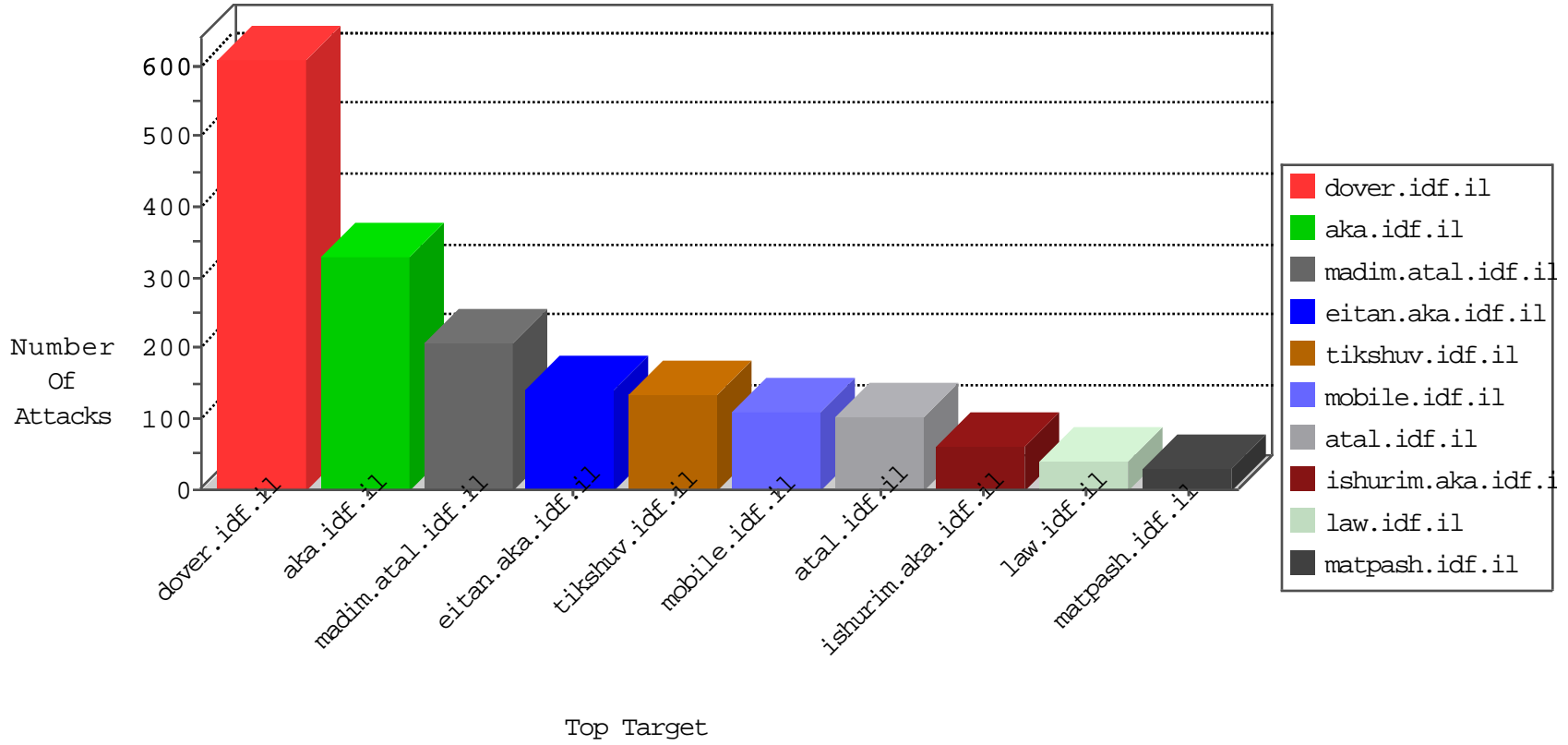


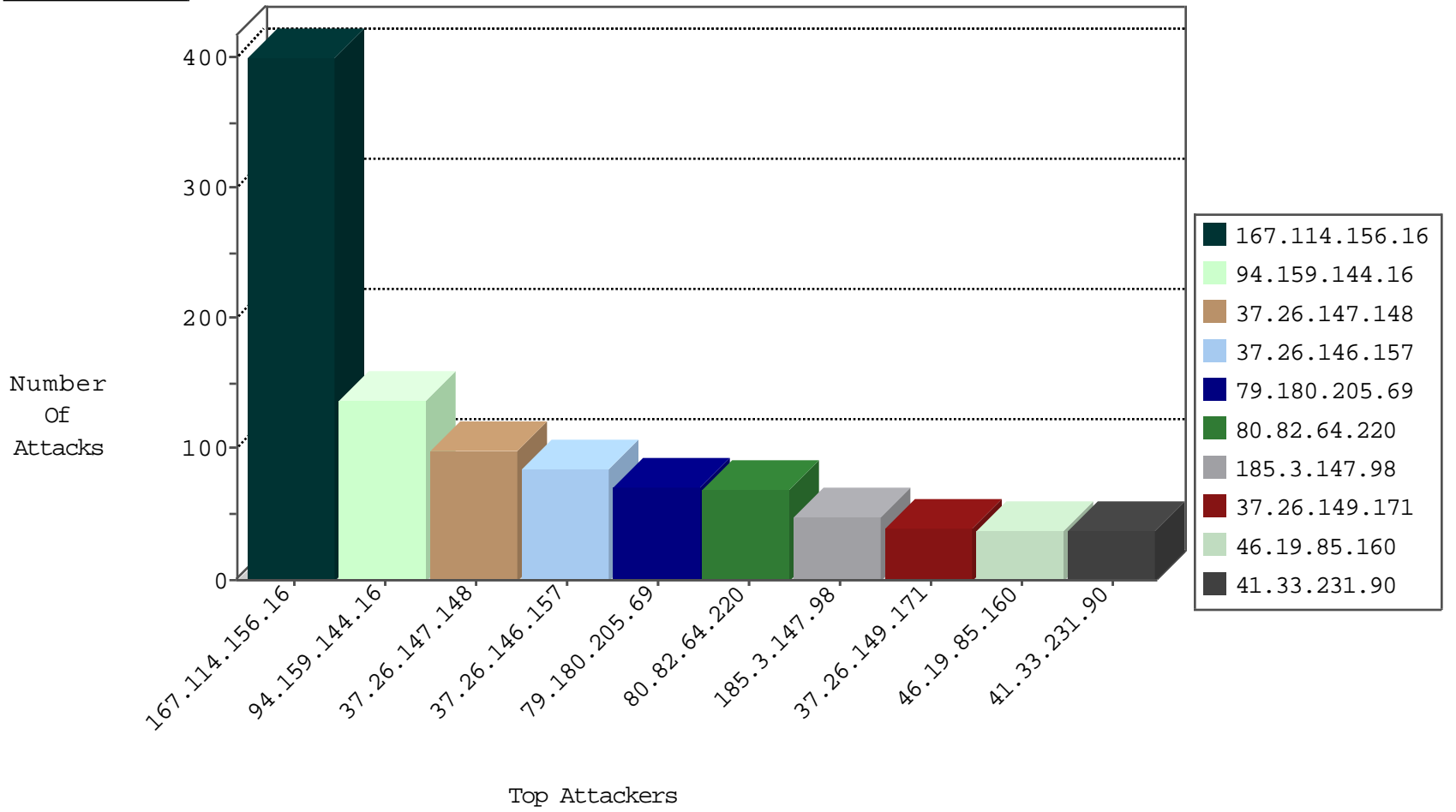
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3005
80.82.64.220	Netherlands	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	198
80.82.64.220	Netherlands	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	9
84.109.112.159	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
80.82.64.220	Netherlands	147.237.77.205	prisha.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
89.248.174.4	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

01-09-2016-19:04:03 to 01-09-2016-20:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
94.102.48.195	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.8.45	Kazakstan	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
88.204.187.90	147.237.8.45	Kazakstan	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
80.82.64.220	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.188	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
79.180.100.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.130.5.247	147.237.77.61		e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 1024	1
131.109.15.15	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.203	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.8.45	Kazakstan	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
88.204.187.90	147.237.0.35	Kazakstan	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
79.181.119.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
43.245.183.201	147.237.0.33	Japan	idf.il	ET SCAN NMAP -sS window 3072	1
185.130.5.247	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.147.148	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	99
37.26.146.157	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	83
79.180.205.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	68
46.19.85.160	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	38
37.26.149.171	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
85.130.130.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.3.147.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
212.14.239.10	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
172.56.27.85	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
77.127.136.51	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
109.64.25.7	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
2.54.23.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.12.246	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
87.69.246.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.65.125.131	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	8
82.166.216.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	8
82.166.216.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.116.196.23	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.100	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.144.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.210.183.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.229.161.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.214.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.46.39.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.171	Israel	147.237.8.45	e.eitan.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.219	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.176.23.115	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.229.134.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.253.221.223	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.64	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
197.165.156.240	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.161.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.253.195.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.129.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.4.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.208.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.8.204.40	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
149.78.4.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.144.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.159.144.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
94.159.144.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
2.52.173.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.120.6.53	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
109.67.160.225	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
176.13.20.9	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
46.120.219.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.253.133.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
185.3.147.98	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
85.64.189.210	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
79.176.218.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.3.147.98	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
149.78.182.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.150.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.75	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
2.52.173.143	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
149.78.254.50	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.254.50	Block	3
46.19.85.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.100.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
141.101.249.231	Russian Federation	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/452-en/	Block	2
82.146.43.18	Russian Federation	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/452-en/	Block	2
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.3.147.98	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
2.54.39.5	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	2
89.139.163.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
37.26.148.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
185.3.147.252	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
46.121.194.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	2
109.65.155.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	2
79.178.184.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
141.101.249.104	Russian Federation	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/452-en/	Block	2
50.62.176.161	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
85.64.217.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/	Block	1
213.8.204.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/60041.pdf	Block	1
95.85.84.231	Russian Federation	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/452-en/	Block	1
79.180.205.69	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.146.224	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.46	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1766	Block	1
149.88.41.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.195.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.164.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.118.79.22	Russian Federation	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.64.25.7	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
80.87.200.35	Russian Federation	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/452-en/	Block	1
77.127.136.51	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
176.13.11.219	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1