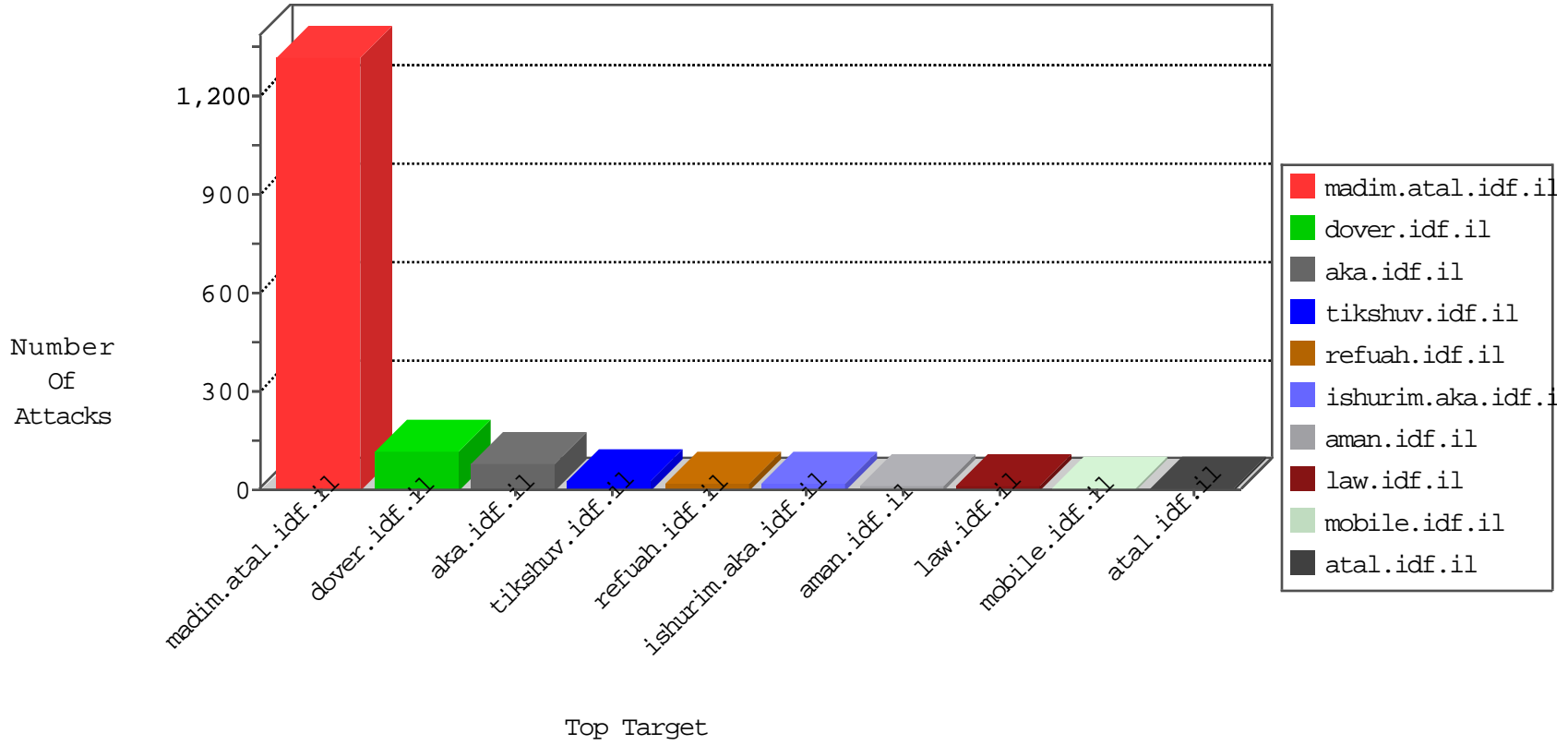


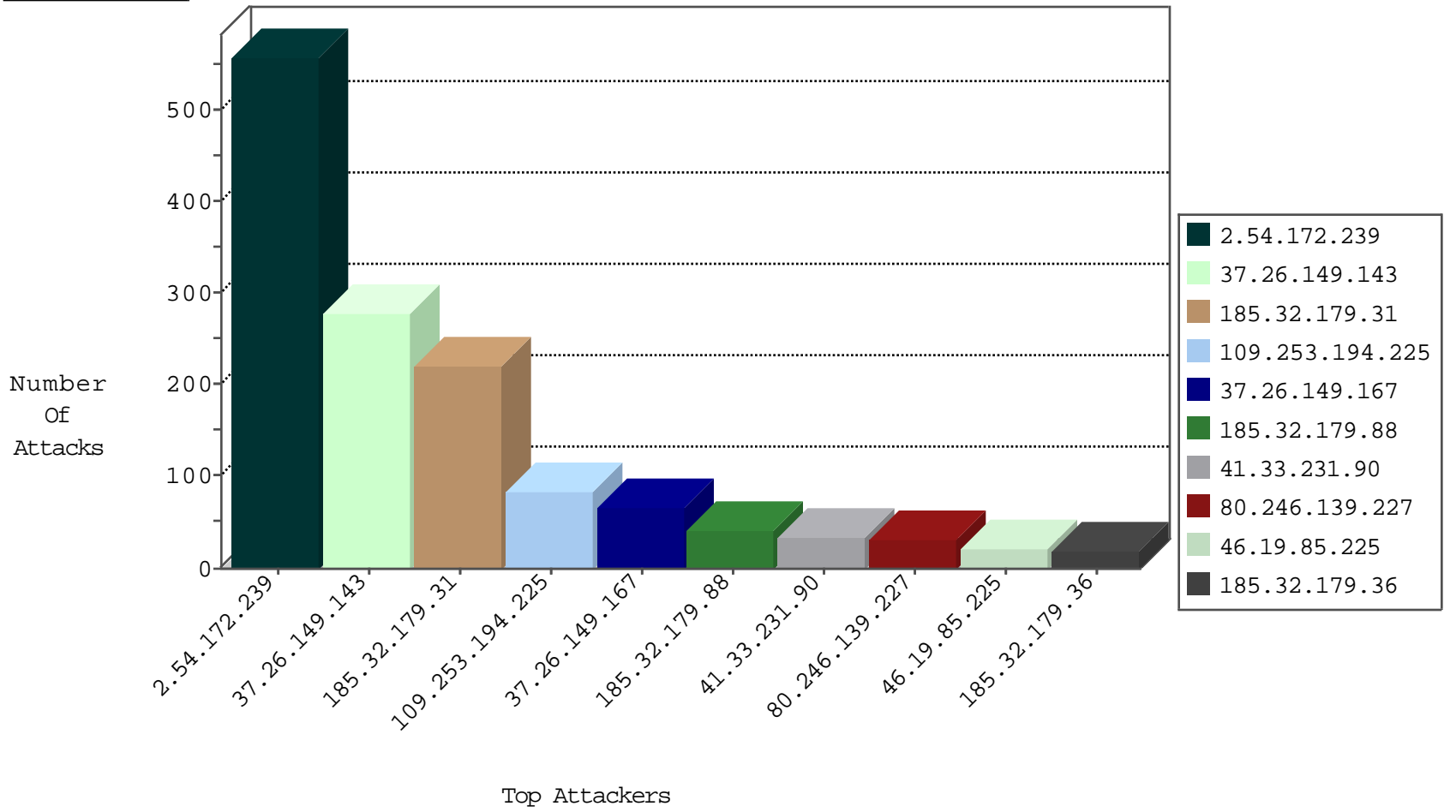
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.231.36	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
112.74.135.36	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	2
185.130.5.201		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
46.32.234.20	United Kingdom	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

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	3
185.32.179.31	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
122.160.9.51	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.189.26.18	147.237.76.44	Austria	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.207.60.30	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.149.252.58	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
40.115.57.147	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
177.238.45.181	147.237.72.217	Mexico	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.53.133.242	147.237.76.42	Thailand	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.207.60.30	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.113	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.149.252.58	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
46.45.137.67	147.237.77.216	Turkey	dover.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.57.147	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.0.33	United States	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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
46.19.86.85	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.225	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.162.195	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.29.233.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.225	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
79.179.11.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.153.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.179.14.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.192	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.81.76.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.6	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.86.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.3	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.9.148.10	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.102.254.157	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.179.9.7	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.102.254.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.24.182	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.254.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.130.239.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.139.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
86.106.17.166	Romania	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
37.26.146.139	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.49	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.179.9.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
176.13.22.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.88	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.139.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.172.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	326
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	162
2.54.172.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	129
185.32.179.31	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.31	Block	125
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
2.54.172.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
185.32.179.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
109.253.194.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
37.26.149.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
185.32.179.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
37.26.149.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
80.246.139.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.121.78.175	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.78.175	Block	15
80.246.139.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
185.32.179.88	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 185.32.179.88	Block	11
185.32.179.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
185.32.179.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	4
109.253.130.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.219.236.222	Hungary	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	3
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	3
37.26.149.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.223.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
202.78.237.210	India	147.237.77.216	doover.idf.il	PHP Attempt	Block	2
157.55.39.211	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
202.78.237.210	India	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
91.219.236.222	Hungary	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	2
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	2
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
185.32.179.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
149.78.215.133	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
2.52.158.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
216.218.206.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
66.249.78.159	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
46.117.78.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.250.226.92		147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=0cpx8rsylit6fkjxnpdb9cgol4-	Block	1
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
66.249.66.113	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
89.178.175.233	Russian Federation	147.237.77.216	doover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.54.55.92	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
216.245.218.190	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
46.121.78.175	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
66.249.66.117	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1