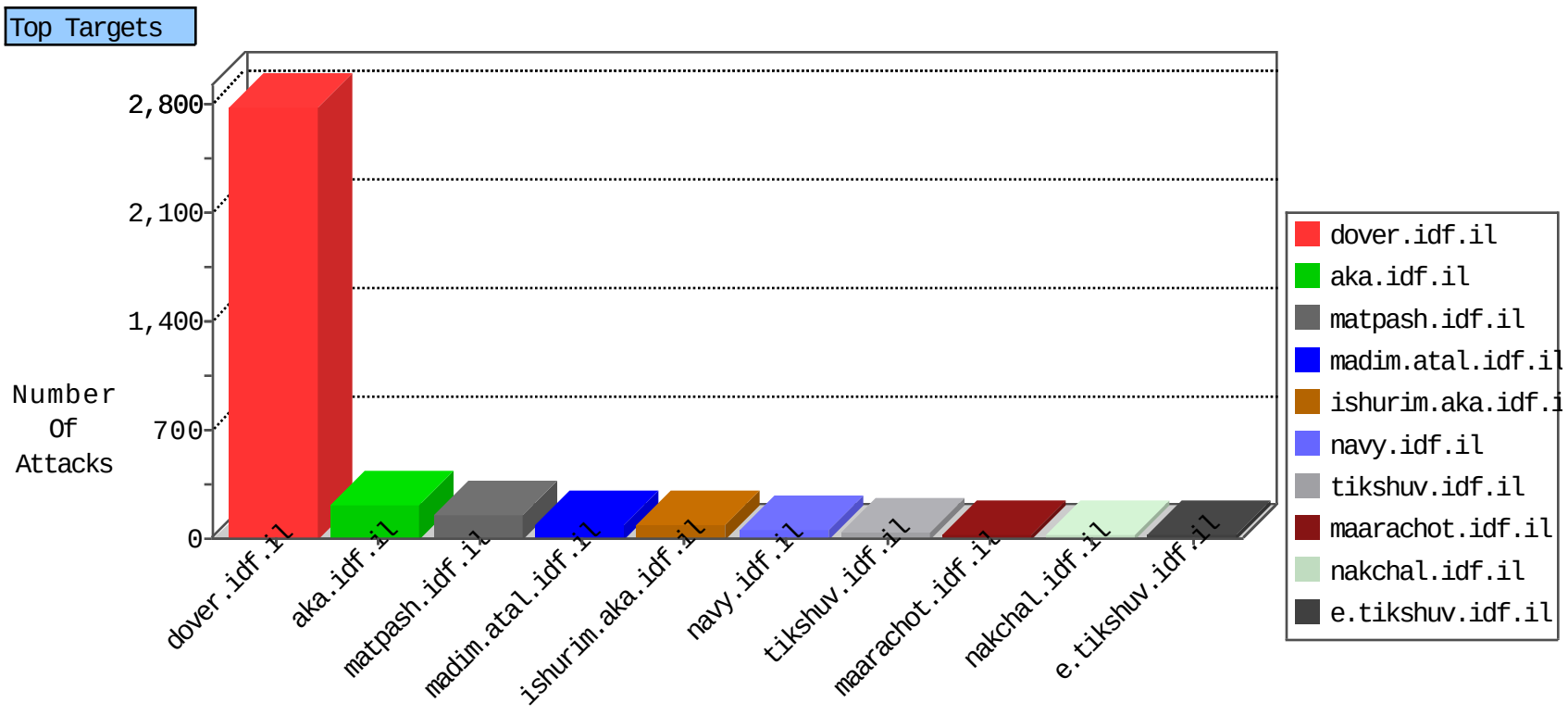
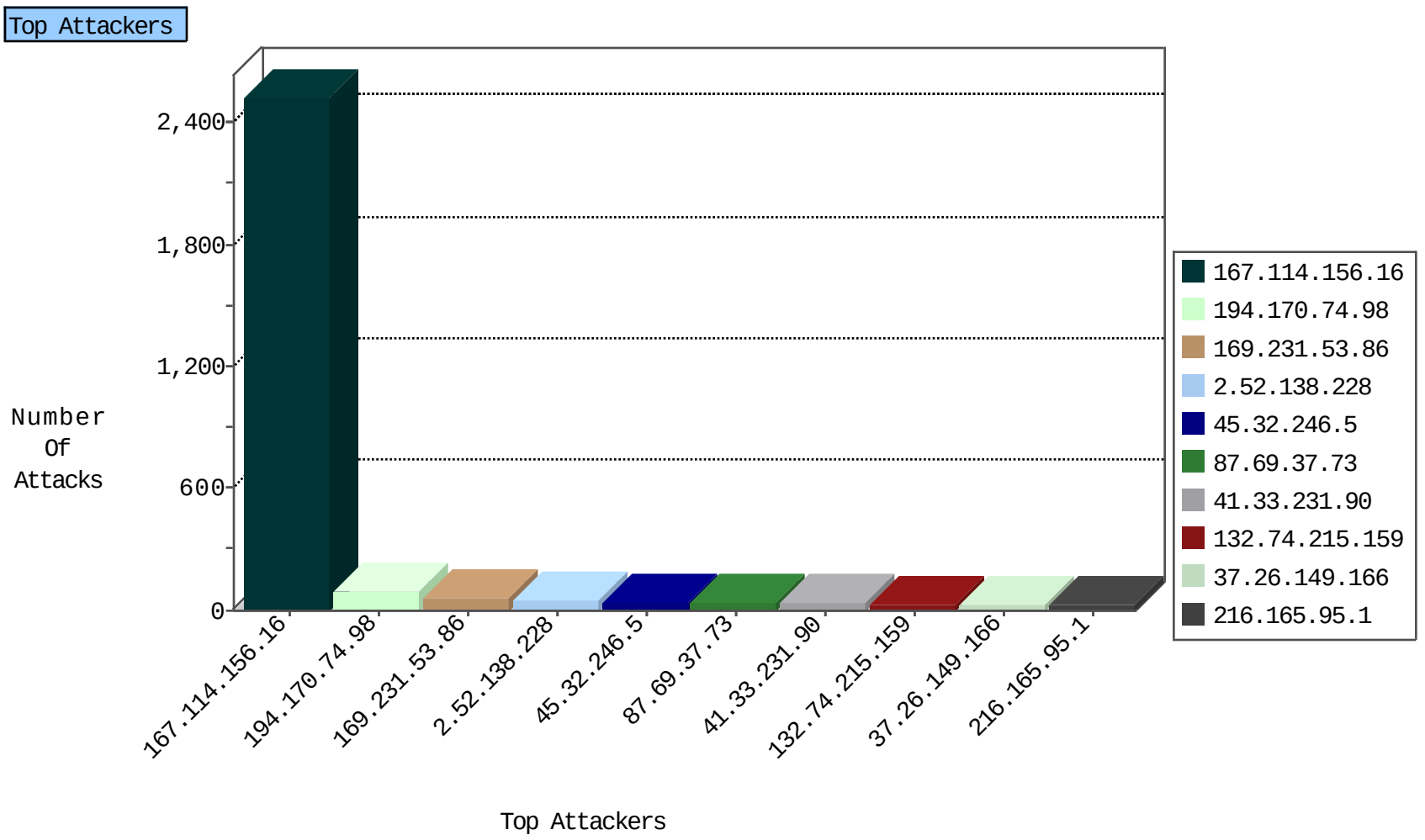
12-10-2015-09:04:08 to 12-10-2015-10:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-10-2015-09:04:08 to 12-10-2015-10:04:08

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	3624
66.249.79.10	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3088
216.165.95.1	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
45.32.246.5		147.237.8.50	e.tikshuv.idf.il	Invalid TCP Flags	drop	6
45.32.246.5		147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	6
98.209.136.30	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
66.151.55.112	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
66.151.55.110	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
167.88.12.209	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
77.158.88.41	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.151.55.114	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
82.80.217.70	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.55.103.19	United States	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
66.151.55.117	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

12-10-2015-09:04:08 to 12-10-2015-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.33.106.123	United States	147.237.77.176	matpash.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
52.35.180.120	United States	147.237.76.200	eitan.aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1

12-10-2015-09:04:08 to 12-10-2015-10:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
212.235.80.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.93.218.250	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.34	Ukraine	yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
85.65.190.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 2048	1
45.32.246.5	147.237.76.86		navy.idf.il	ET SCAN NMAP -f -sS	1
213.8.204.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.230.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
158.255.2.52	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.155	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.2.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.57.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-10-2015-09:04:08 to 12-10-2015-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.170.74.98	United Arab Emirates	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	90
169.231.53.86	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	46
87.69.37.73	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
169.231.53.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.197	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
77.158.88.41	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
216.165.95.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.64	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.143.61.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
132.74.215.159	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
77.158.88.40	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
93.94.40.14	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.178.15.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.118	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
213.57.128.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
132.74.215.159	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	10
213.57.128.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
45.32.246.5		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.8	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
45.32.246.5		147.237.8.50	e.tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
120.36.226.3	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
45.32.246.5		147.237.8.50	e.tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
46.19.85.173	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.92	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
87.68.23.228	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
147.236.238.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.160.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.109.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.44.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.7.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.202	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.202	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.41.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.173	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.241.226.39	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	5
94.230.86.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.116.90.139	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.142.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.203	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
83.130.100.176	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.116.90.139	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
83.130.100.176	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.183.193.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-10-2015-09:04:08 to 12-10-2015-10:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
37.26.149.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
213.8.204.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	7
185.32.179.114	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	5
176.13.1.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
213.8.204.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.204.37	Block	4
213.8.204.37	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.155.179	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.68.155.179	Block	3
176.13.4.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.156.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
52.33.106.123	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 52.33.106.123	Block	2
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	2
52.35.180.120	United States	147.237.76.200	eitan.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
52.35.180.120	United States	147.237.76.200	eitan.aka.idf.il	Distributed NULL Character in Method	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
212.25.102.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.61.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/founded.htm	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
37.26.147.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
184.105.247.196	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
2.52.11.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.235.189.141	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/163-en/patzar.aspx	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8810-he/refuah.aspx	Block	1
45.55.132.217		147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on /	Block	1
198.20.87.98	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
79.183.186.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
2.54.63.204	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation fromDate in www.navy.idf.il/shared/ajax/getnewslobbycontent.aspx	Block	1
149.88.152.99	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
52.33.106.123	United States	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method Â„ ;*Ã¢[[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]]{Ã„Ã• [[#29]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]]wTÃ„ in URL	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.108.236.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.92.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.127.162.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.97	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /x	Block	1
66.249.74.100	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-9481-he/cogat.asp	Block	1
213.8.204.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
52.33.106.123	United States	147.237.77.176	matpash.idf.il	Multiple NULL Character in Method from 52.33.106.123	Block	1
45.55.147.127		147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on /	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
66.249.79.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/main35cc.html	Block	1
157.55.39.242	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1

12-10-2015-09:04:08 to 12-10-2015-10:04:08