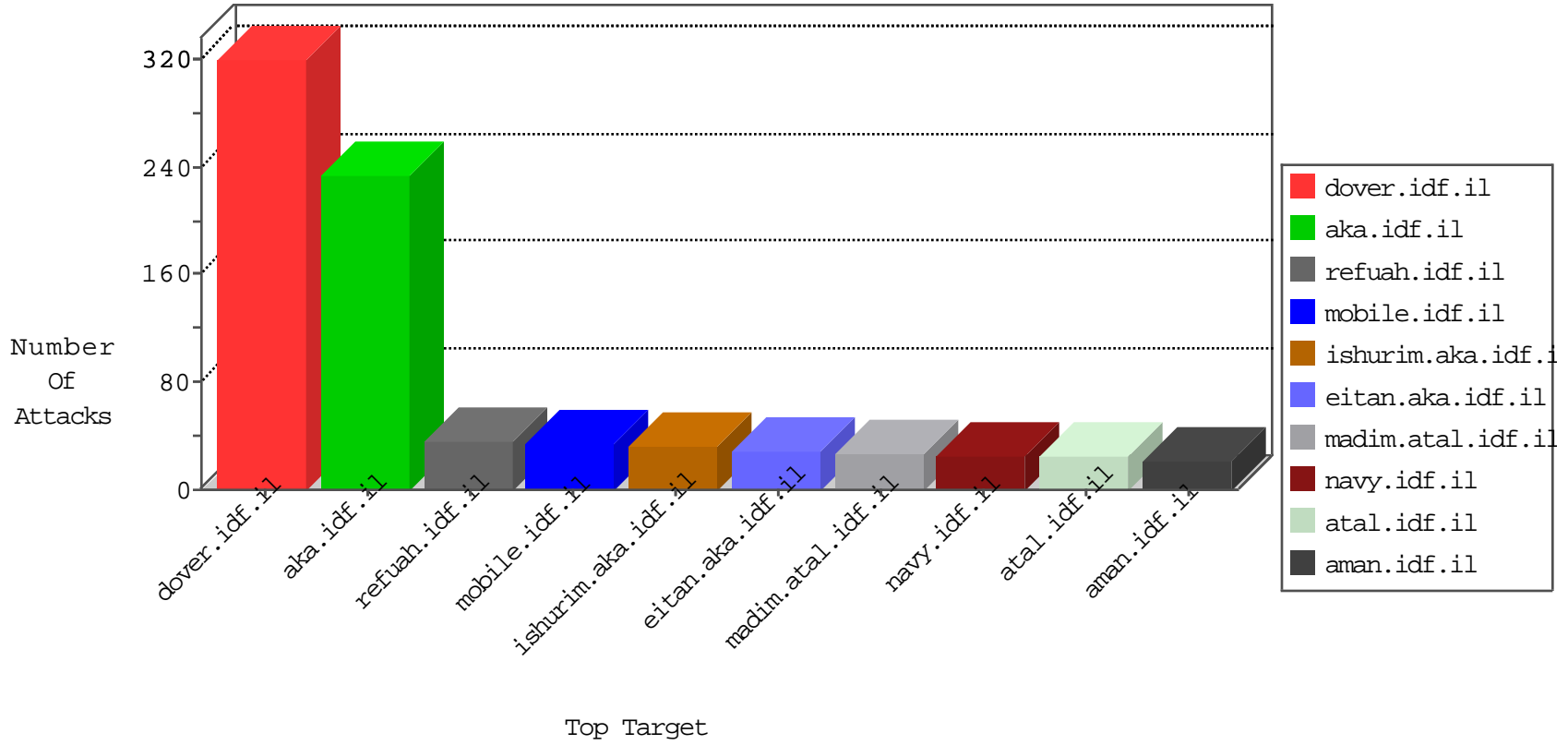


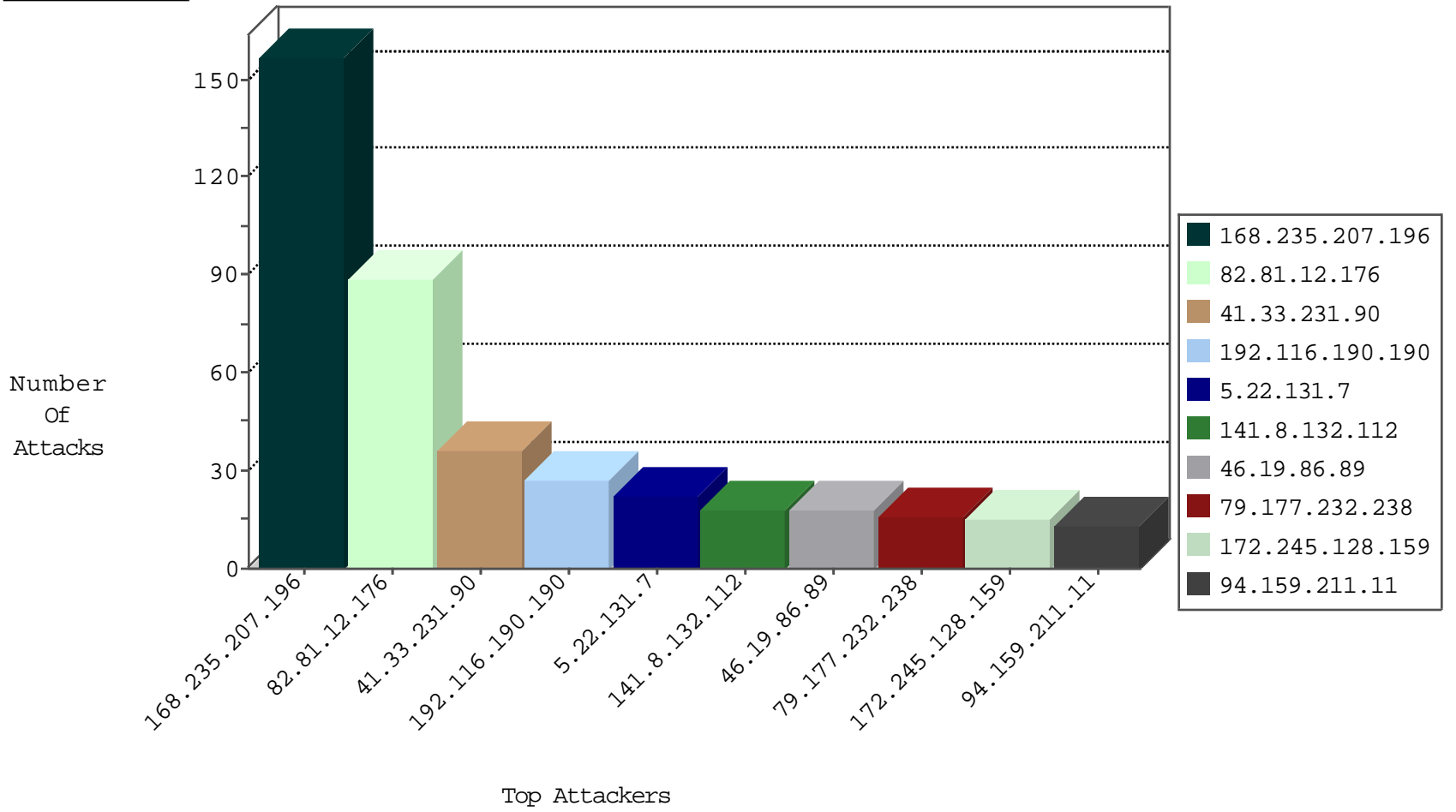
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	89
79.183.151.252	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
168.235.207.196	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
157.55.39.114	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
142.54.169.163	United States	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
142.54.169.166	United States	147.237.0.17	m.ny-kosher-kravi.idf.il	block-sp-trafl	forward	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.120.209.148	United States	147.237.77.216	dover.idf.il	C101: HTTP Hacked in the URL	Block	4
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.150	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

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
74.120.209.148	147.237.77.216	United States	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	4
172.245.128.159	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.8.27		e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
115.231.9.148	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.158.140	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
66.240.213.93	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
198.154.60.27	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.207.196	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	153
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
192.116.190.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.89	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
79.177.232.238	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
5.22.131.7	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.155	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
5.66.139.75	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.200.179	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.250	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
69.113.151.67	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
79.182.128.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.116.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.105.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.85.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.190.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.211.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.159.211.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
87.68.158.140	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.172.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
89.177.143.2	Czech Republic	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.75.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.9.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.152.55	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
5.102.254.148	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.59.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.158.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.7	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.108.27.254	Israel	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.179.55.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.254.8.139	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.176.33.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.118.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.146.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.128.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-29-2016-22:04:02 to 01-29-2016-23:04:02

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.104.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.240	Israel	147.237.72.156	anan.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
172.245.128.159	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	4
149.88.85.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.196.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.47.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
172.245.128.159	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 172.245.128.159	Block	3
2.52.144.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
194.105.27.162	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
89.138.23.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
172.245.128.159	United States	147.237.76.86	navy.idf.il	Multiple signatures from 172.245.128.159	Block	2
185.120.126.59		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.163.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.105.27.162	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
93.173.14.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.85.161	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.88.85.161	Block	2
149.88.85.161	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
109.253.129.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
188.161.44.171	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
176.13.12.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.208	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
149.78.81.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
2.54.129.237	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.132.67.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.13.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.27.254	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
157.55.39.163	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp/docid in www.aka.idf.il/giyus/general/	None	1
37.77.54.245	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
109.253.200.179	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.177.170.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
51.254.141.254	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.22.131.7	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
158.69.208.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
41.254.8.139	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 41.254.8.139	Block	1
112.215.124.92	Indonesia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
2.52.172.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.232.238	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
65.208.151.114	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
109.65.36.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.210.188.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.138.1.218	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
84.110.32.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
172.245.128.159	United States	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
69.113.151.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
41.254.8.139	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1