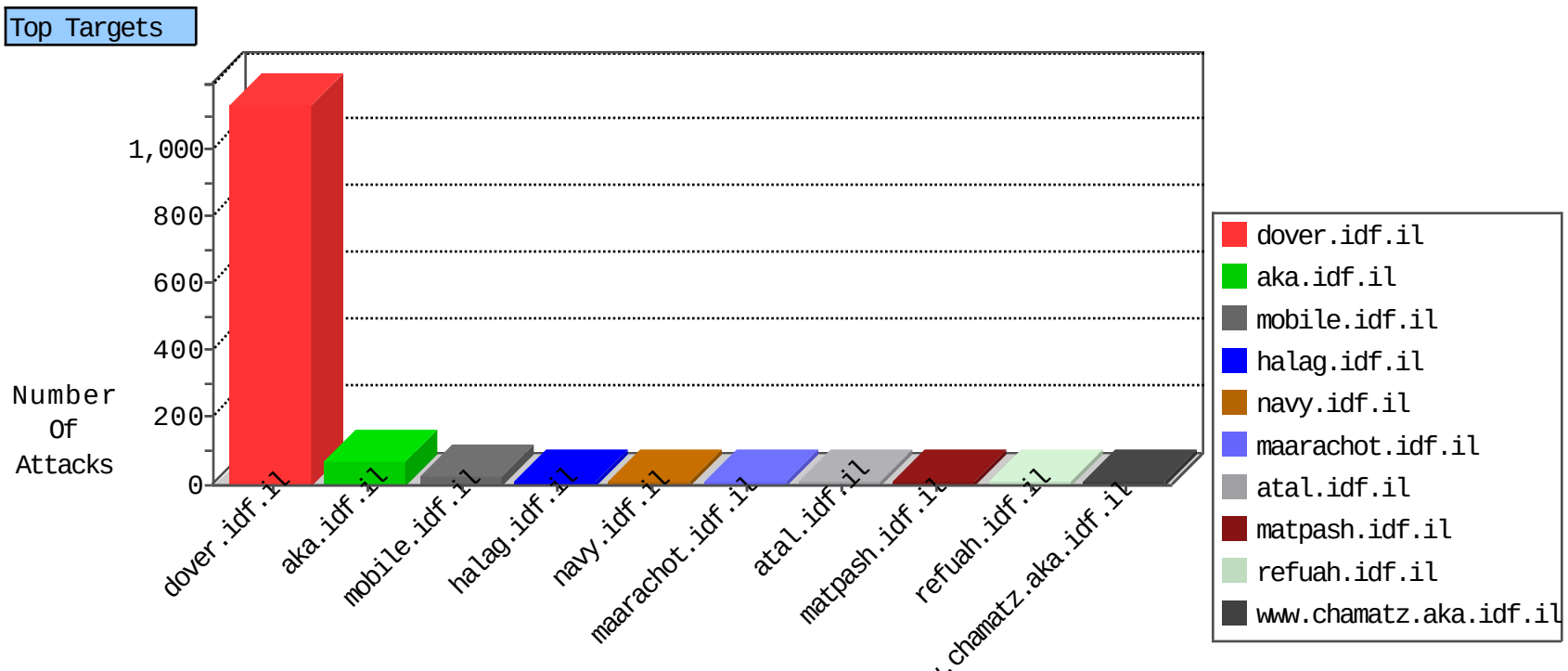
01-01-2016-02:04:03 to 01-01-2016-03:04:03

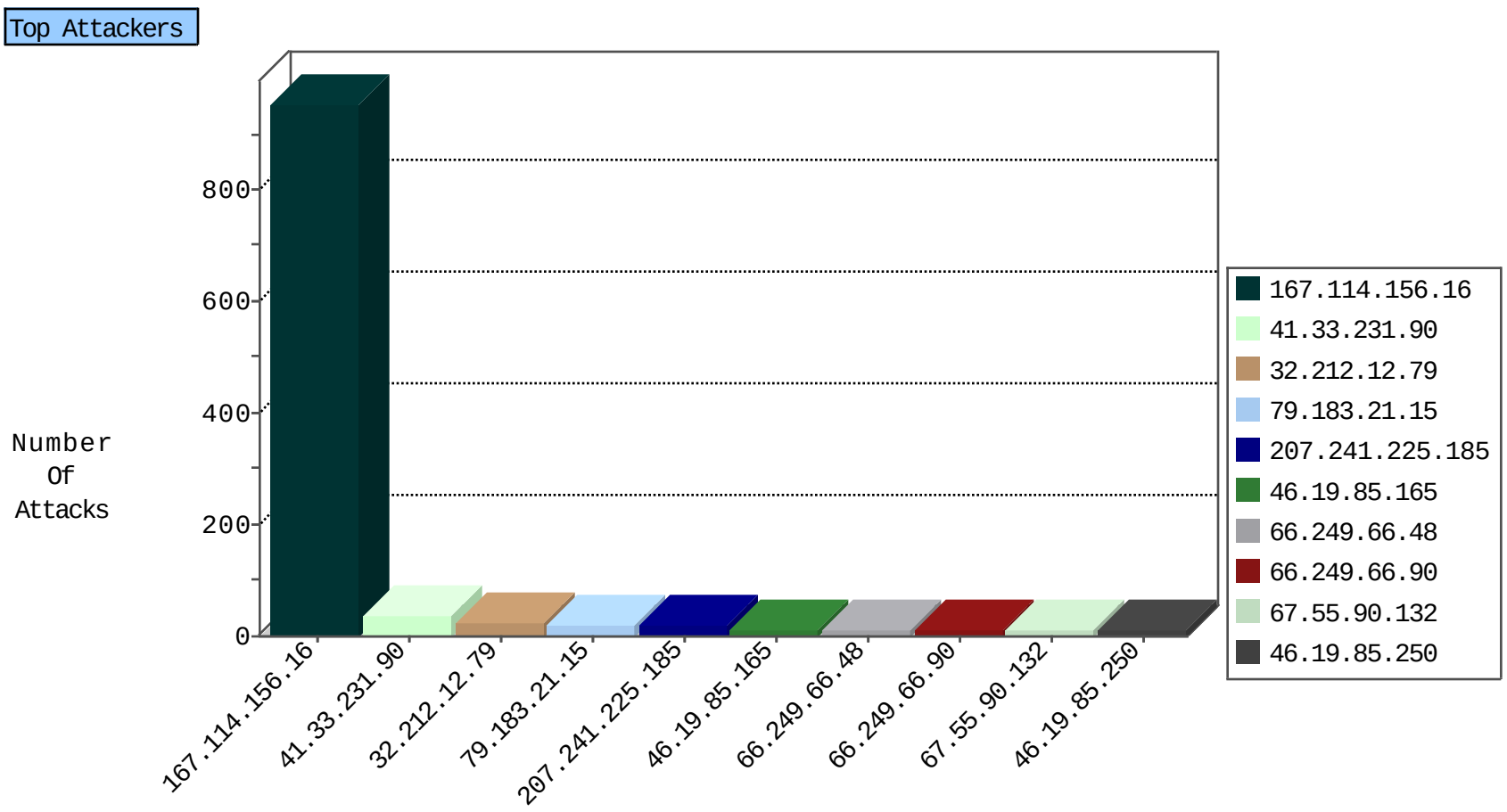
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-01-2016-02:04:03 to 01-01-2016-03:04:03

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	3100
66.249.78.62	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	874
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
106.75.199.186	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

01-01-2016-02:04:03 to 01-01-2016-03:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-01-2016-02:04:03 to 01-01-2016-03:04:03

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	4
79.138.70.153	147.237.0.35	Sweden	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
190.249.184.162	147.237.76.200	Colombia	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
118.68.179.139	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
113.59.33.61	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.177	Ukraine	ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
82.211.60.156	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
79.138.70.153	147.237.76.177	Sweden	ncore.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.76.30	Sweden	himush.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
168.169.16.15	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
113.59.33.61	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.114	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
82.211.60.156	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
82.211.60.156	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
79.138.70.153	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN Potential SSH Scan	1

01-01-2016-02:04:03 to 01-01-2016-03:04:03

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	35
79.183.21.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
207.241.225.185	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.66.48	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
32.212.12.79	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
32.212.12.79	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.221.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.87.71	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	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	6
199.30.25.24	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.212.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
67.55.90.132	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.175.26.46	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
67.55.90.132	United States	147.237.77.226	www.chamatz.aka.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
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.195.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.116.54.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.202.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.130.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.89.217.225		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
109.64.23.114	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
5.175.26.46	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
66.249.79.133	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
132.66.237.115	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.111.55.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
101.198.159.31	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
190.162.230.204	Chile	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
87.69.197.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
67.55.90.132	United States	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.89.217.226		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
32.212.12.79	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.64.97.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	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
79.183.21.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.47.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.186.59.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.188.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.121.134.54	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/dover.aspx'	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
64.86.221.101	Costa Rica	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
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	1
84.111.55.83	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
190.210.186.137	Argentina	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
109.253.195.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.175.26.46	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
88.235.240.122	Turkey	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
213.251.182.115	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
77.126.144.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.66.23	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1153-en/hamaz.aspx	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
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	1
114.97.58.24	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1026-he/shared/usercontrols/headerupper/	Block	1
88.235.240.122	Turkey	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
173.252.120.120	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.214.11.209	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
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	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
136.243.36.96	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/undefined	Block	1
37.60.47.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.224.140.78	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.52.171.22	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
207.46.13.121	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
68.180.230.160	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.227.71.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.80.168.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
187.109.10.111	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
5.175.26.46	Germany	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 5.175.26.46	Block	1