2015-09:04:06 to 10-27-2015-10:04:06

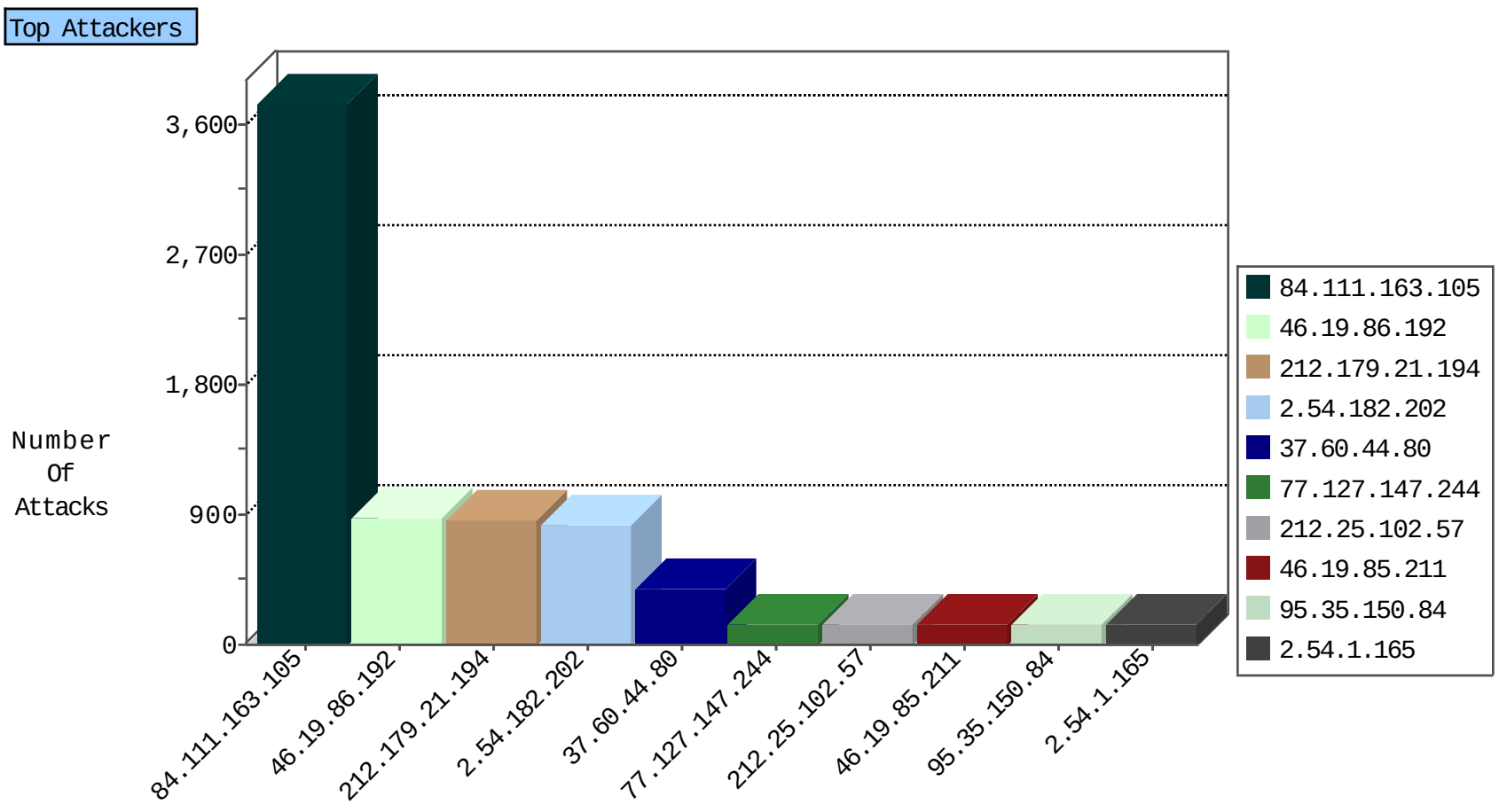
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-27-2015-09:04:06 to 10-27-2015-10:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
46.19.85.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
37.142.168.26	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	26
46.19.85.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
212.143.40.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
46.19.86.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
77.158.88.42	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
37.142.158.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.66.17.132	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
192.168.1.102		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.86.213	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	5
46.19.86.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.67.139.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.228.106.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.148.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.6.119.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.169.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.64.254.199	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
37.26.147.233	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	3
91.227.164.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
81.218.97.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.109	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
95.35.150.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
77.158.88.42	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.85.131	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.93.192	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.169.186	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.12.145.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.7.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-27-2015-09:04:06 to 10-27-2015-10:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
24.156.108.59	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-27-2015-09:04:06 to 10-27-2015-10:04:06

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	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
194.90.144.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.176.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.124.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.158.88.41	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
209.88.173.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.178.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.9.31.146	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
192.118.12.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.147.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.108.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.210.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.118.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.102.8.178	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.126.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.148.157.229	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 1024	1

10-27-2015-09:04:06 to 10-27-2015-10:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.182.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	806
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	803
37.60.44.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	380
212.25.102.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	145
46.19.85.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
2.54.1.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
95.35.150.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	137
144.24.20.228	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
107.167.107.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
70.208.66.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
2.54.11.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
46.19.86.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
46.116.143.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
176.13.15.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
46.19.85.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
149.200.222.45	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.19.85.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
78.9.103.66	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
79.177.212.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
2.52.170.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
82.81.193.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
77.158.88.42	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
46.19.86.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
166.137.10.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
176.13.15.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
212.179.159.253	Israel	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	First packet isn't SYN	drop	28
174.139.1.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
84.111.163.105	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
212.235.68.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
213.8.44.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
81.218.116.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
31.168.100.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
37.142.192.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	22
37.142.235.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
213.186.177.2	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
109.65.24.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.163.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3725
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	777
77.127.147.244	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	147
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	96
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	84
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	56
85.65.193.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	28
192.118.11.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
188.143.232.21	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	28
46.19.85.123	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	28
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
176.13.20.92	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	28
132.72.130.160	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
46.19.85.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
31.168.28.39	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
79.176.34.2	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	14
185.101.107.57		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	14
46.19.86.207	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
37.26.148.208	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
81.218.116.129	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
149.88.178.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
37.26.146.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
79.179.108.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
46.120.223.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	14
37.26.148.208	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
109.66.164.194	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	14
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/showbig.aspx	Block	14
212.143.3.44	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method POST for www.chinuch.aka.idf.il/900-he/chinuch.aspx	None	14
176.12.144.148	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
37.26.147.225	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	14
89.139.11.47	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	14
79.181.125.195	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	14
66.249.64.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
188.143.232.21	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/900-en/	Block	14
109.66.164.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	14
74.82.47.4	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	14
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_campaign in www.aka.idf.il/main/home/default.aspx	None	14
37.26.148.208	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.208 (Open Mode)	None	14
89.139.11.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	14
79.181.125.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	14
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9064-he/refuah.aspx	Block	14
109.186.11.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
46.19.85.147	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	14
2.52.8.219	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
176.13.22.63	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1540	Block	14
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_medium in www.aka.idf.il/	None	14
37.26.148.208	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.208 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	14
92.61.225.10	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14