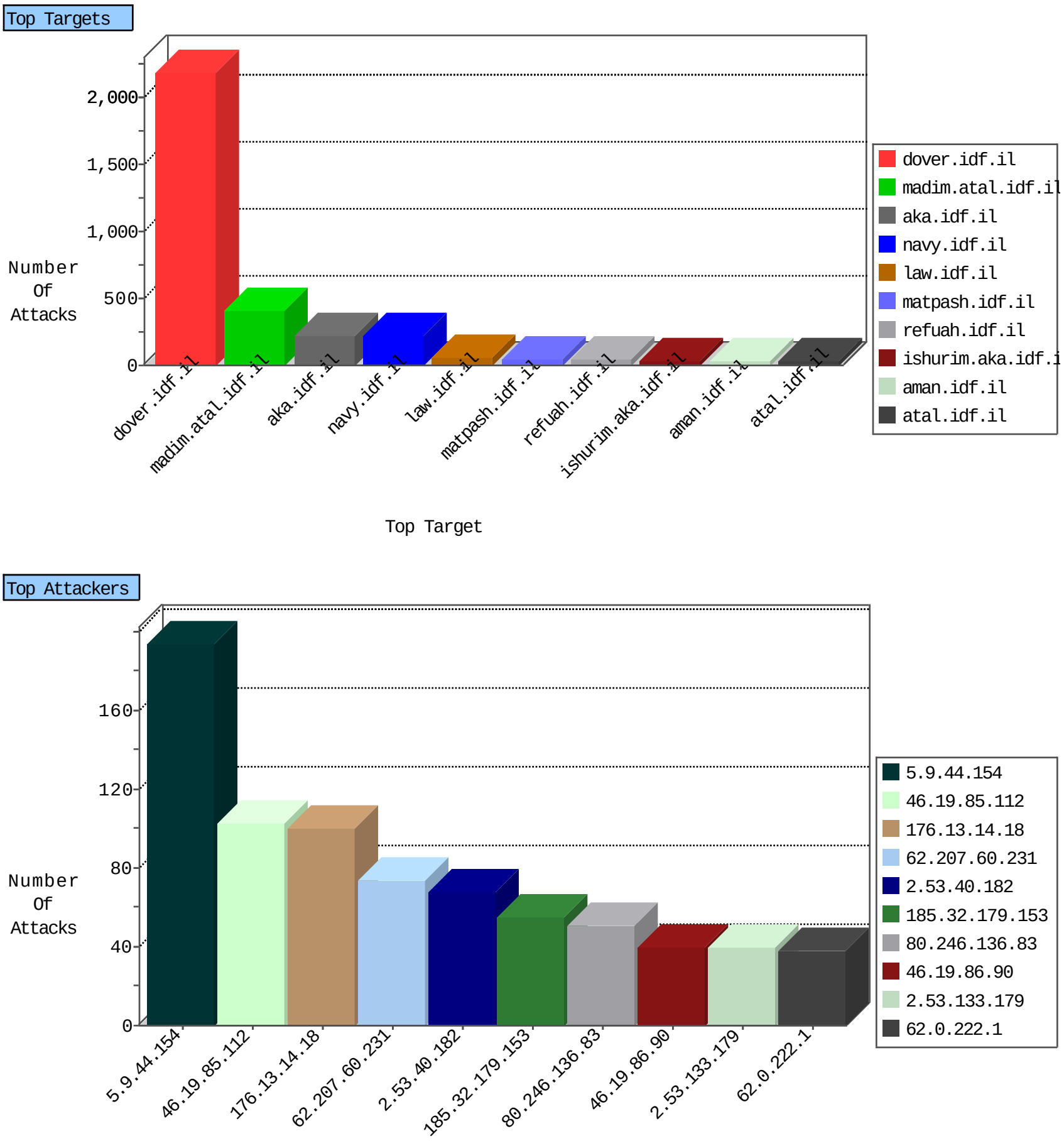
09-22-2016-11:04:04 to 09-22-2016-12:04:04

IDF Under Attack Daily Report



09-22-2016-11:04:04 to 09-22-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.137.204	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
2.53.133.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
176.13.226.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
176.13.13.111	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.67.104.183	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
109.253.223.73	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.253.230.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.53.188.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.188.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
109.253.215.219	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
10.0.0.10		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.253.147.29	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.66.81.51	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.210.174.227	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
80.246.136.83	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
173.208.150.114	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.193.253	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
192.114.105.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.85.209	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
176.13.14.18	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	2
109.253.210.153	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.179.107.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.204.224.237	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
142.54.174.86	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
204.12.220.84	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
62.0.34.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.32.179.191	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
94.188.162.30	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.65.4.192	Israel	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-22-2016-11:04:04 to 09-22-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.119.125.159	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-22-2016-11:04:04 to 09-22-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.125.159	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	28
211.149.244.79	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
192.115.29.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.231.57	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.115.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-22-2016-11:04:04 to 09-22-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	184
62.207.60.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
62.0.222.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
156.197.229.51	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
194.90.66.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
80.246.136.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
80.246.136.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
46.19.86.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
46.19.86.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
176.13.13.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
5.102.242.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
80.246.136.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.180.223.6	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
109.253.134.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
46.19.86.111	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
62.219.131.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.188.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.137.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.225.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.70.52.184	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
85.250.114.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
31.168.242.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.194.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.136	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.241.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.0.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.90	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
2.53.14.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.90	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
85.130.223.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.23.25	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.223.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
2.55.166.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.129.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.196.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
128.139.251.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
188.72.103.230	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8

09-22-2016-11:04:04 to 09-22-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
176.13.14.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
2.53.40.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
185.32.179.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
2.53.149.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
109.253.195.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
212.235.111.188	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
62.219.240.174	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.240.174	Block	5
2.53.50.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.206.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.130.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.23.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.240.114.149	Belgium	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	3
77.138.90.174	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.134.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.185	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
2.53.171.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.197.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.250.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.80	Israel	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
194.90.66.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.15.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.248.24.164	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.19.86.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.33	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
46.19.85.80	Israel	147.237.77.74	law.idf.il	Distributed Malformed URL	Block	2
109.67.10.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
195.160.242.40	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
180.76.15.11	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
213.57.226.66	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
141.226.162.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.113	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
194.78.217.148	Belgium	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Malformed URL [[.¥'œ#16°]]8#[[e]]ק¨`	Block	1
109.253.209.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1

09-22-2016-11:04:04 to 09-22-2016-12:04:04