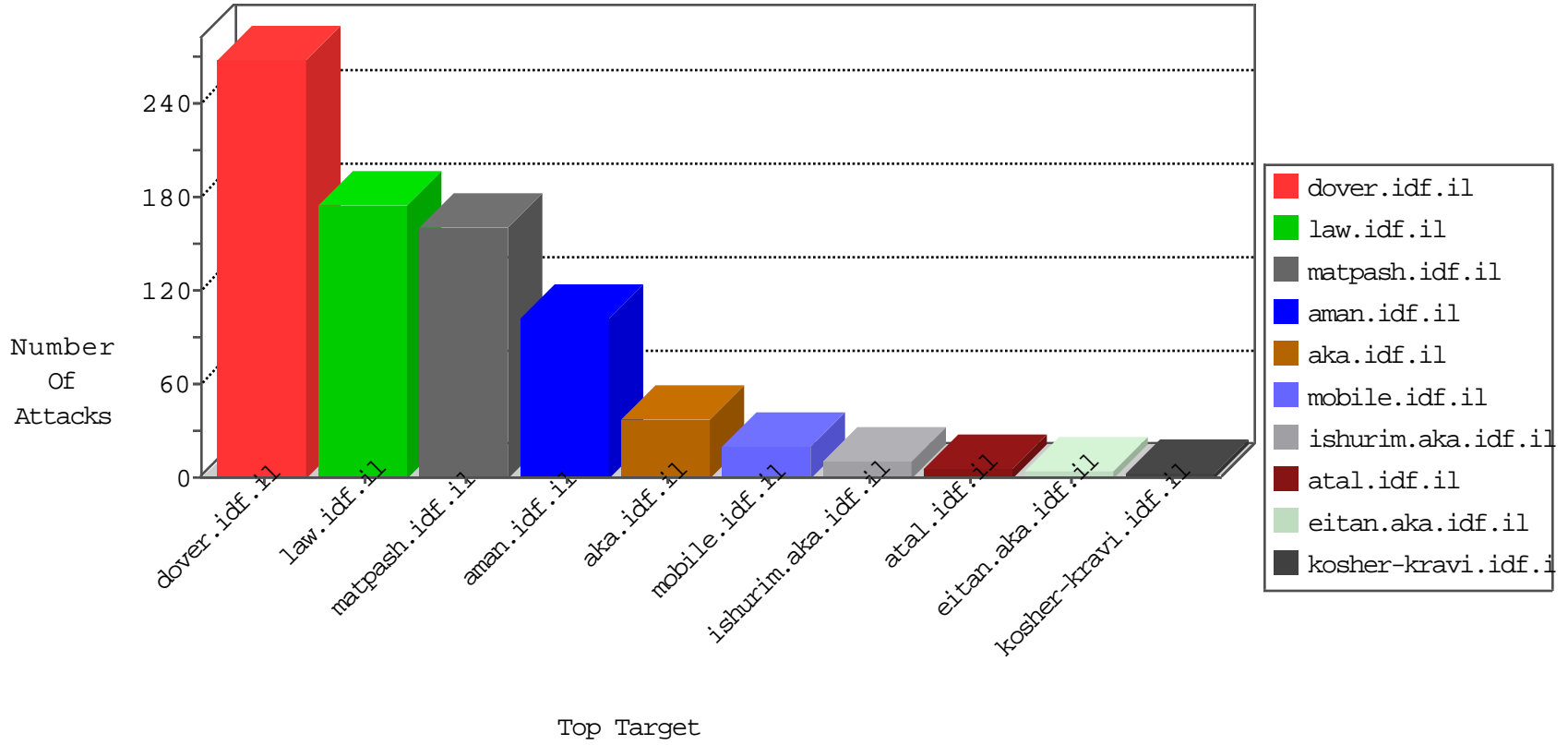


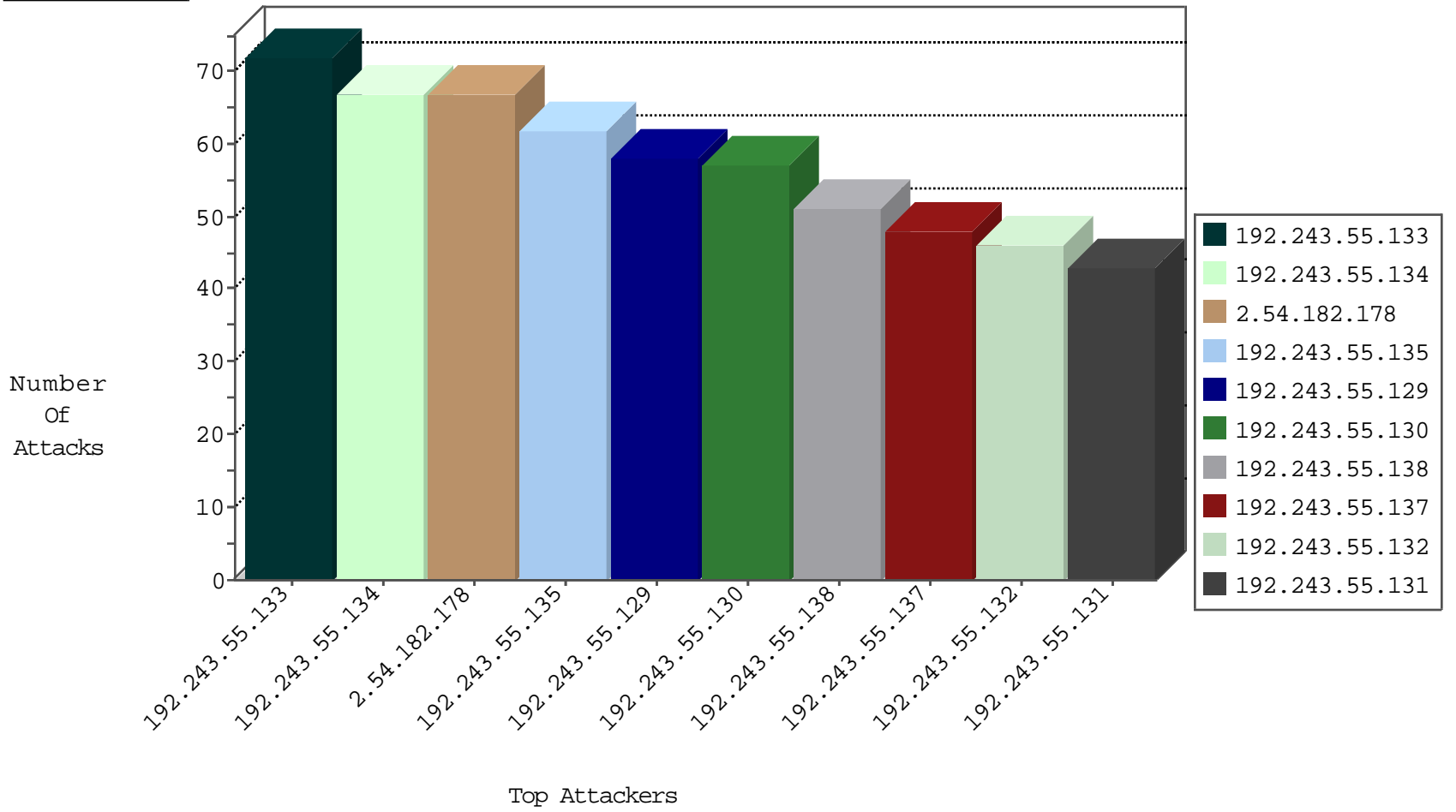
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.72	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.224	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
207.141.11.146	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.208	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.224	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.100	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.216	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.104	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.58	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.220	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
79.25.252.53	Italy	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
104.168.147.242	United States	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
193.105.134.220	147.237.76.198	Sweden	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.94.12	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.145.38	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.170	Sweden	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.0.15	Sweden	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.76.30		himush.idf.il	ET SCAN NMAP -sS window 1024	1
52.87.243.150	147.237.76.44	United States	e.refuah.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
2.54.182.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
2.54.182.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.45.218	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	12
2.54.182.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.182.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.182.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.81.240	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.219.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
186.56.4.3	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.182.178	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.32.179.22	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.45.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.45.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.45.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.46.41.97	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.46.41.97	Block	18
69.41.14.130	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
185.12.108.247	Turkey	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.12.108.247	Block	5
199.30.24.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.61	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0119-	Block	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
173.247.228.10	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/smalim/smalim.aspx	None	1
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
69.41.14.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.46.41.97	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
184.105.247.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /mivtza> ü , ÿ .</p></div>#012#012#012#012#012</div>#012#012<table cellpadding=	Block	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	1
94.230.93.10	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.241.229.223	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/main.asp	Block	1
94.230.93.112	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.24.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/dover.aspx?searchtext=	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
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
173.247.228.10	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
199.30.24.208	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1