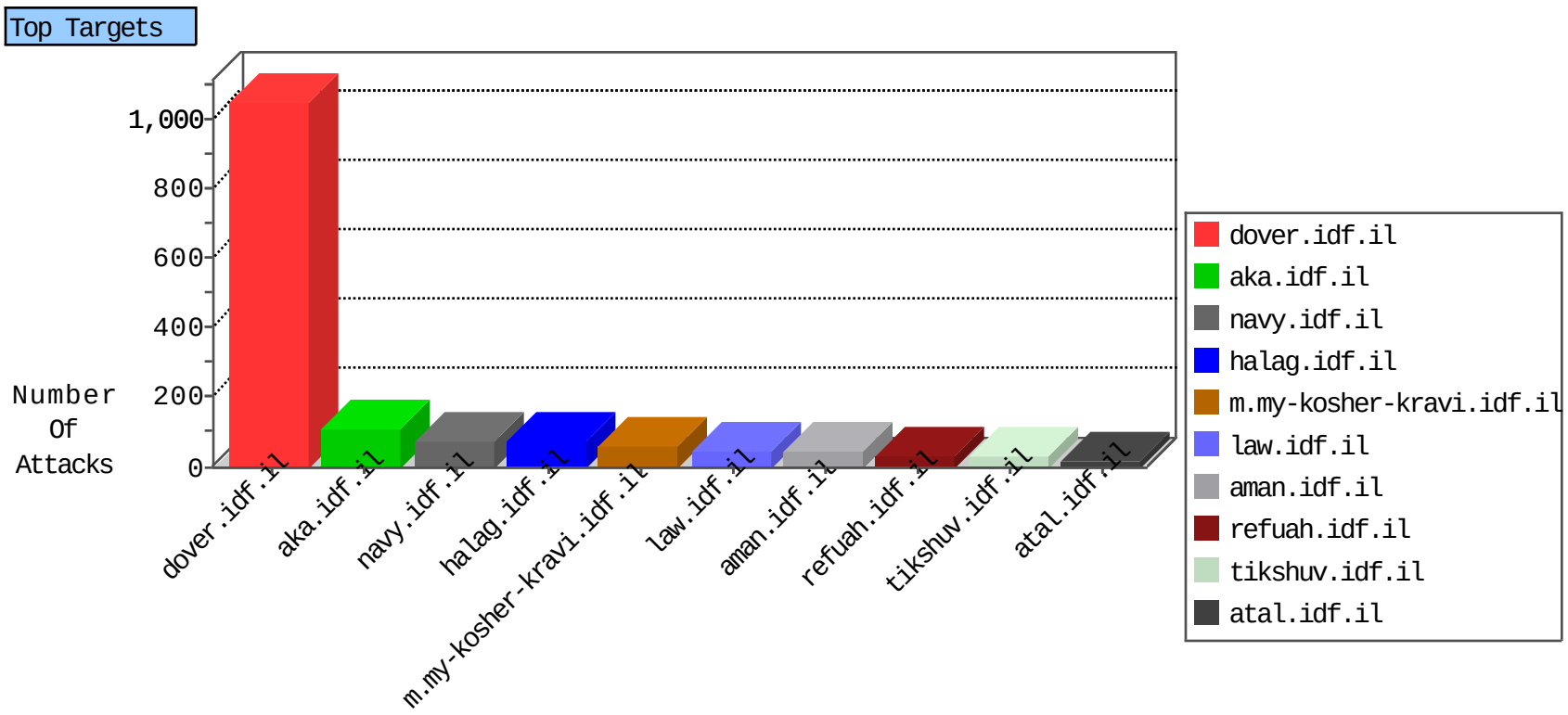
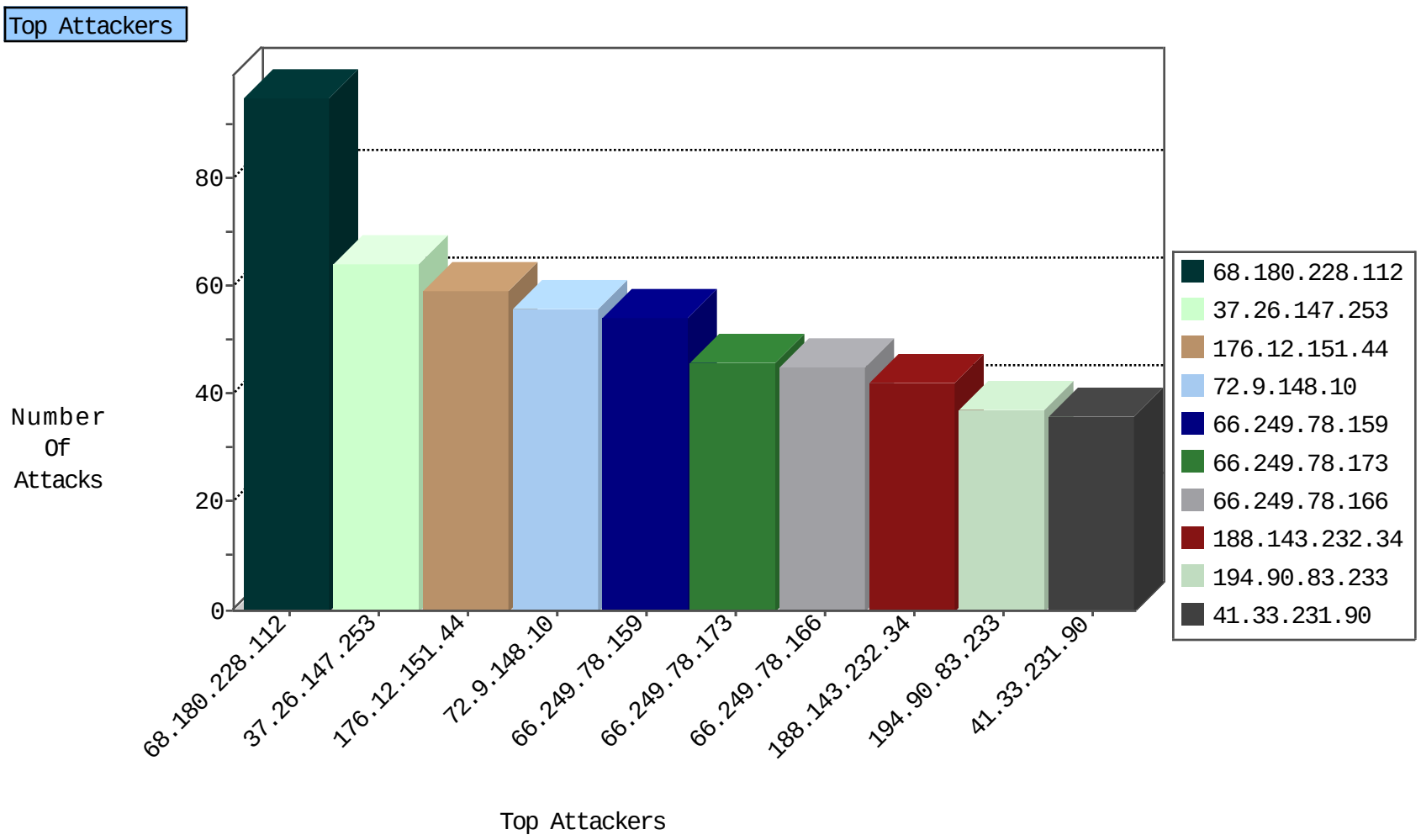
10-23-2015-07:04:00 to 10-23-2015-08:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-23-2015-07:04:00 to 10-23-2015-08:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
194.177.16.3	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
79.178.178.88	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
46.116.106.182	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
10.0.0.1		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
110.251.26.74	China	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
222.186.56.42	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
2.54.36.220	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
142.54.187.44	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
104.193.10.60	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
183.60.48.25	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Udp	drop	1
79.182.100.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.182.100.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.54.172.98	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1
104.193.10.60	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

10-23-2015-07:04:00 to 10-23-2015-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.32.82	United Kingdom	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

10-23-2015-07:04:00 to 10-23-2015-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.113.143	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	6
62.210.113.143	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
54.209.60.63	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
66.249.78.173	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
222.186.30.160	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.160	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.160	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.38	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.186.50.47	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
222.186.50.47	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
62.210.113.143	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP /cgi-bin/ access	1
222.186.50.47	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.160	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.160	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
222.186.30.160	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.38	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.235	United States	sviva.idf.il	ET DROP Dshield Block Listed Source	1
93.174.93.138	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.50.47	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
222.186.50.47	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
222.186.50.47	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1

10-23-2015-07:04:00 to 10-23-2015-08:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.147.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
194.90.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.71.213		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
78.53.226.50	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
77.126.11.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.64.59.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
177.81.40.59	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
100.100.80.250		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	17
79.178.178.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.182.100.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.39.121	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.52.177.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.116.106.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.222	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.83	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
78.53.226.50	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.67.200	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
157.55.39.84	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.33.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.107.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.151.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	6
149.78.190.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.191	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.144.164	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
157.55.39.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

10-23-2015-07:04:00 to 10-23-2015-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
176.12.151.44	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.151.44	None	41
188.143.232.13	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	28
188.143.232.34	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$ddlSearchPlaces in www.mag.idf.il/656-he/patzar.aspx	Block	28
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	28
52.8.90.191	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/iturim/asp/results.asp	None	14
176.12.149.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20236-he/idfgdover.aspx	Block	14
185.32.179.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20379-he/idfgdover.aspx	Block	14
207.46.13.48	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	14
176.12.151.44	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8021-he/dover.aspx	Block	14
213.176.236.108	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	14
45.35.71.181		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	14
188.143.232.34	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$ddlSearchPlaces in www.law.idf.il/656-he/patzar.aspx	Block	14
74.82.47.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
66.249.67.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16893-he/dover.aspx	Block	14
213.176.236.108	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation part in www.idf.il/hebrew/nakhal/page.asp	Block	14
176.13.22.9	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 119 cookies	Block	14
80.246.133.84	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
66.249.75.23	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
182.118.60.193	China	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../shared/clientscripts/jquery/global.js	Block	14
46.19.85.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6

10-23-2015-07:04:00 to 10-23-2015-08:04:00