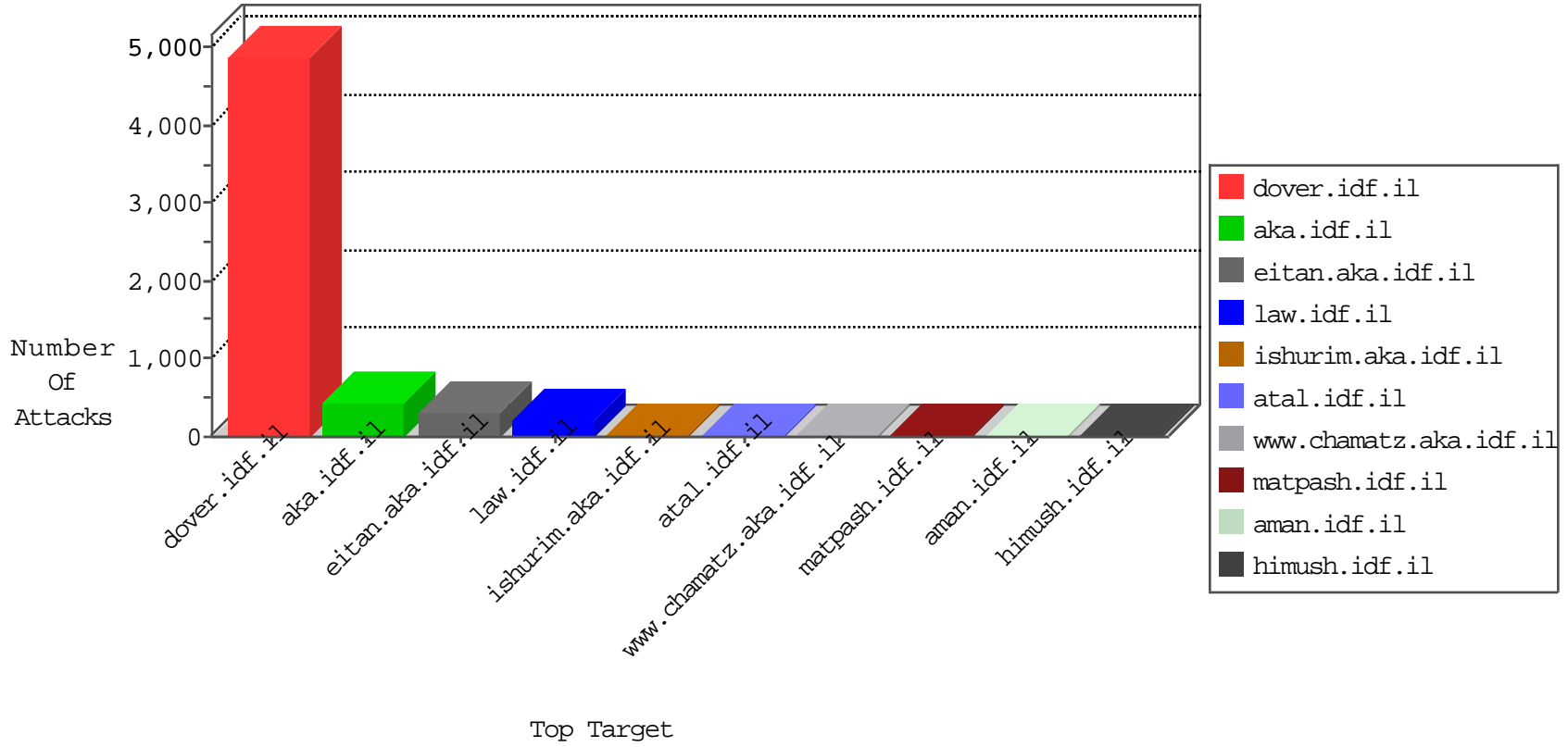


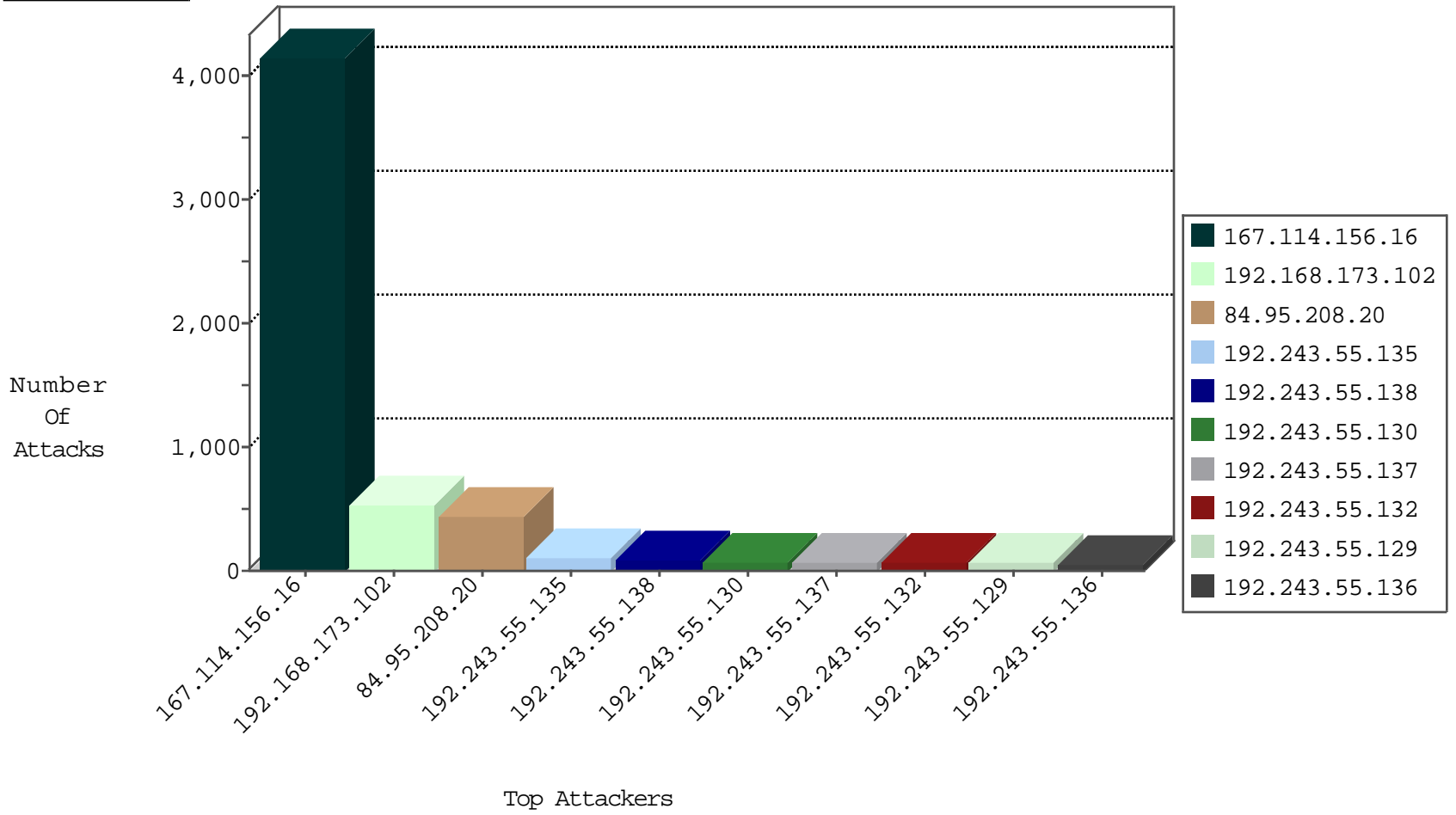
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4133
219.232.243.28	China	147.237.76.30	himush.idf.il	Invalid L4 Header Length	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.50	Switzerland	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
219.232.243.28	China	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	1
115.159.35.109	China	147.237.76.30	himush.idf.il	L4 Source or Dest Port Zero	drop	1
179.43.144.50	Switzerland	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
115.159.150.148	China	147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	1
219.232.243.28	China	147.237.72.14	dover.idf.il(old)	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.62.130	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.36.86	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
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	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
69.30.198.178	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	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
198.20.69.74	147.237.76.38	United States	e.e.meitav.idf.il	ET DROP Dshield Block Listed Source	1
119.93.73.250	147.237.0.33	Philippines	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.76.16.210	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
204.111.81.148	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.216.176.244	147.237.72.167	Latvia	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
179.184.176.50	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Potential SSH Scan	1
118.173.133.47	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.76.16.210	147.237.77.226	United States	www.chamatz.aka.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
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	346
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	187
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
107.167.113.99	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	9
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.135	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.133.192	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.137	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.177.113.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
85.64.76.66	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.129	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.76.66	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.117.82	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.130	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.138	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	99
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
192.243.55.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	7
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
23.254.250.121	United States	147.237.77.176	matpash.idf.il	Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
192.243.55.135	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	3
192.243.55.134	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	3
192.243.55.132	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.243.55.135	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
192.243.55.130	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	2
192.243.55.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
192.243.55.134	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
192.243.55.129	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
192.243.55.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
192.243.55.129	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	2
77.75.76.164	Czech Republic	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
65.55.210.86	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
159.203.170.126	United States	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
199.30.25.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
5.153.234.154	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
85.65.231.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58628&docid=65594	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smali/showbig.aspx	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
207.46.13.144	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/994-7826-he/nakhal.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59390&docid=76115	Block	1
114.98.246.172	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he/shared/usercontrols/headerupper/	Block	1
198.58.102.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
192.243.55.133	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.105.247.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authentication/service.aspx/getauthuser	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59333&docid=68024	Block	1
192.243.55.131	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
45.55.133.129	United States	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.24.185	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1113-2.stm" target="_blank	Block	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
65.55.210.66	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.206	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/	Block	1
199.30.25.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1