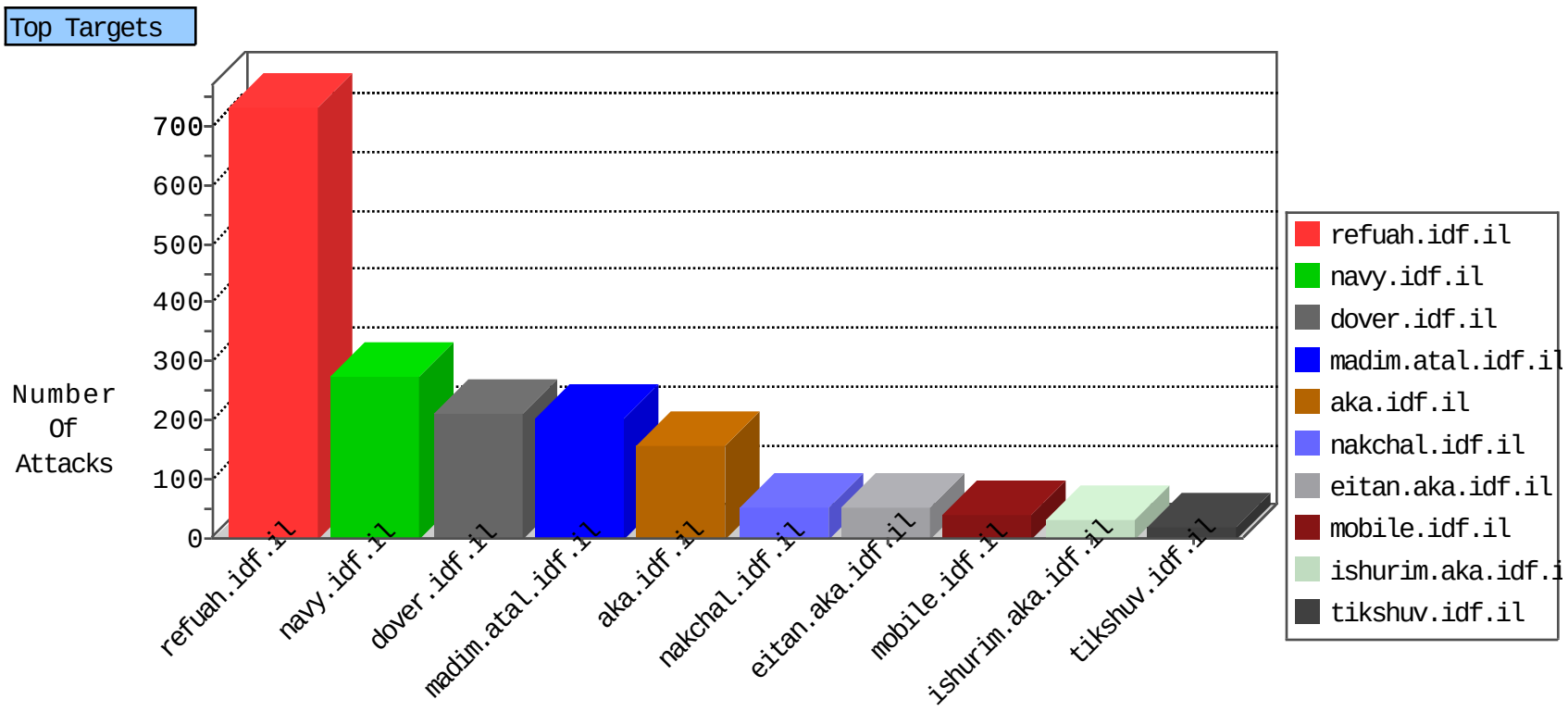
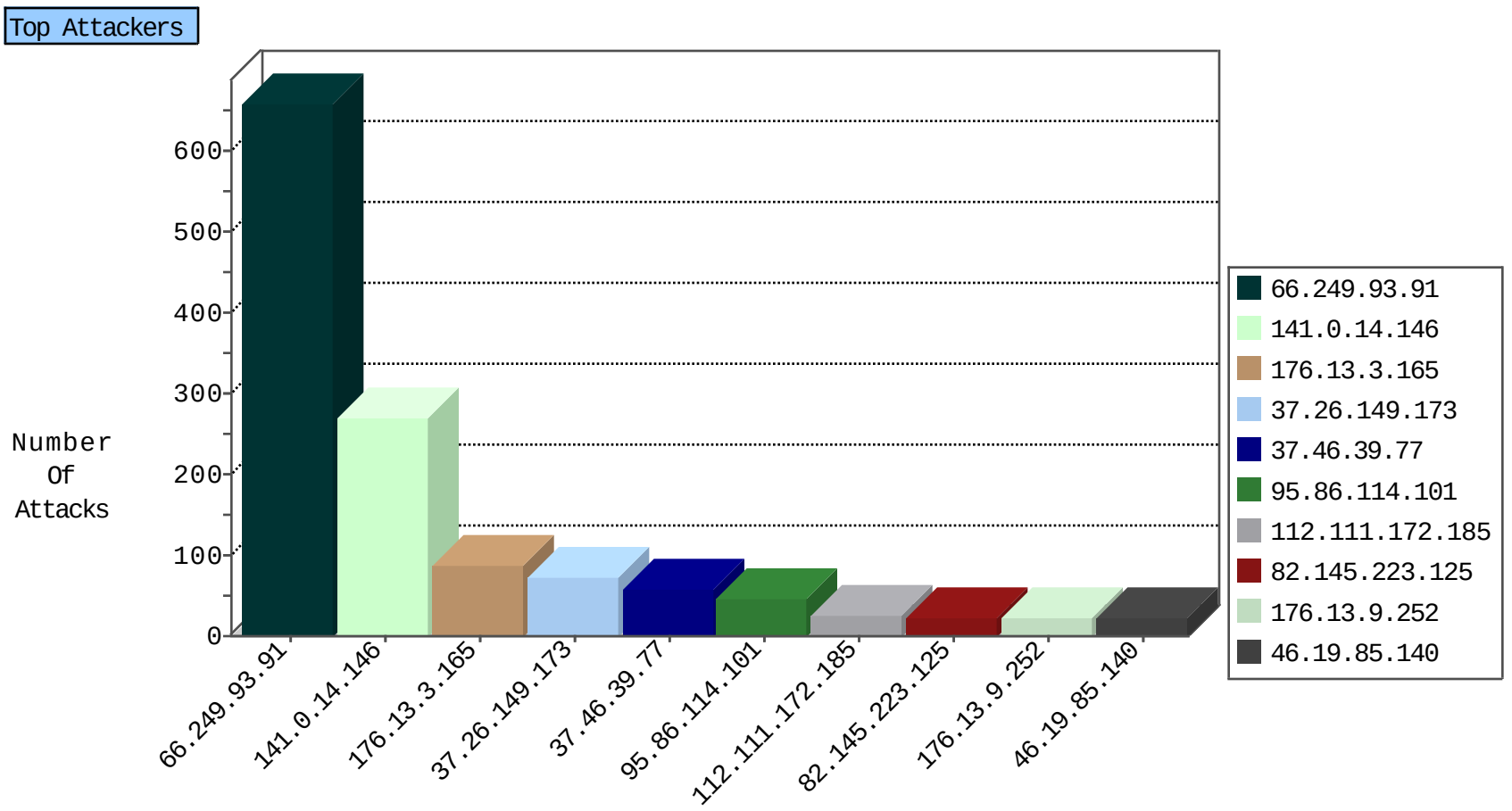
09-21-2016-18:04:09 to 09-21-2016-19:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-18:04:09 to 09-21-2016-19:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.28.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
141.0.14.146	Europe	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
173.208.150.117	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
141.0.14.146	Europe	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
69.30.193.254	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
198.204.224.235	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
204.12.220.86	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
52.53.222.9	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
142.54.174.84	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1

09-21-2016-18:04:09 to 09-21-2016-19:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-21-2016-18:04:09 to 09-21-2016-19:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.91	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	659
91.121.132.153	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
46.19.86.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.124.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
37.142.10.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.201.80	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
180.213.5.205	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
180.213.5.205	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
110.5.109.236	147.237.77.61	Indonesia	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.151	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
64.137.168.128	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.12.86.235	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.151	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.84.213.146	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
218.27.1.174	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.151	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
41.160.222.18	147.237.76.42	South Africa	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
192.223.80.103	147.237.77.179	Bolivia	e.mazi.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.50	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
180.213.5.205	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.129.15	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.119.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
94.102.56.151	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.12.86.235	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.56.151	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.84.213.146	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.56.151	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-21-2016-18:04:09 to 09-21-2016-19:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.14.146	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	264
37.46.39.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
95.86.114.101	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
82.145.223.125	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	21
46.19.85.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.13.9.252	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
207.241.226.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
46.19.86.197	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
2.55.144.138	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
82.81.161.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.202	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.202	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.50	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.245.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.186.148.251	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.107	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
77.127.30.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.107	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.6.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.9.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.32.179.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
94.79.67.17	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.139.142.54	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.154.81.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.3.147.207	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
185.32.179.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
185.3.147.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
101.109.185.208	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.181.37.30	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	4
141.0.14.40	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.226	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.185.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.46.39.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.55.144.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.133.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
207.232.46.209	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.55.13.40	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

09-21-2016-18:04:09 to 09-21-2016-19:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.3.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
112.111.172.185	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.111.172.185	Block	17
109.253.196.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
112.111.172.185	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
46.19.86.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
5.29.7.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
176.13.245.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.8.204.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.227.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.50	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
79.176.3.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
46.19.85.9	Israel	147.237.76.31	nakchal.idf.il	Multiple Malformed URL from 46.19.85.9	Block	2
5.29.182.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.9	Israel	147.237.76.31	nakchal.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.9	Block	2
31.13.113.69	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/5015.jpgthis	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.79.60	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
176.13.241.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.38.47	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.9	Israel	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
2.53.2.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
194.242.163.237	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/lobby	Block	1
66.249.93.91	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/favicon.ico	Block	1
172.56.35.146	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.102.9.154	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.19.85.9	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method 4qk3k55 in URL	Block	1
87.69.225.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.210.187.116	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
66.249.93.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
46.19.86.50	Israel	147.237.77.234	halag.idf.il	Unknown HTTP Request Method oFriend/SendToFriend.aspx?&l=he&f=1130 in URL	Block	1
84.109.240.160	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.9	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version	Block	1
2.53.60.161	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
198.20.164.234	United States	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
66.249.64.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	1
101.109.185.208	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.13.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.26.146.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
66.249.93.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
112.111.172.185	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
84.111.109.138	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
46.19.85.9	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1

09-21-2016-18:04:09 to 09-21-2016-19:04:09