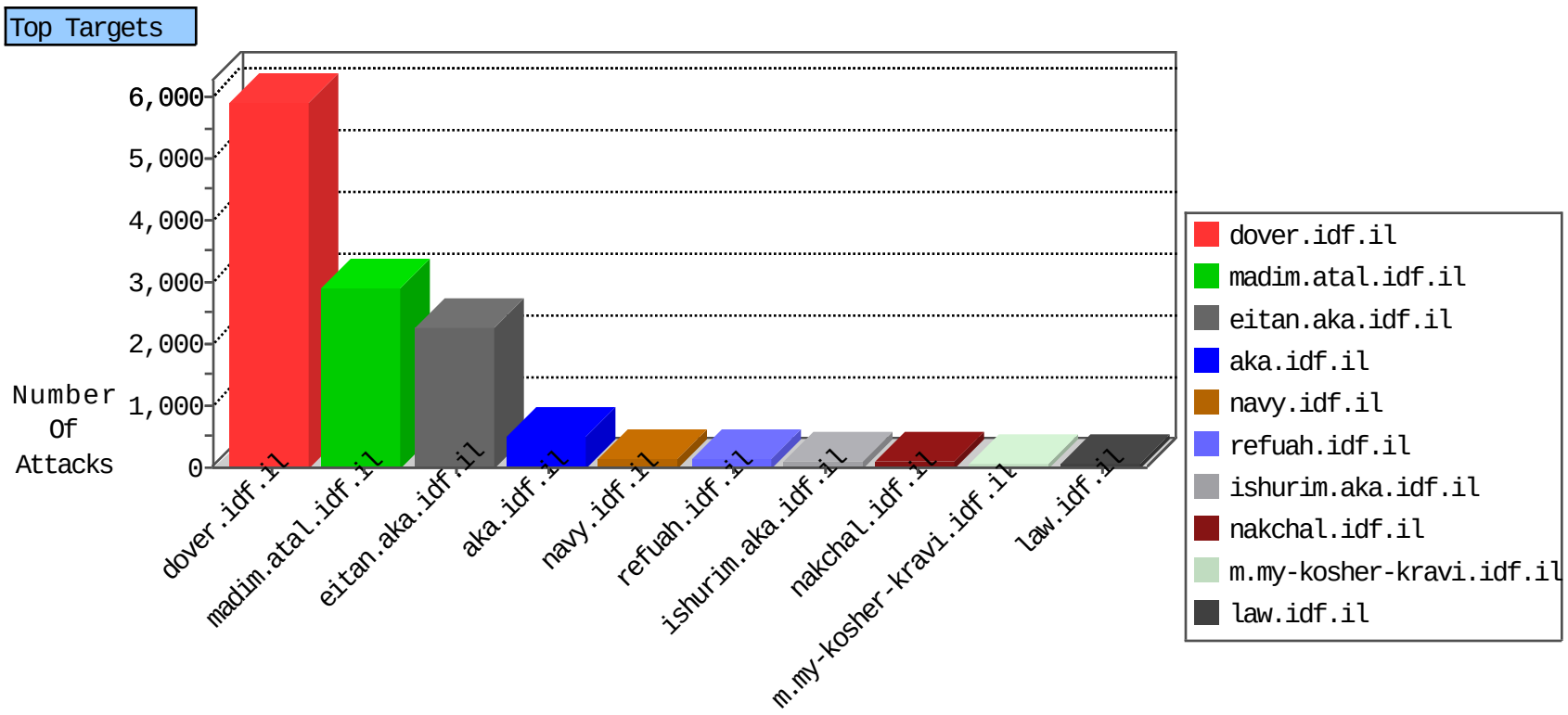
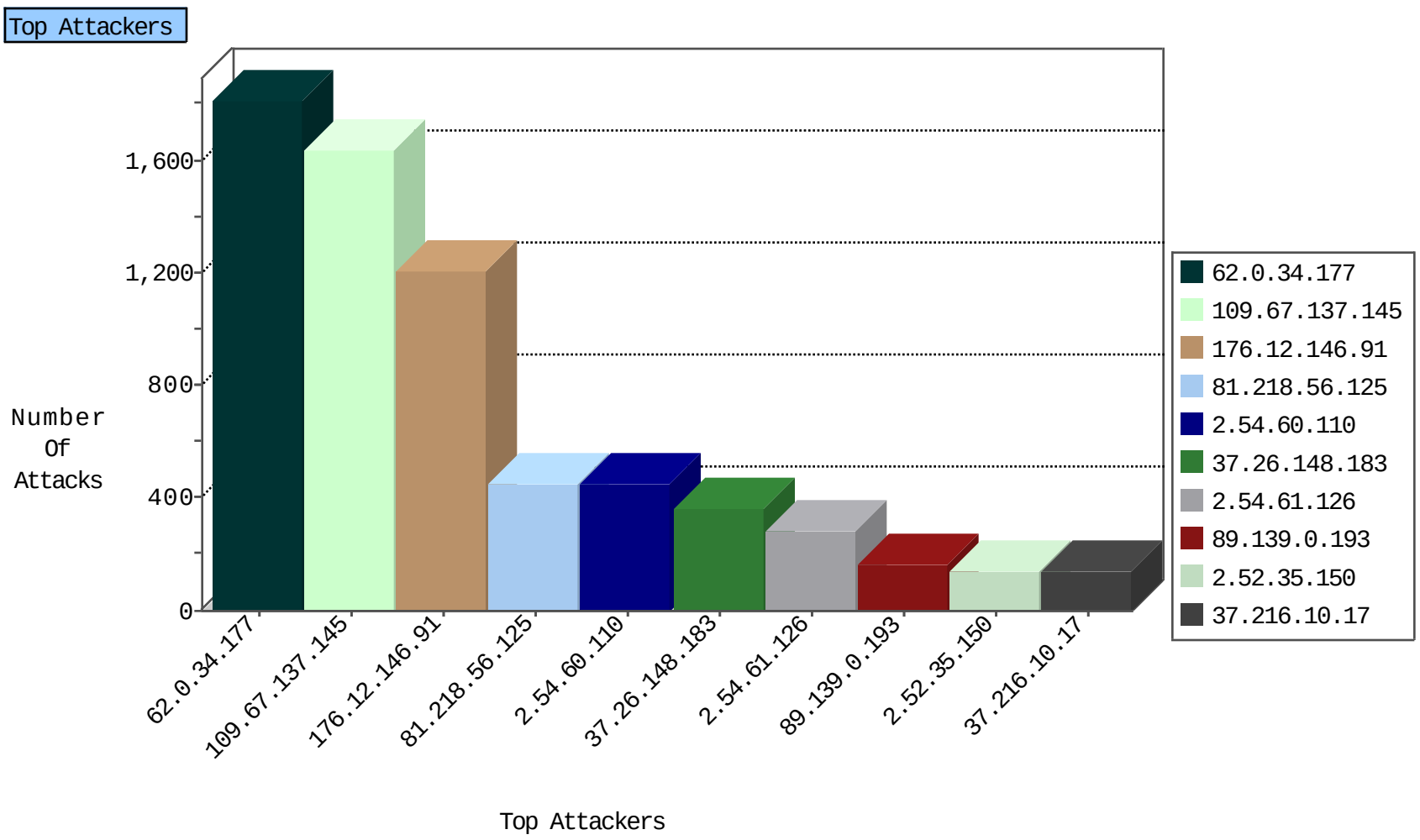
10-25-2015-08:04:02 to 10-25-2015-09:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-25-2015-08:04:02 to 10-25-2015-09:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	295
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
87.69.20.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
87.68.26.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
192.117.10.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
77.126.151.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
46.19.85.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
46.19.85.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
2.54.179.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
212.143.233.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.54.177.182	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	11
62.219.137.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
82.145.218.242	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
192.88.162.1	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
91.227.164.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
77.126.151.92	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.54.177.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.140.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
77.125.79.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.12.146.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.228.215.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.117.0.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.81.3.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.81.17.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.12.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.152	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
5.29.128.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.134.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.28.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.183.22.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.25.112.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.25.112.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.13.19.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.5.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.152	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.13.9.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.18.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.65.29.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
5.8.201.254	Russian Federation	147.237.8.45	e.eitan.idf.il	L4 Source or Dest Port Zero	drop	1
79.180.37.62	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
176.13.16.60	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.22.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.183.0.168	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

10-25-2015-08:04:02 to 10-25-2015-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-25-2015-08:04:02 to 10-25-2015-09:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.230.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.60.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.148.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.175.225.230	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
81.218.33.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.0.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.55.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.59	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.55.40	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.0	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.72.167	United States	ishurim.aka.idf.il	ET DROP Dshield Block Listed Source	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
93.172.136.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.43.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.113.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.140.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.135.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.236.96.52	147.237.72.217	Germany	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1

10-25-2015-08:04:02 to 10-25-2015-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.60.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	448
37.26.148.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	363
2.54.61.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	281
89.139.0.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	163
2.52.35.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
37.216.10.17	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
2.54.26.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
24.52.212.131	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
81.218.33.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
216.183.66.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
46.19.86.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
90.205.38.63	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
62.90.127.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
85.130.247.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
176.228.164.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
109.67.124.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
79.178.165.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
85.158.139.228	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
85.64.102.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
213.57.170.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.86.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
82.102.169.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
31.168.243.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
100.100.46.241		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
5.22.130.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
70.192.193.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
82.81.17.28	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.13.22.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
100.100.119.94		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
46.19.86.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
176.13.22.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
217.194.207.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
176.13.4.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21

10-25-2015-08:04:02 to 10-25-2015-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.0.34.177	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1792
109.67.137.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1638
176.12.146.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1202
81.218.56.125	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.56.125	Block	420
176.12.138.118	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	96
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.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
2.54.150.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
176.13.22.62	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	42
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	42
46.19.85.120	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/clientscripts/scroller/jquery.http/1.1 200 okdate: thu, 22 oct 2015 10:42:15 gmtlast-modified: tue, 26 jun 2012 07:41:22 gmtetag:	Block	28
84.94.161.118	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	28
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	28
2.54.27.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
79.177.20.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	28
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/16481.jpg	Block	14
2.54.28.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	14
95.35.31.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
79.180.176.151	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
176.13.16.183	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
46.19.85.103	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request request version	Block	14
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/leftarrow.png	Block	14
212.25.92.49	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 212.25.92.49	Block	14
46.116.29.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	14
79.182.107.199	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	14
46.19.85.103	Israel	147.237.76.86	navy.idf.il	Illegal HTTP Version __atuvs=562c7be109e011db000	Block	14
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	14
212.117.156.225	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
31.154.91.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	14
79.183.0.136	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
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	14
182.118.54.176	China	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/../shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	14
46.19.85.103	Israel	147.237.76.86	navy.idf.il	Malformed URL __atuvc=1	Block	14
85.250.119.120	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	14
79.177.20.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	14
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation searchText in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	14
37.26.147.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
81.218.56.125	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	14
66.249.78.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
185.32.179.160	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
46.19.85.103	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method enejtuxtmqmdipyl21ay; in URL __atuvc=1	Block	14
86.47.80.146	Ireland	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	14
46.19.85.2	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14

10-25-2015-08:04:02 to 10-25-2015-09:04:02