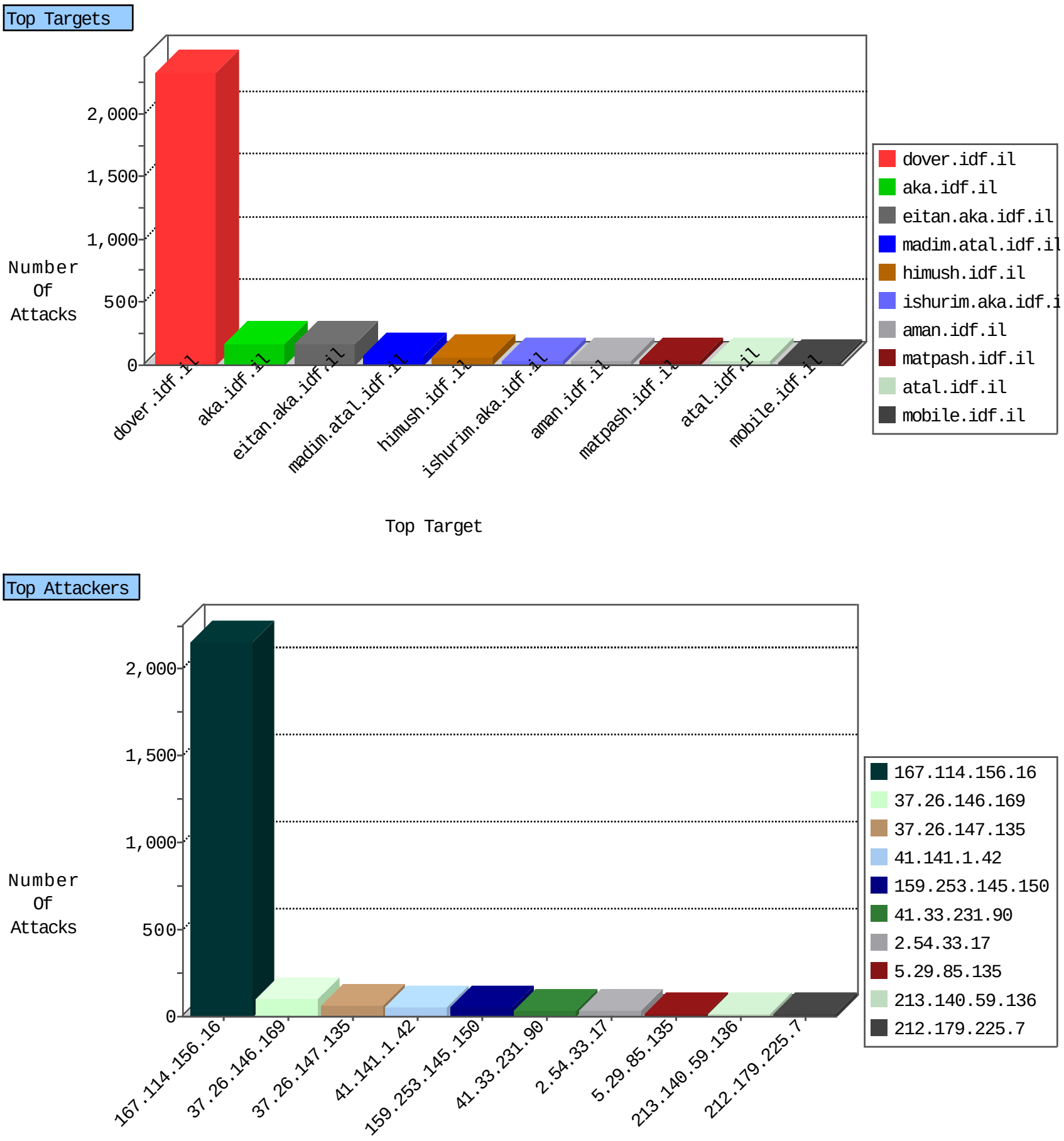
01-22-2016-11:04:04 to 01-22-2016-12:04:04

IDF Under Attack Daily Report



01-22-2016-11:04:04 to 01-22-2016-12:04:04

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	DOS-Tool-SwitchbladG	dest-reset	3057
123.249.56.174	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

01-22-2016-11:04:04 to 01-22-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.253.145.150	United States	147.237.76.30	himush.idf.il	C095: Suspicious Addresses MFA	Permit	47
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	2

01-22-2016-11:04:04 to 01-22-2016-12:04:04

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	3
61.240.144.64	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.170	United States	maarachot.idf.il	ET DROP Dshield Block Listed Source	1
159.8.109.19	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
119.81.188.158	147.237.76.196	Hong Kong	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.64	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.86.38	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
199.191.56.187	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.76.38	Latvia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
182.72.109.162	147.237.77.234	India	halag.idf.il	ET SCAN NMAP -sS window 1024	1
159.8.109.19	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.239.230	147.237.72.156	Netherlands	aman.idf.il	OS-OTHER Cisco IOS HTTP configuration attempt	1
91.201.236.113	147.237.76.177	Ukraine	ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.64	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1

01-22-2016-11:04:04 to 01-22-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
37.26.147.135	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
41.141.1.42	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.140.59.136	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.179.225.7	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	16
46.19.85.220	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.30	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
108.27.145.222	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.52.10.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.38	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.140	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.91	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.29.85.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.207	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.171	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.146.169	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.148.135	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
94.159.141.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.38.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
108.27.145.222	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
91.135.102.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
83.247.89.101	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
77.87.228.69	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.29.85.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4
37.26.148.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
188.120.148.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.38.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.19.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.47	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
217.132.11.98	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
2.54.146.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.169	Israel	147.237.8.45	e.eitan.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.14.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.201.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.23.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.123	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.43.174	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.33.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.33.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.148.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
2.54.14.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
185.32.179.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
185.32.179.54	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 185.32.179.54	Block	7
37.26.146.169	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 37.26.146.169	Block	6
132.70.66.13	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112427.pdf	Block	2
2.52.16.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.80.53.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.195.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.179.30.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.137.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/y1cebowm67a	Block	1
84.108.184.59	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
2.54.24.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.106.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113085.pdf&sa=u&ved=0ahukewipv9nzkr3kahudc3ikhbukduiqfggkmae&usg=afqjcngyvmfwfnc01onsm71gxqbnncw8bq	Block	1
80.246.139.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
46.19.86.130	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
104.128.144.131	Canada	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/redirect.php	Block	1
84.108.184.59	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.nakhal.idf.il/xmlrpc.php	Block	1
2.54.147.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/client_204	Block	1
188.138.61.79	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
71.161.114.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
157.55.39.70	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/news/news.asp	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/105641.pdf	Block	1
40.77.167.64	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/www.navy.idf.il	Block	1
84.228.150.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.27.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.199.57.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
109.163.234.5	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.86.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.184.59	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
2.54.147.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.138.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
193.254.206.6	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 193.254.206.6	Block	1
79.178.99.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.86	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/112900.pdf	Block	1
41.141.1.42	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
94.159.141.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.108.184.59	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
213.57.157.210	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
71.161.114.179	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
185.32.179.54	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
46.120.68.255	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
84.108.184.59	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.108.184.59	Block	1
2.54.11.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1