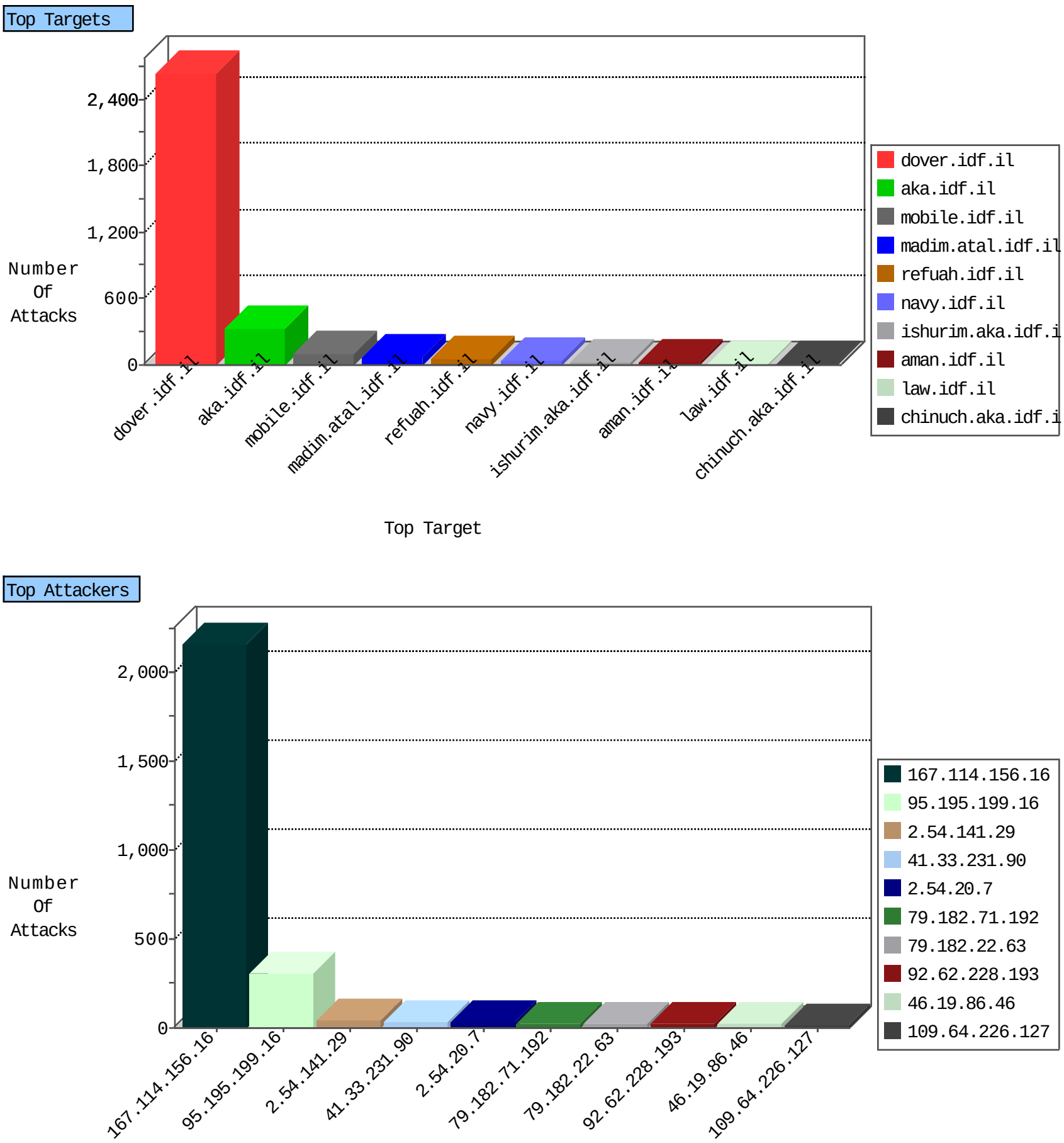
01-12-2016-18:04:08 to 01-12-2016-19:04:08

IDF Under Attack Daily Report



01-12-2016-18:04:08 to 01-12-2016-19:04:08

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	3277
109.65.30.217	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
109.64.68.161	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
61.101.8.15	Korea, Republic of	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
85.25.217.16	Germany	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
61.101.8.15	Korea, Republic of	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
61.101.8.15	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

01-12-2016-18:04:08 to 01-12-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-12-2016-18:04:08 to 01-12-2016-19:04:08

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
79.183.241.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
213.57.237.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
73.17.14.46	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
212.76.101.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.93.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.22.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.159.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
131.109.15.15	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
131.109.15.15	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.0.33	Canada	idf.il	ET SCAN NMAP -sS window 2048	1
84.108.189.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.62.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.38	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
79.177.196.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.202.100	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
37.142.237.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.15.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
134.213.177.204	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
131.109.15.15	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
109.66.132.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.0.33	Canada	idf.il	ET SCAN NMAP -f -sS	1
84.108.100.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.38	147.237.77.235	China	sviva.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1

01-12-2016-18:04:08 to 01-12-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.195.199.16	Sweden	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	306
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
2.54.141.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.182.22.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
92.62.228.193	Czech Republic	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
79.179.27.206	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	12
85.65.217.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.228.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.62.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
132.70.66.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.71.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.182.71.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
79.182.71.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.13.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.226.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.20.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.127.59.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.17.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.20.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.210.187.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.199.254	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.67.59.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.20.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.159.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.174.145	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.117.157.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.20.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.13.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.20.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.66.219.192	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.120.228.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.230.86.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.211	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.32.179.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.143	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.116.92.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.22.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.179.21.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.128.165	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.167.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.180.203.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-12-2016-18:04:08 to 01-12-2016-19:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
109.64.226.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
2.54.141.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
109.253.136.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.44.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
2.54.62.65	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	3
176.13.17.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.70.66.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
2.54.151.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
132.70.66.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
84.94.182.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.228.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.176.63.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.76.123.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/undefined	Block	2
109.186.148.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.13.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
54.161.160.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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
83.130.118.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.68.54	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
176.13.17.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.187.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.22.198	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.138.1.218	Germany	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
87.68.55.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.0.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.137.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.206.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
62.90.147.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/forgotpassword.aspx	Block	1
40.77.167.62	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/general.aspx	Block	1
180.97.221.22	China	147.237.77.216	dover.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 180.97.221.22	None	1
2.54.171.8	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
141.8.142.99	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.25.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.109.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.117.157.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.116.142.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-12-2016-18:04:08 to 01-12-2016-19:04:08