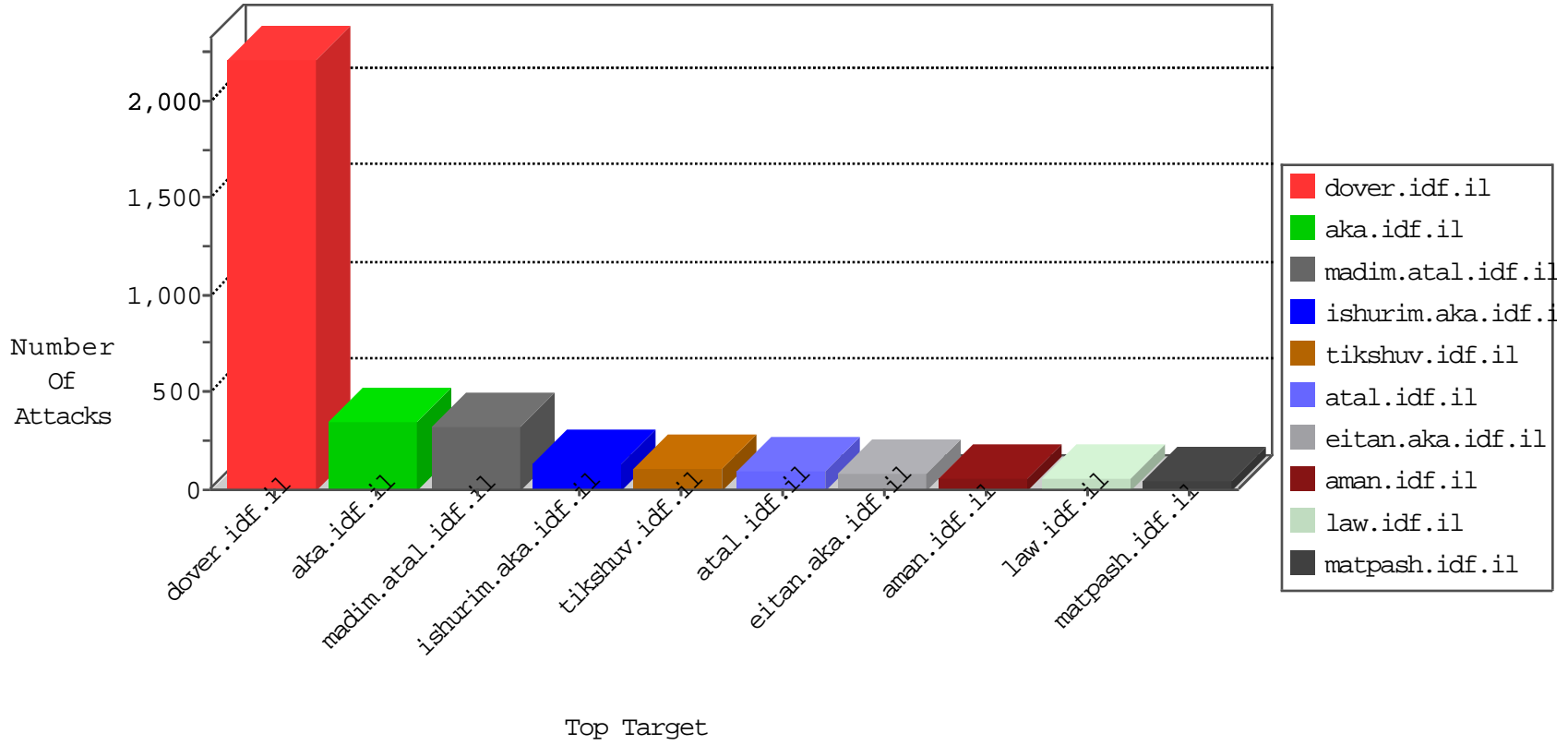


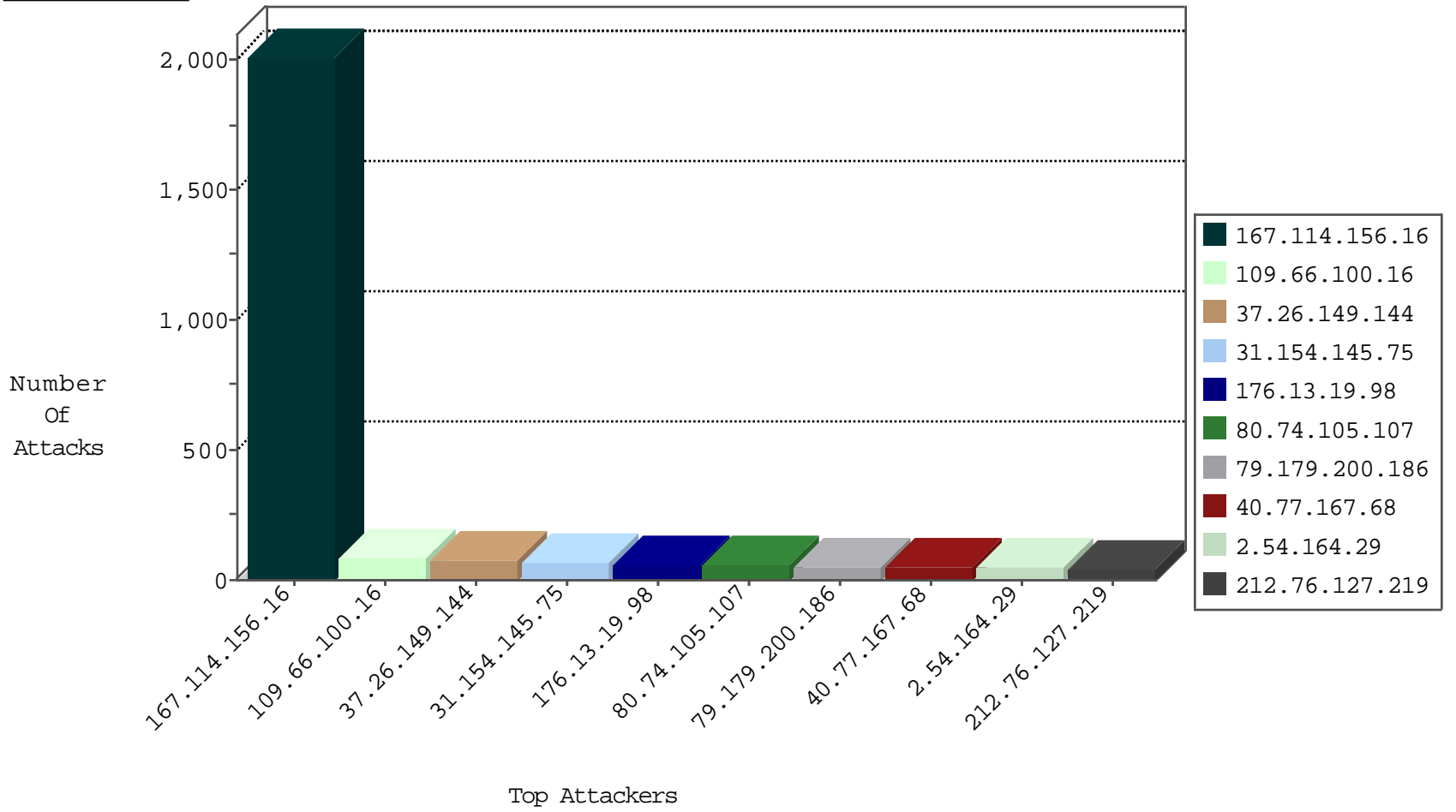
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3008
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	9
84.108.85.95	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
213.151.53.59	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.130.5.224		147.237.76.177	ncore.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
80.246.130.24	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
66.249.81.201	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
213.57.180.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
106.66.229.36	147.237.0.16	India	my-kosher-kravi.idf.il	GPL SCAN nmap TCP	1
77.125.124.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.219.246.172	147.237.76.196	Taiwan	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.227.254.67	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.107	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.125.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.135.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.100.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	42
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
37.216.18.164	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.117	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
149.78.253.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
80.178.147.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
80.246.130.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.223	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.206	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
82.166.57.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.163.203	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
80.246.130.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
80.178.231.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.65.19.65	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
5.102.214.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.61.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.169.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.242	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.33.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.18.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.68	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
87.69.55.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.81.57.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.108.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.1.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.55.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
80.246.139.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.28	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.52.173.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.28	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.177	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.94	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.186	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.188.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
185.3.146.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.188.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK 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
46.19.85.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
31.154.145.75	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
176.13.19.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
80.74.105.107	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 80.74.105.107	Block	56
79.179.200.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
2.54.164.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.54.150.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.54.163.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
87.68.37.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	16
5.28.136.29	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
176.13.17.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
79.178.116.48	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.116.48	Block	8
37.26.149.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
37.26.149.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.11.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.116.48	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	2
109.253.193.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.185.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
2.54.168.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
23.94.80.194	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 23.94.80.194	Block	2
212.179.159.253	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
109.253.147.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
212.76.97.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.223.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.75.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14322-he/d	Block	1
192.198.151.45	Europe	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/rabanut/scriptresource.axd	None	1
149.78.253.39	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.138.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.167.206	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
109.65.1.154	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
77.125.121.255	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ca-x@x'x*x x"xa x"xa" x"xa"tId in www.aka.idf.il/main/giyus/general.aspx	None	1
194.90.88.105	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
2.54.55.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
92.126.50.145	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
85.130.220.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3295.jpg	Block	1
80.178.157.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.0.56.125	Switzerland	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
212.150.7.77	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18863-en/dover.aspx.	Block	1
89.248.172.78	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
149.88.181.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.174.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1