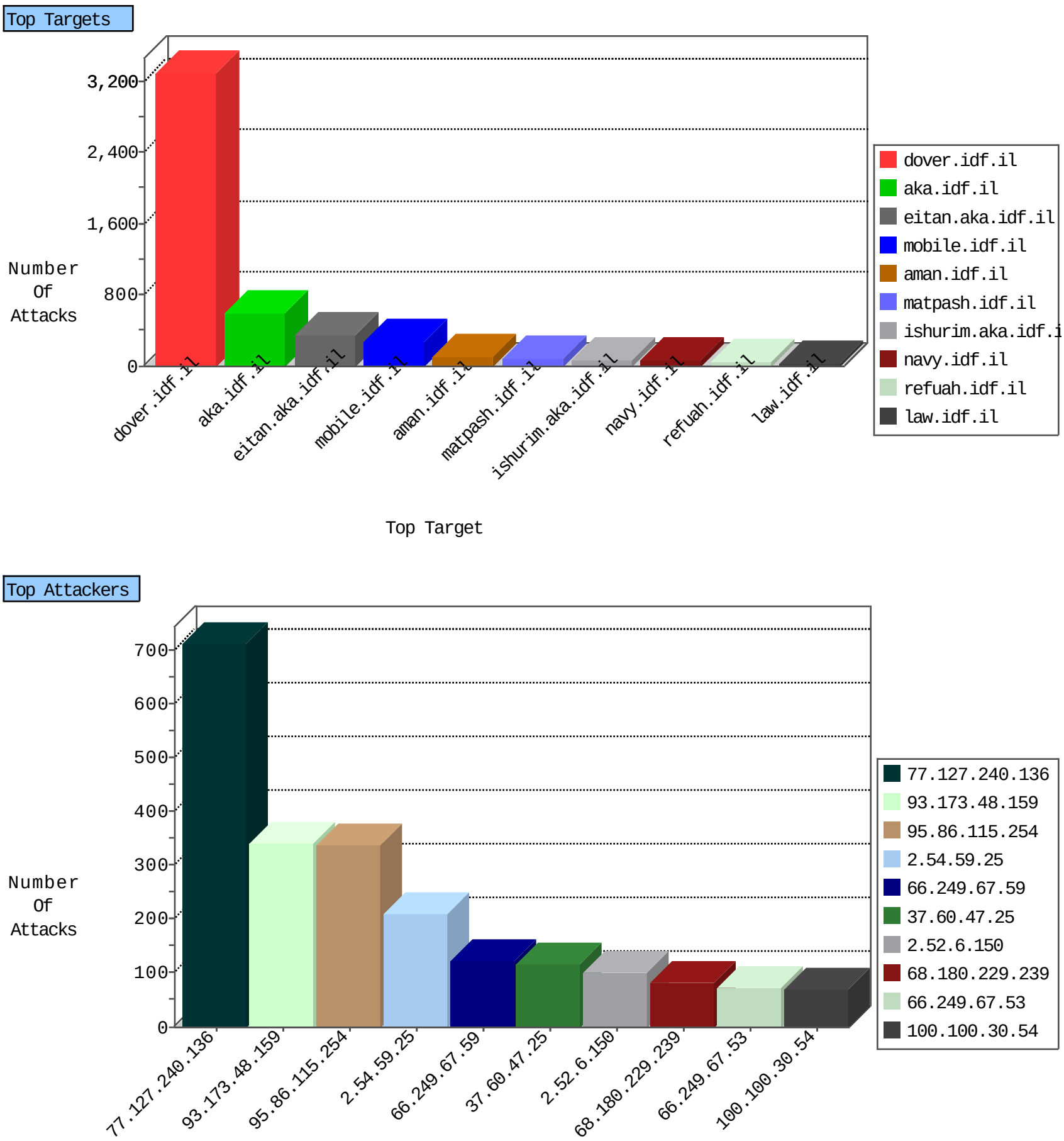
10-24-2015-21:04:09 to 10-24-2015-22:04:09

IDF Under Attack Daily Report



10-24-2015-21:04:09 to 10-24-2015-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.145.70	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	37
77.127.242.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
84.228.210.246	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
84.228.210.246	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
31.154.91.43	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	21
95.86.72.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
79.176.188.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.183.167.208	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
176.13.2.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.65.52.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.182.169.102	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.182.160.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
151.49.91.26	Italy	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.173.239	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
73.208.92.19	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
85.65.52.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
77.125.158.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.178.125.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
5.22.131.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.22.131.203	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-24-2015-21:04:09 to 10-24-2015-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-24-2015-21:04:09 to 10-24-2015-22:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
66.249.67.79	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.67.202	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.151.52.8	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 1024	2
182.48.105.216	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
123.151.149.222	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.190.71	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.186.190.71	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
62.210.25.83	147.237.0.35	France	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
217.147.86.8	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.151.52.8	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
198.12.97.86	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
198.12.97.86	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
182.48.105.216	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
182.48.105.216	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.138	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
222.186.190.71	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
222.186.190.71	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
198.12.97.86	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
43.229.53.89	147.237.0.16	Japan	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.12.97.86	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	147.237.77.61	Russian Federation	e.cogat.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

10-24-2015-21:04:09 to 10-24-2015-22:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.240.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	712
95.86.115.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	339
2.54.59.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	209
2.52.6.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
100.100.30.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	59
79.178.39.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
62.163.108.186	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
82.145.220.166	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.85.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	41
87.69.140.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
84.228.126.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
176.12.151.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
92.10.3.249	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
93.186.31.114	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
84.108.214.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
100.100.11.249		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
213.57.138.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
85.65.52.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
79.176.193.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
74.62.240.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	18
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
84.109.56.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.178.125.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.67.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
31.154.190.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
84.108.39.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
46.19.85.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.248.73.43	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.181.19.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
76.201.96.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
77.127.242.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
93.186.31.114	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.30.120		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
2.54.52.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.67.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
95.86.72.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12

10-24-2015-21:04:09 to 10-24-2015-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.48.159	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 93.173.48.159	Block	322
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	84
37.60.47.25	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.60.47.25	Block	70
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	56
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	56
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	42
37.60.47.25	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1884	Block	42
79.179.208.18	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	28
84.108.39.65	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/	Block	28
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	28
109.67.68.115	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	28
79.180.39.71	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	28
84.109.153.131	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	28
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	28
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
188.36.70.175	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	14
46.19.86.36	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	14
79.176.8.39	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.176.8.39 (Open Mode)	None	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	Block	14
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1158-he/dover.aspx	Block	14
188.165.15.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/349-he/patzar.aspx	Block	14
46.117.83.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
2.54.59.168	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
84.109.56.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	14
79.176.8.39	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
206.253.224.14	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	14
109.67.174.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.181.19.244	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	14
195.154.226.90	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-content/	Block	14
52.91.173.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
5.29.19.132	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	14
79.176.145.245	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/trajector/	Block	14
79.183.112.61	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/3/size220x0/15863.jpg	Block	14
62.0.67.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	14
5.29.219.141	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	14
93.173.48.159	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	14
79.176.145.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
176.12.148.194	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
80.246.130.35	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	14
77.127.242.84	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/16900.jpg	Block	14
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
31.168.90.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	14

10-24-2015-21:04:09 to 10-24-2015-22:04:09