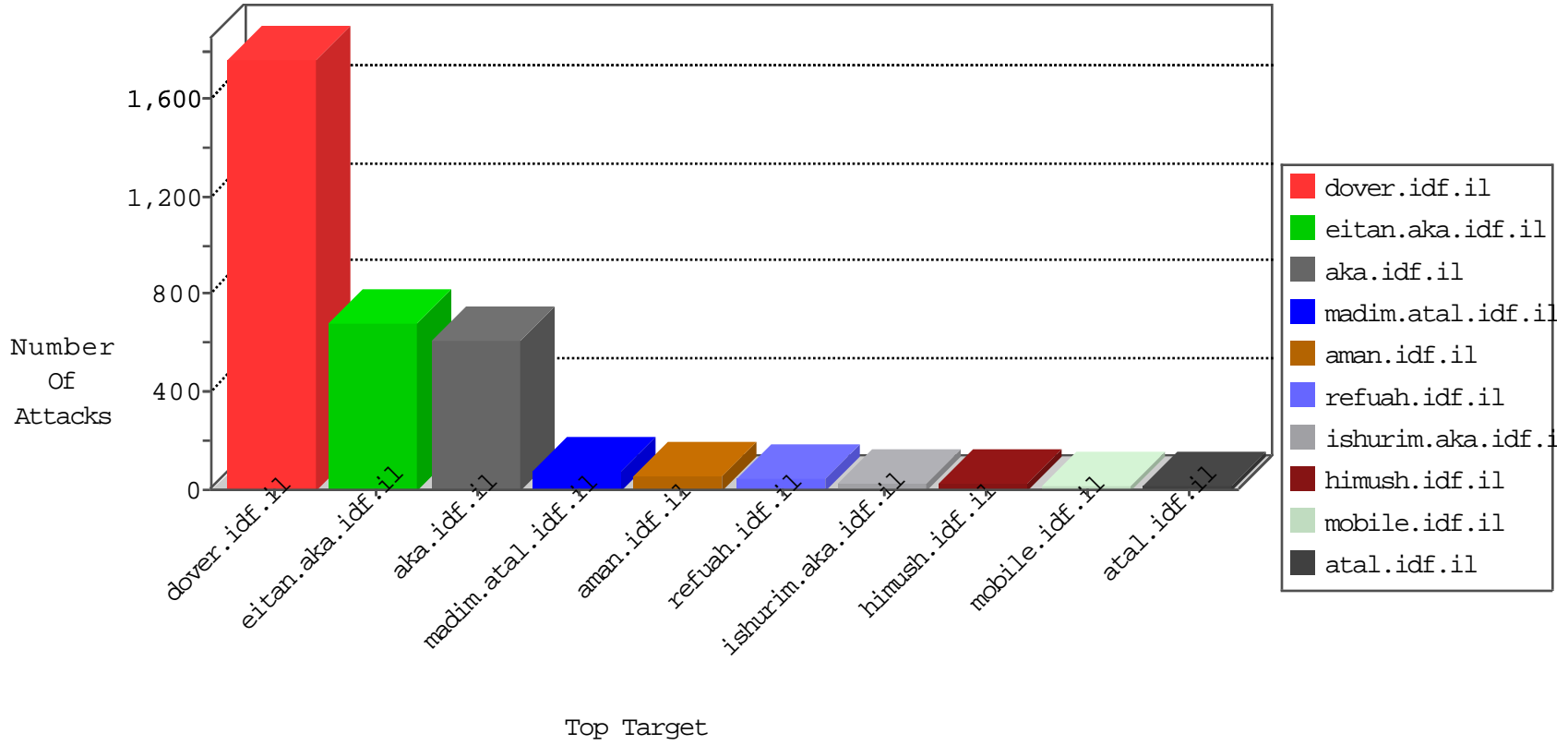


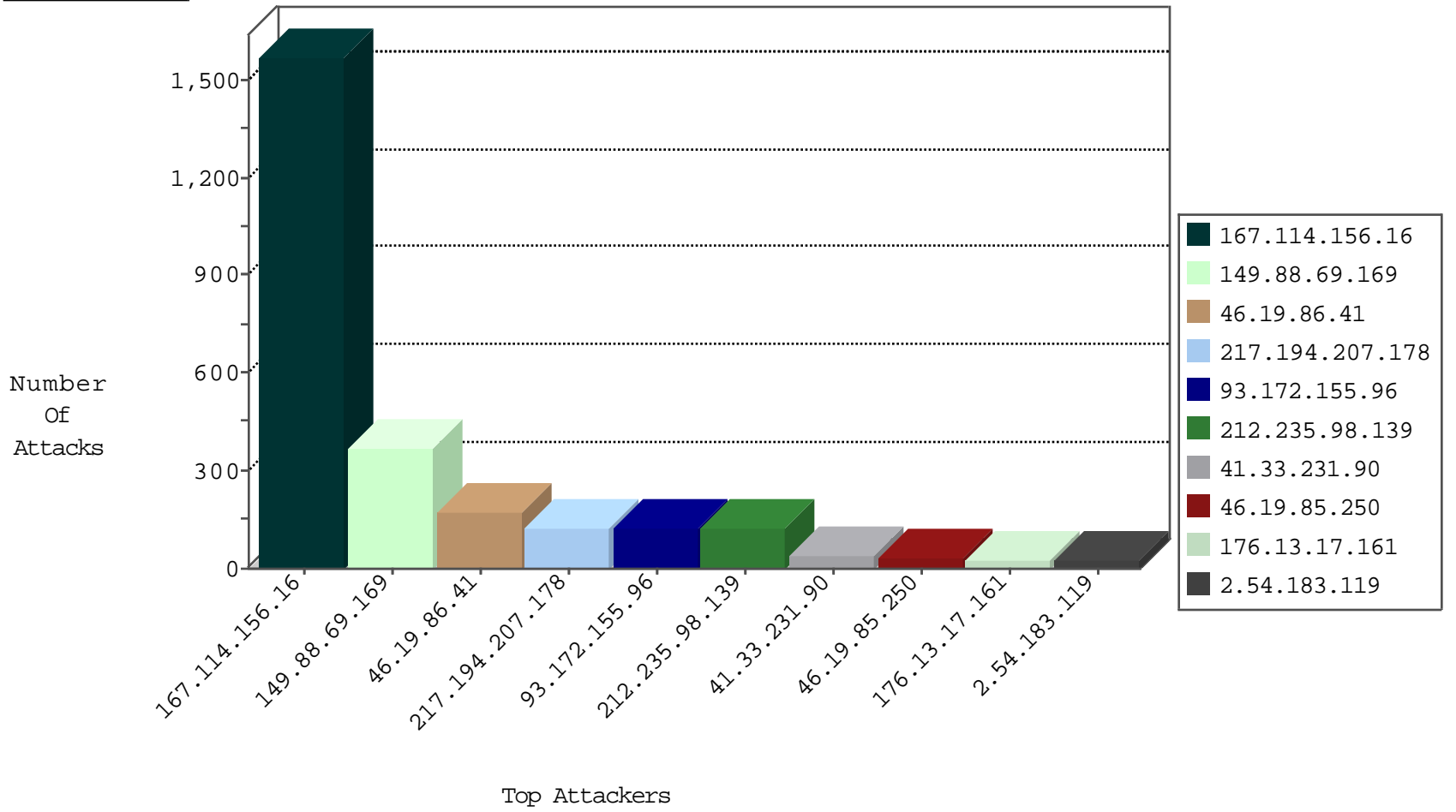
IDF Under Attack Daily Report



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	3273
79.181.154.209	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
66.249.66.36	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1

12-15-2015-10:04:05 to 12-15-2015-11:04:05

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	2
81.218.182.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.199	Cote D'Ivoire	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
79.180.155.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.97	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
180.97.106.162	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.19.158.160	147.237.72.217	Brazil	e.idf.il	ET SCAN NMAP -f -sS	1
37.26.148.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.136.140	147.237.72.167	Israel	ishurim.aka.idf.il	portscan: TCP Distributed Portscan	1
128.199.175.104	147.237.72.167	Singapore	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
108.30.83.8	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
85.250.178.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.199	Cote D'Ivoire	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
79.182.179.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.199	Cote D'Ivoire	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
79.179.11.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.29.32.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.117.47.183	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
177.19.158.160	147.237.72.217	Brazil	e.idf.il	ET SCAN NMAP -sS window 2048	1
45.55.173.20	147.237.0.16		my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
176.13.18.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
158.255.2.52	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.175.85	147.237.72.167	Singapore	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.218.246.103	147.237.76.42	Russian Federation	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
46.19.86.41	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	174
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	120
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
2.54.144.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
192.116.232.69	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.86.116	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	11
217.194.199.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
80.246.138.161	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.54.183.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
83.221.173.41	Uzbekistan	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.179.21.194	Israel	147.237.76.177	ncore.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.200.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.24.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.142	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.125.26	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.251.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
88.79.95.146	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
77.126.10.252	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.138.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
62.90.147.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.183.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.137.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.183.57.72	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
213.57.131.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.183.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.136.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.138.10.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.183.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.14	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.148.164	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.140.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.14	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
203.133.169.84	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.131.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.246.139.148	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.116.239.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
93.172.155.96	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.11.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.173.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
217.194.199.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.95.251.244	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
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	358
217.194.207.178	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	124
93.172.155.96	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	115
46.19.85.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.17.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	5
109.65.39.30	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	4
37.26.147.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.151.252	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.aspx/getauthuser	Block	3
82.166.184.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
176.13.11.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.66.83	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.140.54	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
80.246.137.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.25.85.234	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
77.125.117.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
66.249.66.81	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
31.168.28.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
2.54.50.14	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers Referer	Block	1
83.244.55.106	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2827.jpg	Block	1
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
217.74.241.24	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
176.13.15.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.39.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
68.180.229.27	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
212.143.76.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.150.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1
87.68.47.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.86.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.30	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
81.218.44.254	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
79.179.146.223	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
212.199.71.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
45.55.173.20		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
173.252.112.98	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	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
2.54.51.116	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.111.225.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1