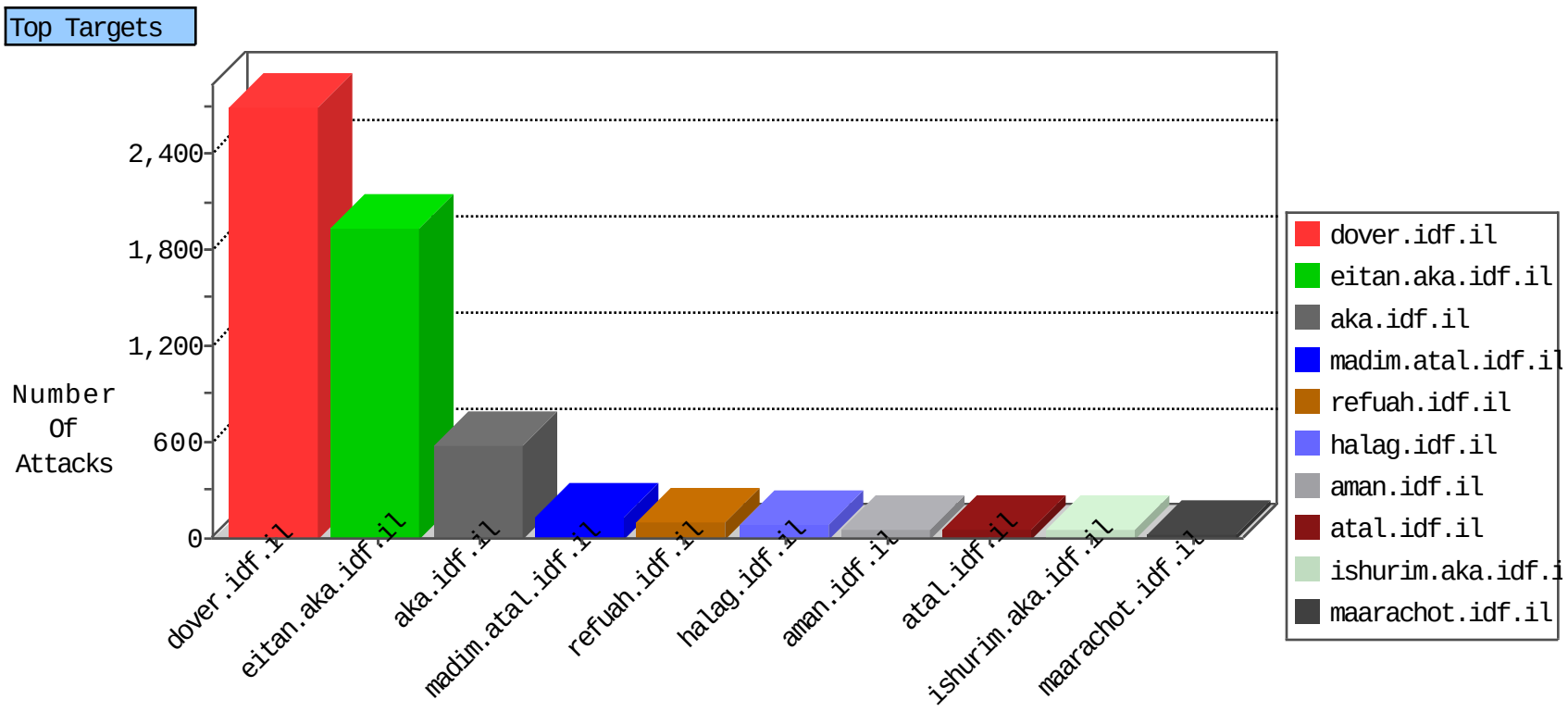
12-06-2015-22:04:04 to 12-06-2015-23:04:04

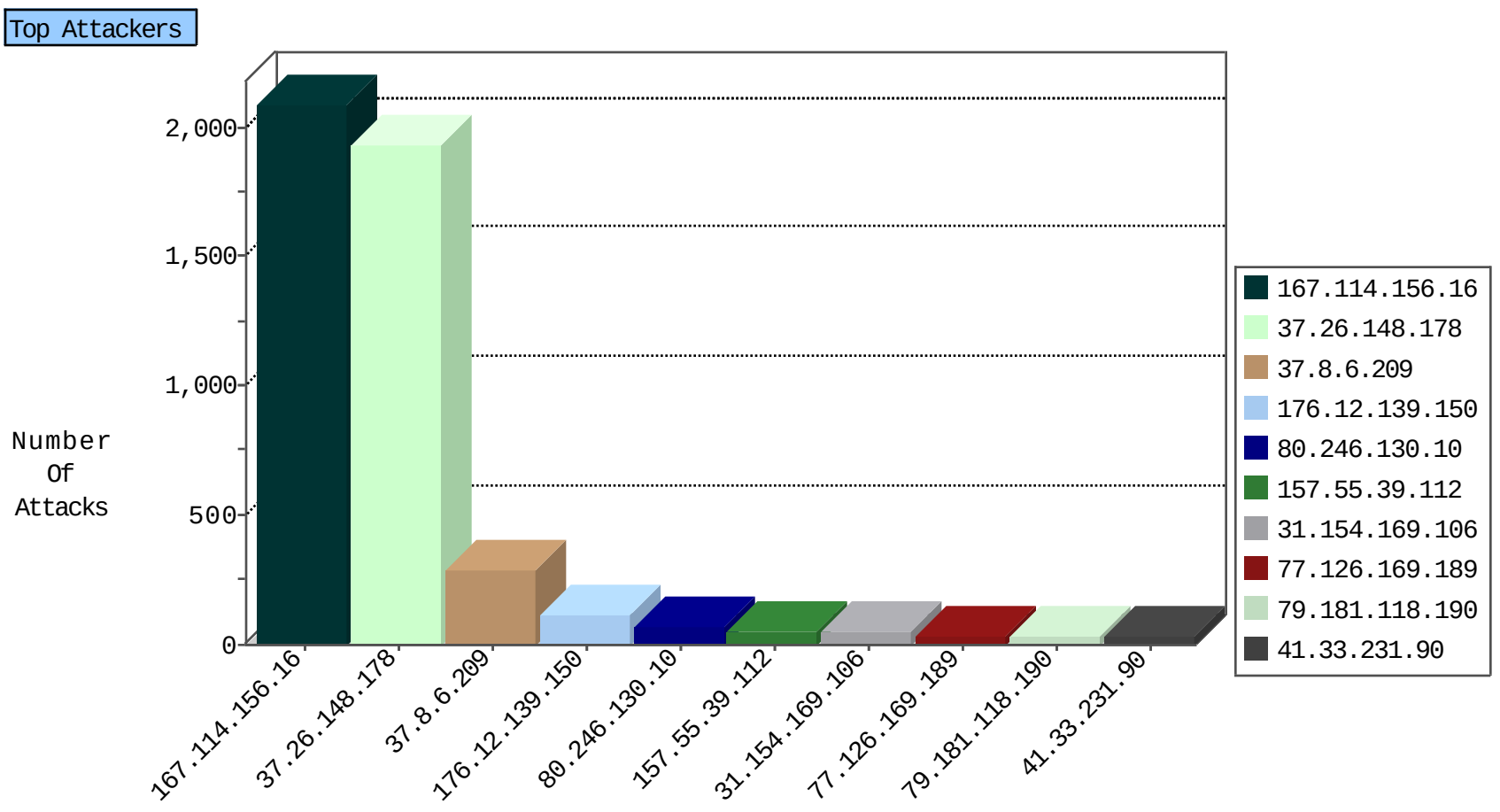
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-06-2015-22:04:04 to 12-06-2015-23:04:04

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	DOS-Tool-SwitchbladG	dest-reset	3386

12-06-2015-22:04:04 to 12-06-2015-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-06-2015-22:04:04 to 12-06-2015-23:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.10	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.146.220.220	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.16	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.146.220.220	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
220.245.240.26	147.237.8.50	Australia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
113.106.129.219	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
220.245.240.26	147.237.8.50	Australia	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
199.101.186.202	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
74.117.209.135	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.16	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.146.220.220	147.237.77.74	Russian Federation	law.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.16	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
46.146.220.220	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.33	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
113.106.129.219	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
220.245.240.26	147.237.8.50	Australia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
89.163.140.142	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
199.101.186.202	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
78.193.2.8	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.202	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -f -sS	1
74.117.209.135	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
185.106.94.16	147.237.77.178		e.matpash.idf.il	ET SCAN Potential SSH Scan	1
46.146.220.220	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

12-06-2015-22:04:04 to 12-06-2015-23:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.148.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1677
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	SAM rule	drop	133
31.154.169.106	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
79.181.118.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
157.55.39.112	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
80.246.130.10	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence		monitor	22
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
84.228.148.65	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
77.127.206.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
80.246.130.10	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
5.28.169.108	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
77.126.169.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.23.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
157.55.39.112	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
79.179.18.103	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.143.83	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.28.158.80	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
176.12.141.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.31.103.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
5.28.158.80	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
46.19.86.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
77.126.169.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.143.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
77.126.169.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.142.226.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.28.136.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.23.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.130.10	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.2.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.65	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.126.152.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.189.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.10	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.146.247	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.187.101.7	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.38.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.112	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.206.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.22.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.134.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.190.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
149.78.37.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.103	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.2.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

12-06-2015-22:04:04 to 12-06-2015-23:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.178	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	245
176.12.139.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.8.6.209	Block	16
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1133-he/dover.aspx	Block	6
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1362-he/dover.aspx	Block	5
88.128.80.66	Germany	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.178	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 37.26.148.178	Block	3
176.13.22.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
157.55.39.112	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
95.86.116.125	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21811-he/idfgdover.aspx&sa=u&ved=0ahukewjikohrhmjjahuedw8khbikdmyqfggimaa&usg=afqjcne5nfosmshhgfxopawypgppoqrtwa	Block	3
77.127.169.22	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
37.59.62.43	France	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
84.228.148.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.14.119	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.12.139.150	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.139.150	Block	2
176.13.6.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	2
85.64.202.120	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1414-10846-he/dover.aspx	Block	1
207.46.13.26	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/	Block	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1133-22985-he/dover.aspx	Block	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1842-he/dover.aspx	Block	1
109.64.3.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1414-10824-he/dover.aspx	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9434-he/dover.aspx	Block	1
185.3.144.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1133-22449-he/dover.aspx	Block	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1806-he/dover.aspx	Block	1
31.13.110.126	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1415-10810-he/dover.aspx	Block	1
84.108.47.67	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1362-17745-he/dover.aspx	Block	1
46.19.85.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.94	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
37.26.148.178	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 37.26.148.178	Block	1
109.230.245.229	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/cms_wysiwyg/directive/index/	Block	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1414-22566-he/dover.aspx	Block	1
79.179.189.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1150-he/dover.aspx	Block	1

12-06-2015-22:04:04 to 12-06-2015-23:04:04

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1133-22955-he/dover.aspx	Block	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1815-he/dover.aspx	Block	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.8.6.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation __EVENTTARGET in www.idf.il/1414-10835-he/dover.aspx	Block	1
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2424.jpg	Block	1
195.154.226.90	France	147.237.77.74	law.idf.il	Illegal HTTP Version HTTP/	Block	1

12-06-2015-22:04:04 to 12-06-2015-23:04:04