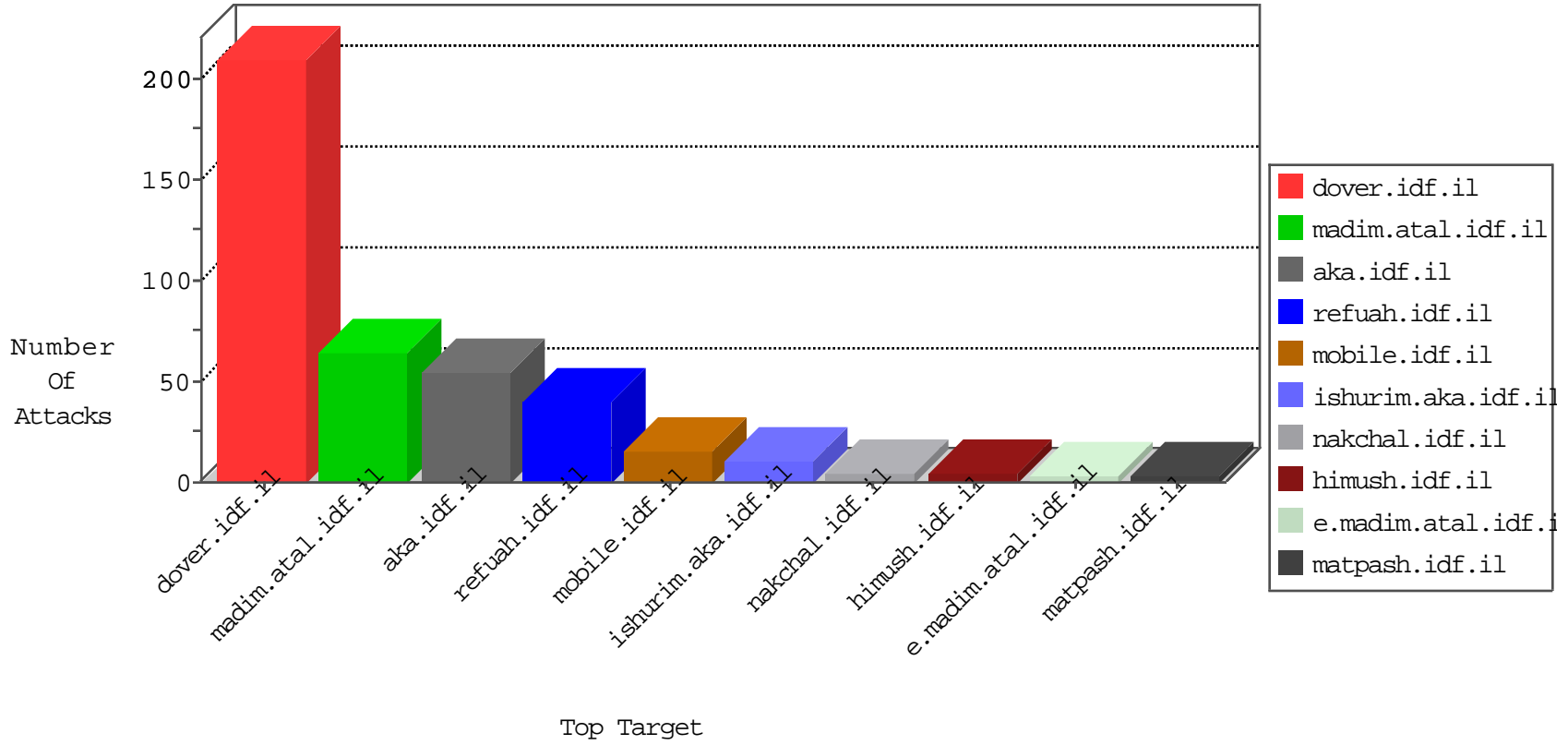


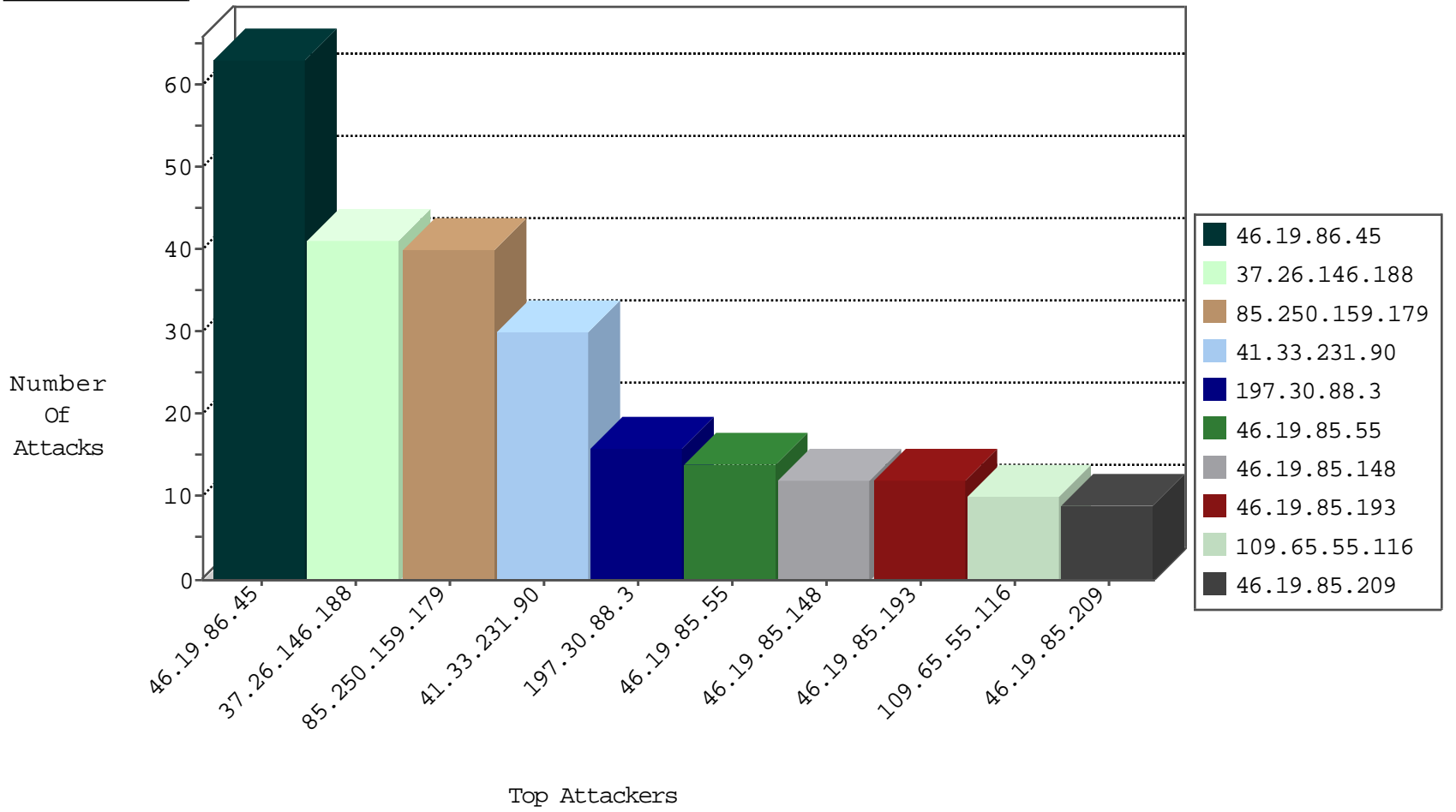
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.67.38.74	United States	147.237.76.39	mobile.meitav.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	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	4
66.249.78.67	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.15	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
94.76.3.229	147.237.76.39	Bahrain	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
94.76.3.229	147.237.76.31	Bahrain	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.201	Ukraine	e.atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
172.98.200.238	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
117.21.248.87	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.76.14.46	147.237.76.39	Bahrain	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.10.145	147.237.0.33	Bahrain	idf.il	ET SCAN NMAP -sS window 1024	1
94.76.3.229	147.237.76.38	Bahrain	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.3.229	147.237.76.30	Bahrain	himush.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
82.145.33.11	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -f -sS	1
117.21.248.87	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
94.76.14.46	147.237.76.44	Bahrain	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.76.14.46	147.237.0.16	Bahrain	my-kosher-kravi.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
85.250.159.179	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
37.26.146.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.209	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.146.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.146.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.26.146.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.146.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
37.26.146.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.140.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.159.179.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	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
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.116.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.55.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
197.30.88.3	Tunisia	147.237.77.216	dover.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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.133.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.128.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.213.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
197.30.88.3	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.221.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.229	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.30.88.3	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
187.189.195.40	Mexico	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
66.147.244.216	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
176.13.10.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
109.65.55.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
197.30.88.3	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
149.78.116.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.65.55.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
197.30.88.3	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
61.135.190.197	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
109.65.55.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
197.30.88.3	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.210.196.97	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
204.79.180.185	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
5.29.231.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
17.138.57.216	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/apple-app-site-association	Block	2
207.46.13.10	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.10	Block	2
17.138.59.24	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/apple-app-site-association	Block	2
17.138.59.213	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	2
149.78.116.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.97.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl38\$ctl01\$ctl03\$cbQuestio n\$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
194.63.133.5	Poland	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	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
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;w in www.aka.idf.il/main/giyus/captcha.ashx	None	1
31.44.138.242	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
157.55.39.141	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
83.83.196.198	Netherlands	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$ImageButton1.y in www.idf.il/1397-en/dover.aspx	Block	1
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.163.234.9	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cgi-bin/v.il	Block	1
37.26.146.188	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
158.69.225.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
85.250.159.179	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
17.138.59.24	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
109.186.8.24	Israel	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 112 cookies	Block	1
74.208.45.22	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
40.77.167.76	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×³×Ÿ Å¿Å¿×³×ŸÅ¿Å¿×³×ŸÅ¿Å¿×³×ŸÅ¿Å¿×³×ŸÅ¿Å¿	Block	1
158.130.0.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
95.86.96.214	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/5/2875.pdf&sa=u&ved=0ahukewjtoa w6jsvkahvc8rqkhdjgcbqqf1ggnmai&usg=afqjcnh5gwwvyljpiba_pbmahp n4khja	Block	1
61.135.190.72	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	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
112.142.129.127	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.208.45.22	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main3/giyus/general.aspx	Block	1
2.54.148.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.63.133.5	Poland	147.237.76.200	eitan.aka.idf.il	PHP Attempt	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
61.135.190.200	China	147.237.0.17	m.my-kosher-kravi .idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
213.57.229.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$emailUpdate\$rpEmailSubjects List\$ct101\$cbEmailSubject in www.aka.idf.il/main/giyus/faq.aspx	None	1