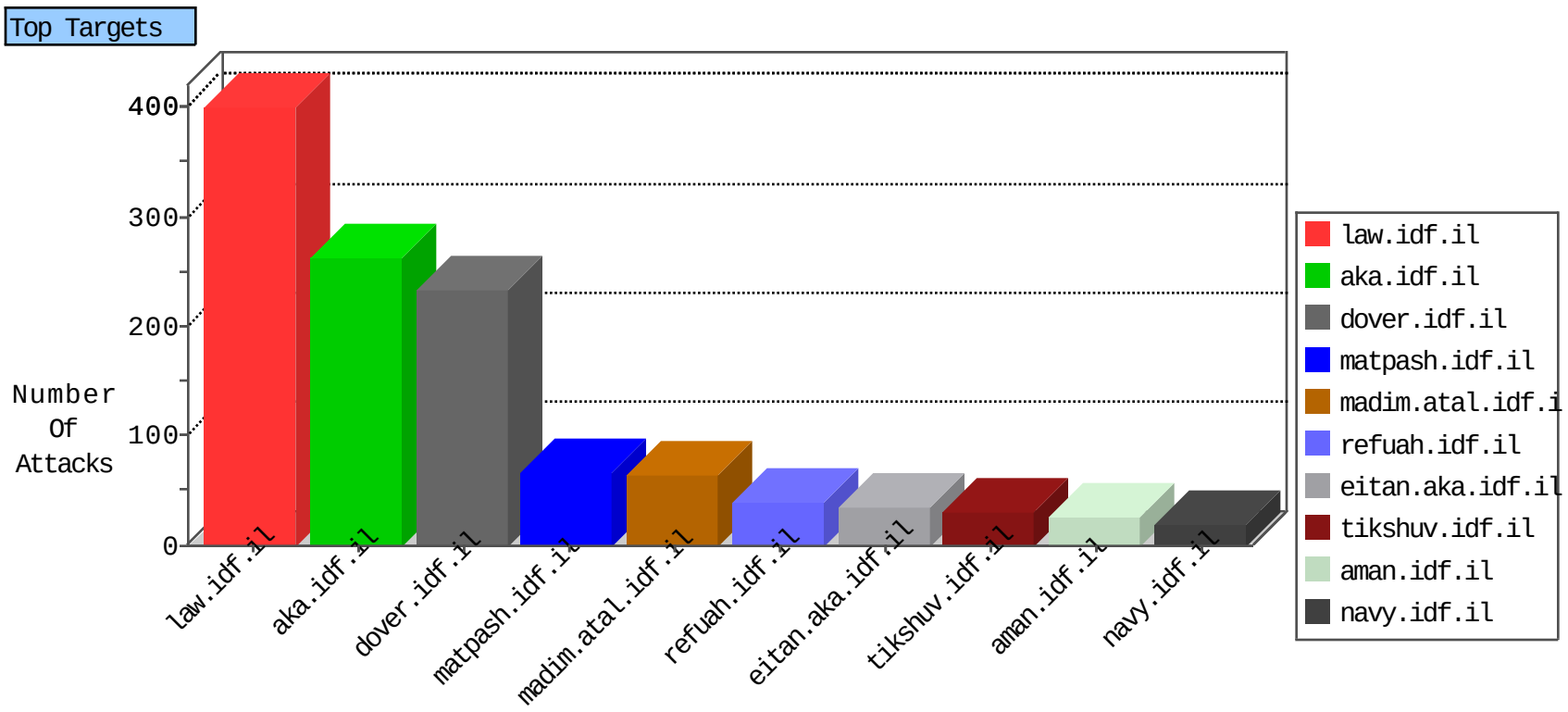
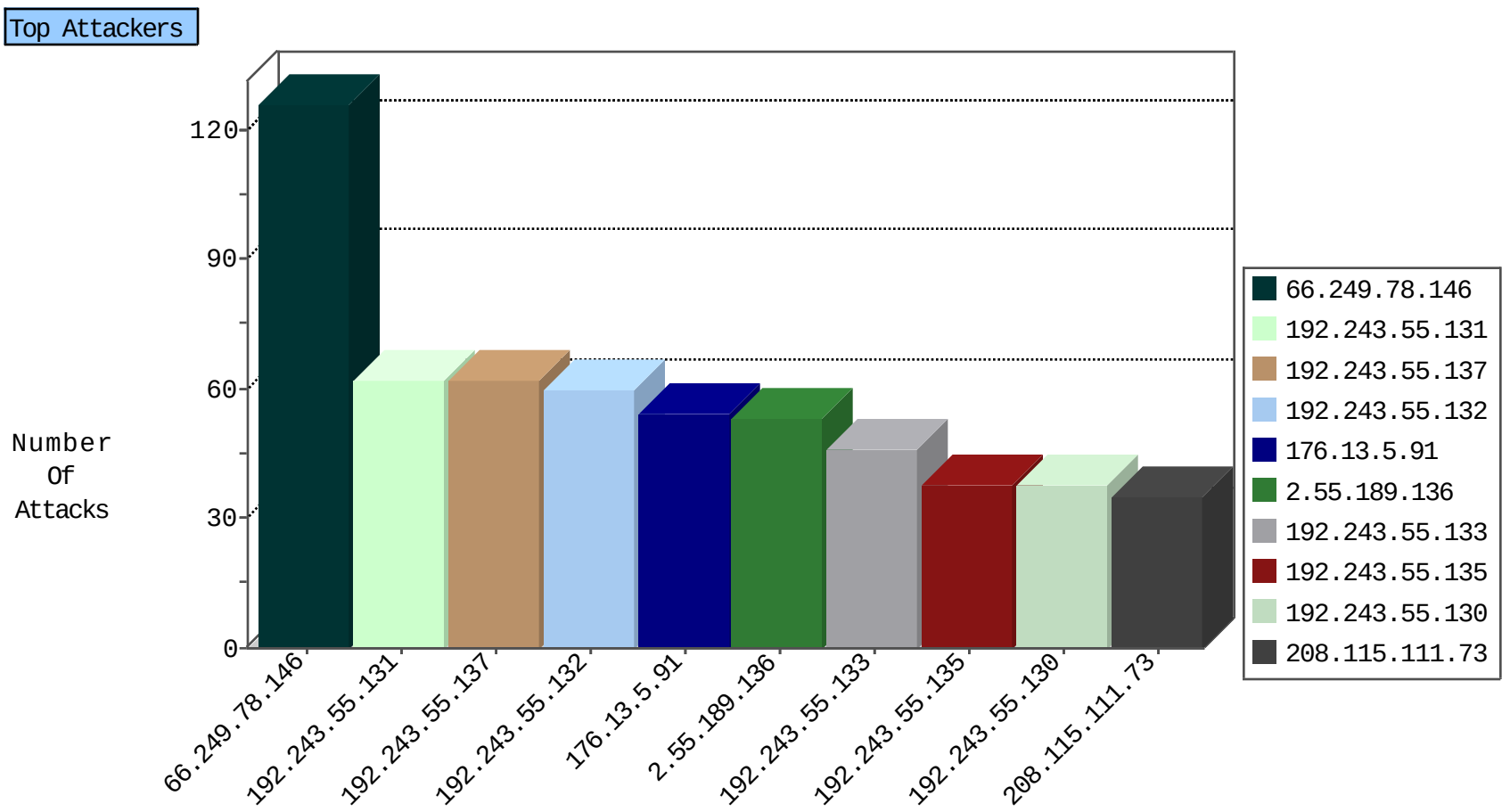
04-23-2016-17:04:03 to 04-23-2016-18:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-23-2016-17:04:03 to 04-23-2016-18:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.137	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2573
128.79.204.115	France	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2445
198.58.102.96	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2327
212.34.11.39	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	553
109.66.83.54	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
111.3.108.151	China	147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	1
192.243.55.133	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1

04-23-2016-17:04:03 to 04-23-2016-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-17:04:03 to 04-23-2016-18:04:03

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	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
187.160.84.208	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.59.33.61	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.99	147.237.76.198	Lithuania	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.147	Lithuania	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.30	Lithuania	himush.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.8.50	Lithuania	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.34	Lithuania	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
187.160.84.208	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.248.100.195	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.77.205	Lithuania	prisha.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
185.130.5.99	147.237.76.148	Lithuania	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.34	Lithuania	yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.72.167	Lithuania	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.35	Lithuania	akaws.idf.il	ET SCAN Potential SSH Scan	1
176.119.41.178	147.237.76.177	Poland	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.76.196	Latvia	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
189.219.80.202	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-23-2016-17:04:03 to 04-23-2016-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
77.125.84.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
2.55.189.136	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
148.163.73.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
64.216.107.11	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
109.65.8.229	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.148.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
109.65.125.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.213.219.229	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
2.55.189.136	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
37.26.148.227	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.213.219.229	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
141.0.15.157	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
84.94.114.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	8
109.186.63.53	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
66.102.7.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
46.121.144.142	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.144.142	Block	6
93.173.21.82	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
109.64.172.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.255.115	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
80.246.136.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
88.200.215.151	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1414-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	NULL Character in Method	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
104.251.82.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
188.227.36.36	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/ge	Block	1
157.55.39.216	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
40.77.167.12	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.186.63.53	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
88.200.215.151	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1393-en/dover.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
1.65.167.196	Hong Kong	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
107.150.46.38	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
188.227.36.36	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
81.95.96.160	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
159.253.0.17	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
109.253.133.149	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
88.200.215.151	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1393-en/dover.aspx	Block	1
178.27.135.54	Germany	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
72.29.127.13	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
131.253.25.252	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	1
1.65.167.196	Hong Kong	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
212.227.119.162	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
82.166.244.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/faq.aspx	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
123.231.125.140	Sri Lanka	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
46.213.200.208	Syrian Arab Republic	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
178.27.135.54	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
77.125.84.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
149.50.24.197	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/lomdim/pniot/	None	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
109.65.8.229	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opevent/opevent.in.aspx	Block	1
84.111.188.178	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method	Block	1