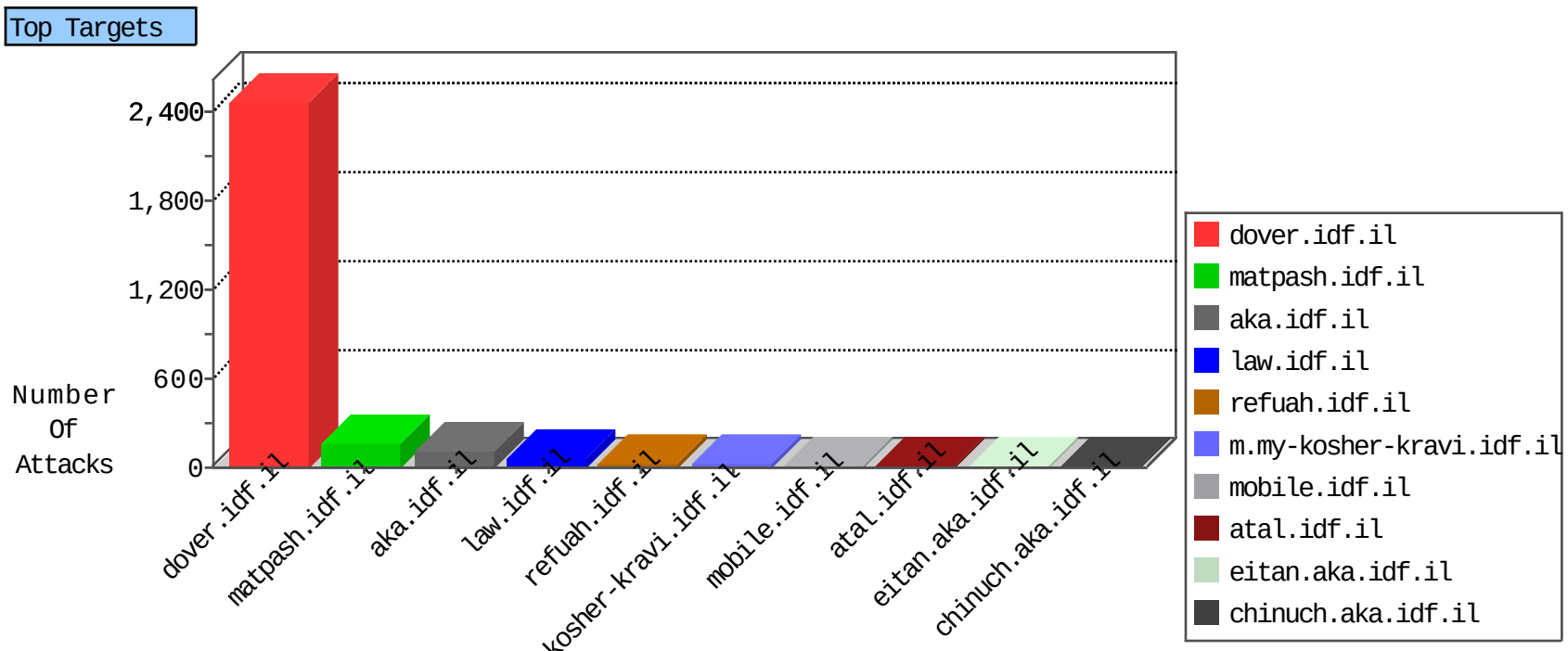
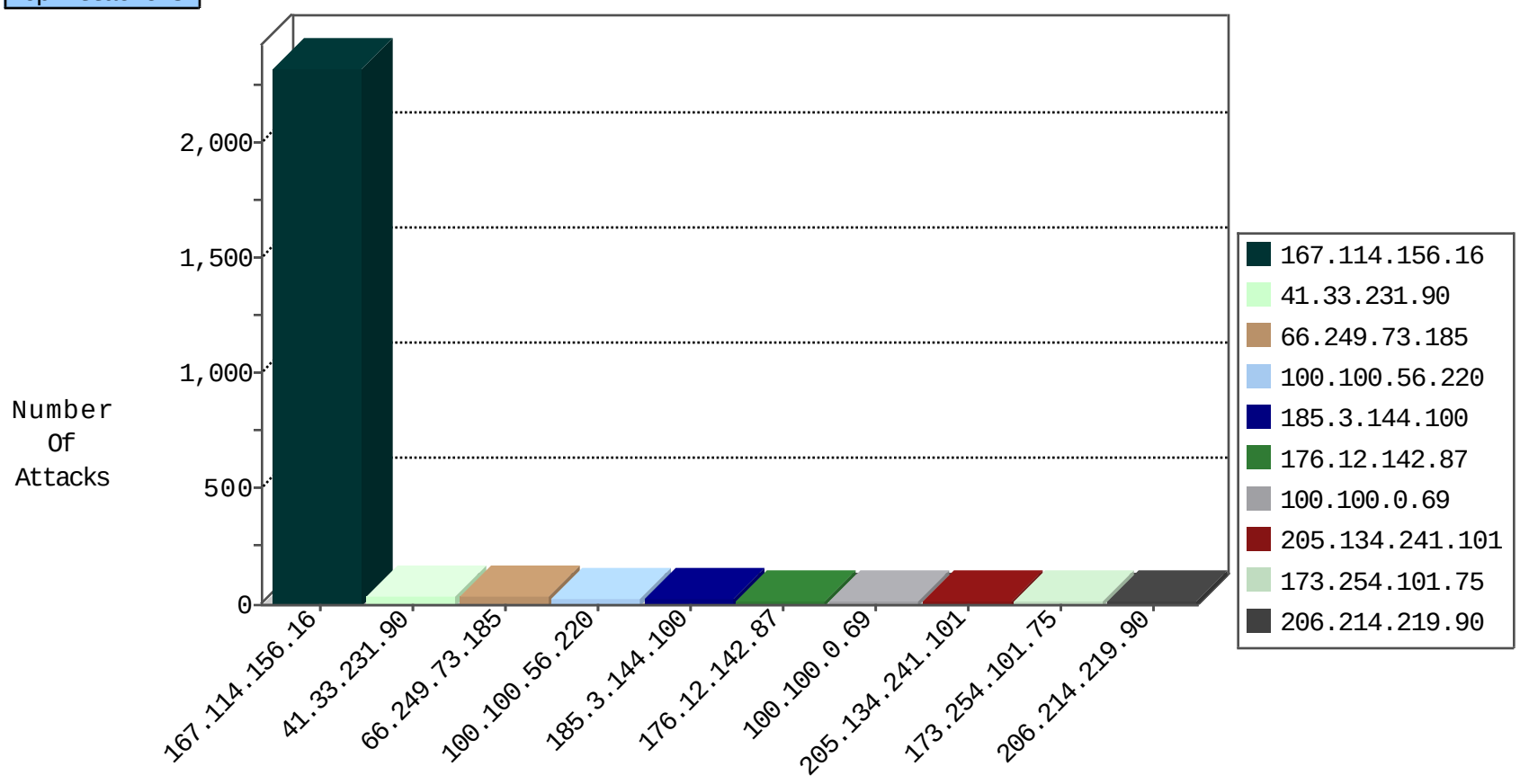
11-28-2015-08:04:07 to 11-28-2015-09:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-28-2015-08:04:07 to 11-28-2015-09:04:07

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	3770
66.249.66.39	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
58.215.79.100	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.35.62.42	Switzerland	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1
216.239.179.230	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-28-2015-08:04:07 to 11-28-2015-09:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-28-2015-08:04:07 to 11-28-2015-09:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
37.238.75.80	147.237.76.147	Iraq	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
37.238.75.80	147.237.77.216	Iraq	dover.idf.il	ET SCAN Potential SSH Scan	1
37.238.75.80	147.237.76.198	Iraq	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.238.75.80	147.237.76.39	Iraq	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
37.238.75.80	147.237.72.167	Iraq	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
5.140.213.201	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.179.59.13	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.238.136.116	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -f -sS	1
37.238.75.80	147.237.76.200	Iraq	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
37.238.75.80	147.237.76.177	Iraq	ncore.idf.il	ET SCAN Potential SSH Scan	1
37.238.75.80	147.237.76.42	Iraq	refuah.idf.il	ET SCAN Potential SSH Scan	1
37.238.75.80	147.237.76.31	Iraq	nakchal.idf.il	ET SCAN Potential SSH Scan	1
31.6.71.154	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 1024	1
149.202.186.50	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.136.116	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
101.187.183.201	147.237.77.74	Australia	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-28-2015-08:04:07 to 11-28-2015-09:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.56.220		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
185.3.144.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.12.142.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
100.100.0.69		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
82.80.42.185	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.0.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.54.143.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.119	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.46.39.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.241.226.41	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
5.22.134.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
74.85.66.62	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
31.15.10.16	Czech Republic	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
74.85.66.62	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
77.125.161.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.175.106.199	Canada	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
50.87.35.180	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
195.178.106.120	Romania	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
5.22.131.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
50.87.119.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
149.78.46.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
24.17.155.131	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
195.178.106.120	Romania	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
188.40.0.148	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
85.250.252.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
87.69.67.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
71.6.158.166	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
216.218.206.78	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.162.141.118	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.108.123.46	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.228	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.79.166.59		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.211	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.28.173.89	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
112.74.67.109	China	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.78	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.40.0.148	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
37.26.149.212	Israel	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
139.162.141.118	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.244	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.41	United States	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 207.241.226.41	Block	4
176.56.62.44	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
205.134.241.101	United States	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
162.242.152.71	United States	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
154.66.204.37	South Africa	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
85.17.48.237	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
205.134.241.101	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	3
162.144.249.119	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
91.201.60.3	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
69.50.222.20	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
216.172.176.112	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	3
198.1.99.25	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
206.214.219.90	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
50.87.107.49	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
129.7.107.7	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
113.192.21.100	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
95.76.161.34	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
196.2.164.70	South Africa	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
67.20.76.105	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
206.214.219.90	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
91.194.234.18	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
50.87.11.34	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
117.55.235.30	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
173.254.101.75	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	3
192.145.239.21	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
205.134.251.17	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
173.254.101.75	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
188.65.113.171	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
173.254.83.101	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
192.145.239.21	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.145.239.21	Block	2
50.87.107.49	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
205.134.251.17	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 205.134.251.17	Block	2
113.192.21.100	Australia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	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
196.2.164.70	South Africa	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2
67.20.76.105	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
188.65.113.171	United Kingdom	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.65.113.171	Block	2
50.87.11.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
117.55.235.30	Australia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
216.172.180.60	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
176.56.62.44	United Kingdom	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 176.56.62.44	Block	2
205.134.241.101	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/index.php	Block	2
173.254.101.75	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2
162.242.152.71	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/index.php	Block	2
99.249.104.45	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	2
85.17.48.237	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 85.17.48.237	Block	2
173.254.83.101	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
162.144.249.119	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.144.249.119	Block	2

11-28-2015-08:04:07 to 11-28-2015-09:04:07