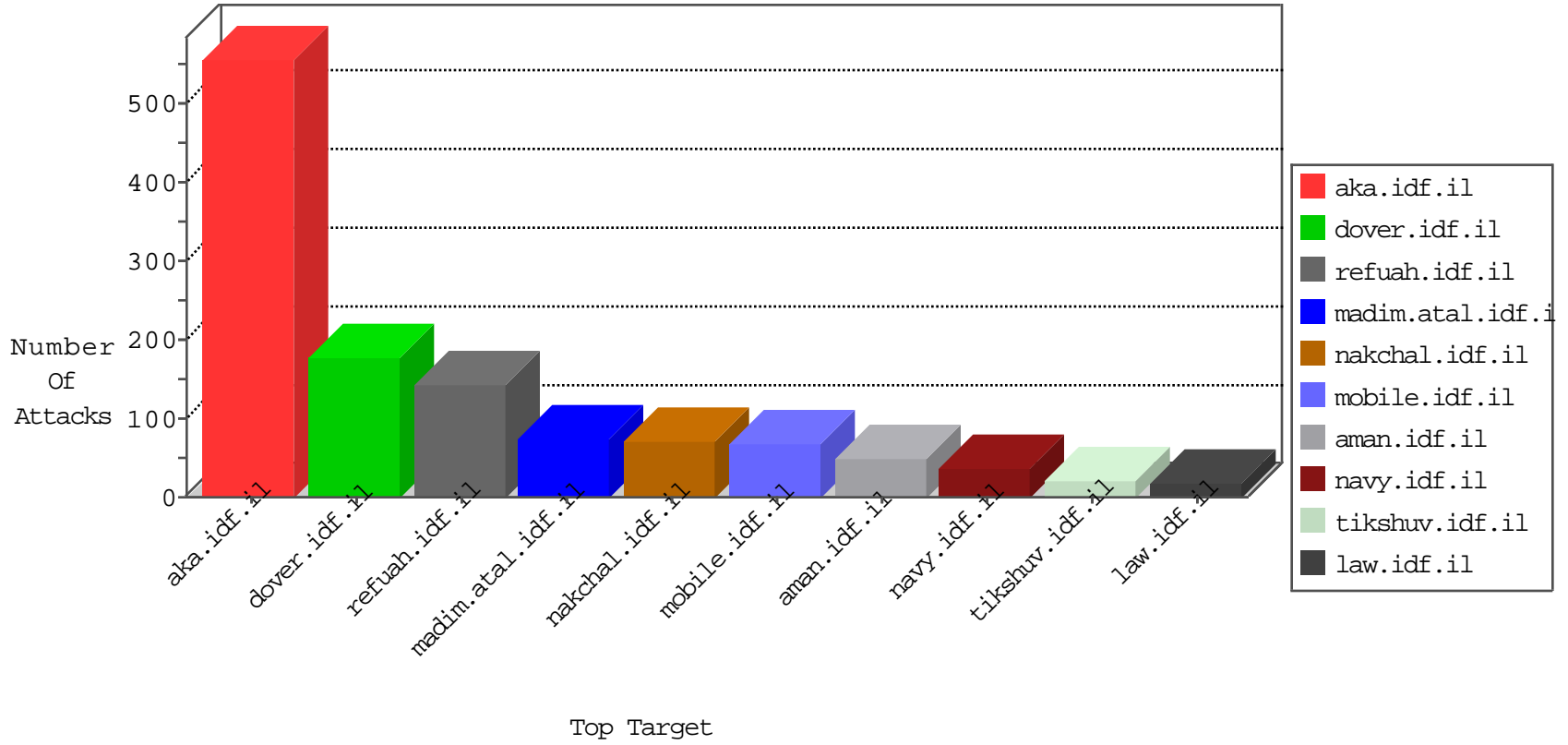


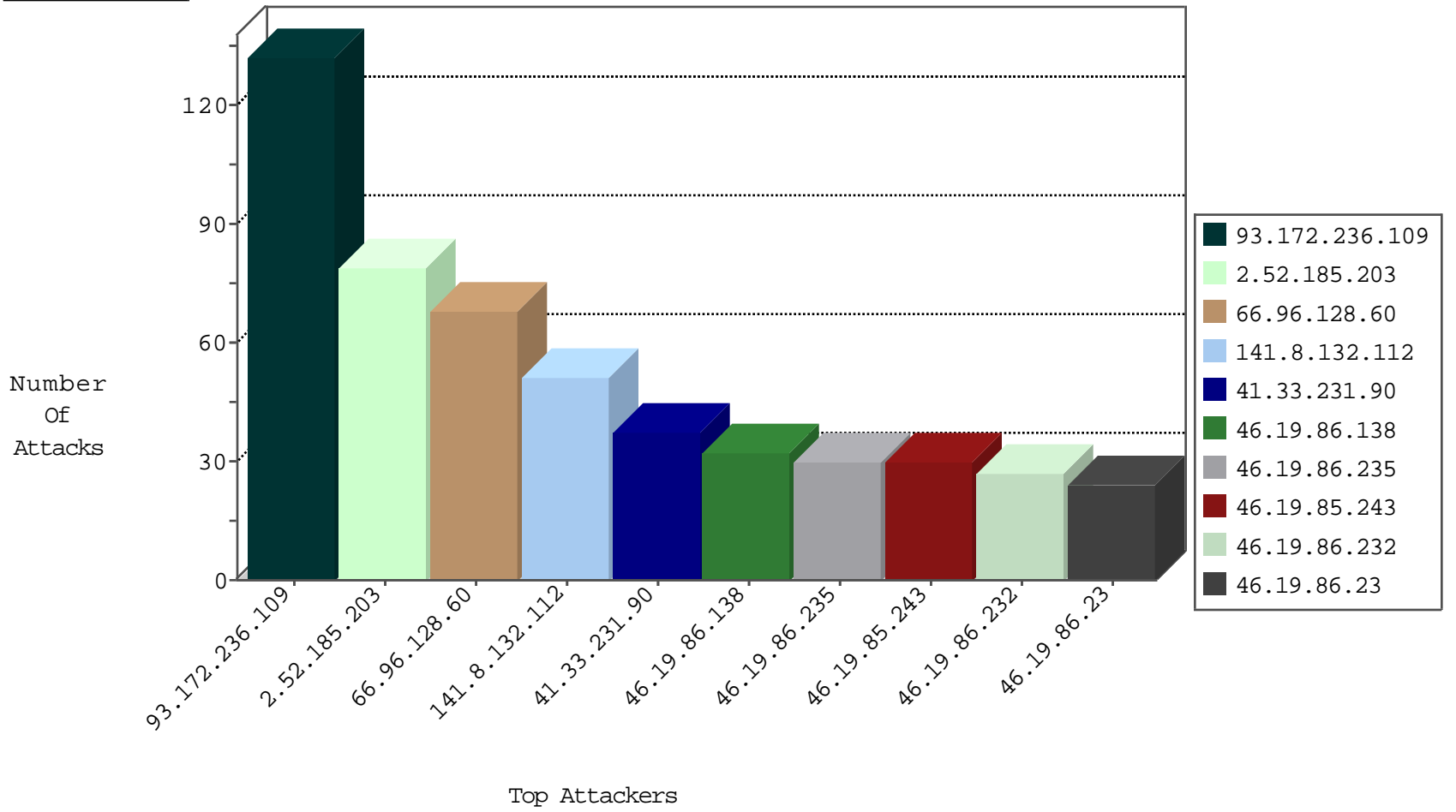
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.248.160.138	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
157.55.39.32	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
117.190.96.206	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.124	Switzerland	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
117.190.96.206	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
117.190.96.206	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.96.128.60	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
66.96.128.60	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.96.128.60	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
70.89.127.77	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
151.80.41.169	Italy	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.239	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.96.128.60	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	48
70.89.127.77	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.81.196	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
185.53.91.144	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.225.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.145.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
193.105.134.220	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.53.91.144	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
115.28.247.220	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.197	Ukraine	e.himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.82.79.104	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
71.6.165.200	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 3072	1
189.219.185.91	147.237.0.16	Mexico	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.236.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	131
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
46.19.86.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.52.185.203	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
5.22.135.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
213.57.60.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.52.185.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
2.52.185.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
2.52.185.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.81.21.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.244.74	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.222.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.185.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
89.42.96.182	Romania	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
89.42.96.182	Romania	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.86.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.183.161.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.127.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.135.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.145.142	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
87.68.151.243	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.249.81.199	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
82.80.173.54	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.210.187.105	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.125.90.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
66.96.128.60	United States	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
66.249.81.202	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
84.109.9.72	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
77.125.90.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.24.146.74	Germany	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.233.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.94.174.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
212.235.21.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.53	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
176.13.13.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
77.127.29.174	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.29.174	Block	11
79.180.182.200	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.182.200	Block	7
77.127.29.174	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
79.183.224.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.180.182.200	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
85.64.233.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.38.119	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.38.119	Block	3
109.65.2.186	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.65.2.186	Block	3
93.173.36.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.184.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.38.119	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
185.89.217.230		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.149.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.6.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.90.28.94	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1293-he/refuah.aspx	Block	2
109.253.193.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
213.57.60.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
79.179.31.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
109.65.2.186	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
37.26.149.199	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
197.33.182.2	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
157.55.39.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
91.196.50.33	Poland	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
31.168.246.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
217.132.227.220	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
79.179.201.192	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
185.89.217.234		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
85.65.131.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$91 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
198.58.102.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
79.180.182.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
93.172.236.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.94.38.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
31.184.238.132	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.184.238.132	Block	1
79.179.201.192	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.201.192	Block	1
185.89.217.235		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/××ž×××××	Block	1
87.69.125.118	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
37.46.38.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
213.8.204.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
62.90.28.94	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1476-he/refuah.aspx	Block	1
84.94.49.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
31.184.238.132	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
190.83.209.133	Trinidad and Tobago	147.237.77.216	dover.idf.il	PHP Attempt	Block	1