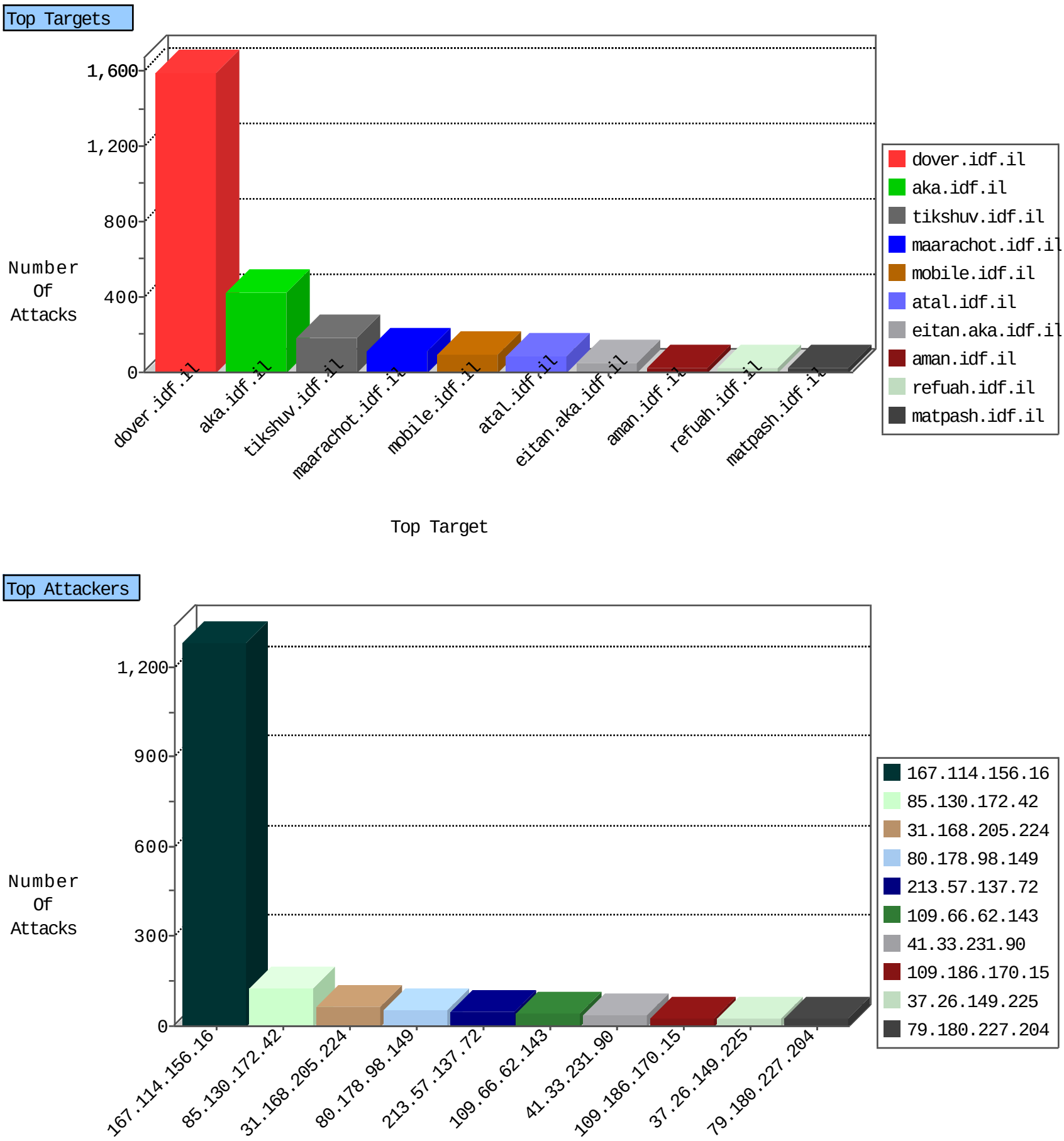
12-31-2015-17:04:02 to 12-31-2015-18:04:02

IDF Under Attack Daily Report



12-31-2015-17:04:02 to 12-31-2015-18:04:02

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	3043
198.58.102.49	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
222.186.21.81	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
189.251.176.210	Mexico	147.237.77.243	mobile.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
146.185.239.100	Russian Federation	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1

12-31-2015-17:04:02 to 12-31-2015-18:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-31-2015-17:04:02 to 12-31-2015-18:04:02

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
110.154.157.29	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.198.216.130	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
84.111.111.134	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
168.62.238.153	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.207.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.200.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.137.231.190	147.237.76.86	Thailand	navy.idf.il	ET SCAN NMAP -sS window 1024	1
124.65.231.114	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
111.196.66.207	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
111.196.66.207	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
111.196.66.207	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
192.198.216.130	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.121	Ukraine	e.navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.198.216.130	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
84.109.82.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.88.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
124.65.231.114	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
111.196.66.207	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
111.196.66.207	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
111.196.66.207	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1

12-31-2015-17:04:02 to 12-31-2015-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
31.168.205.224	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
80.178.98.149	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
213.57.137.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	45
109.66.62.143	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.149.225	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
85.130.172.42	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
79.180.227.204	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
85.130.172.42	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
79.183.152.117	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
85.130.172.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
85.130.172.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
85.130.172.42	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
85.130.172.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.179.198.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.128.41.103	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
5.102.220.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.118.11.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
31.154.161.56	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
79.177.41.123	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
213.57.141.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
5.28.173.47	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.13.17.57	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
94.230.86.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
45.34.1.142		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
81.218.148.149	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
77.127.215.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.17.57	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.253.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.168.198	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
192.0.80.128	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.180.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.162.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.137.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.199.57.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.139.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.122.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.116.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.134.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.106.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.160.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

12-31-2015-17:04:02 to 12-31-2015-18:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.229.153.11	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	12
84.108.5.55	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	12
82.81.12.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	5
72.167.159.8	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 72.167.159.8	Block	5
212.25.102.57	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 212.25.102.57	Block	5
109.253.193.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.195.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.18.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.120.125.56		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.109.68.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.180.66.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.50.87.26	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.118.11.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
89.138.163.228	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
213.57.164.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.183.118	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
109.253.157.190	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
109.253.216.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.179.125.162	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
173.199.65.26	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.168.206.91	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
77.125.89.175	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
2.54.141.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.201.242.50	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/templates/navmenu/navmenu.css.aspx	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
212.143.43.42	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
84.108.70.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatus in www.aka.idf.il/main/sachar/payslips.aspx	None	1
41.44.161.55	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
79.179.198.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.57.252.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main-sachar	Block	1
5.29.97.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
109.67.109.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.182.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.12.186.103	Germany	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
52.90.147.70	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery.plugins/slider.js	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/17857.jpg	Block	1
82.80.57.177	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.138.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.3.5.77	Italy	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.142.28	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.211.0.114	Netherlands	147.237.72.166	aka.idf.il	Unknown Parameter author in www.aka.idf.il/	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-14220-he/dover.aspx	Block	1

12-31-2015-17:04:02 to 12-31-2015-18:04:02