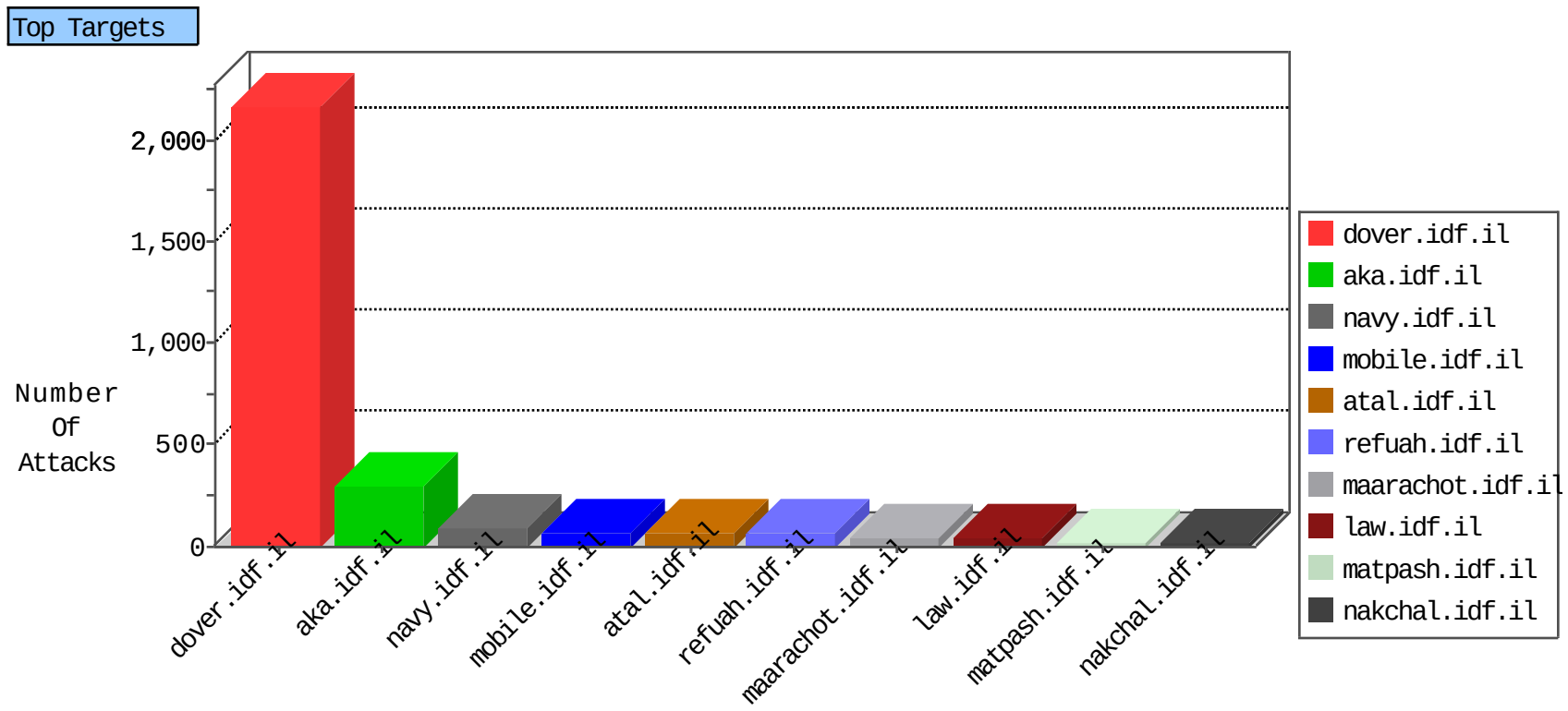
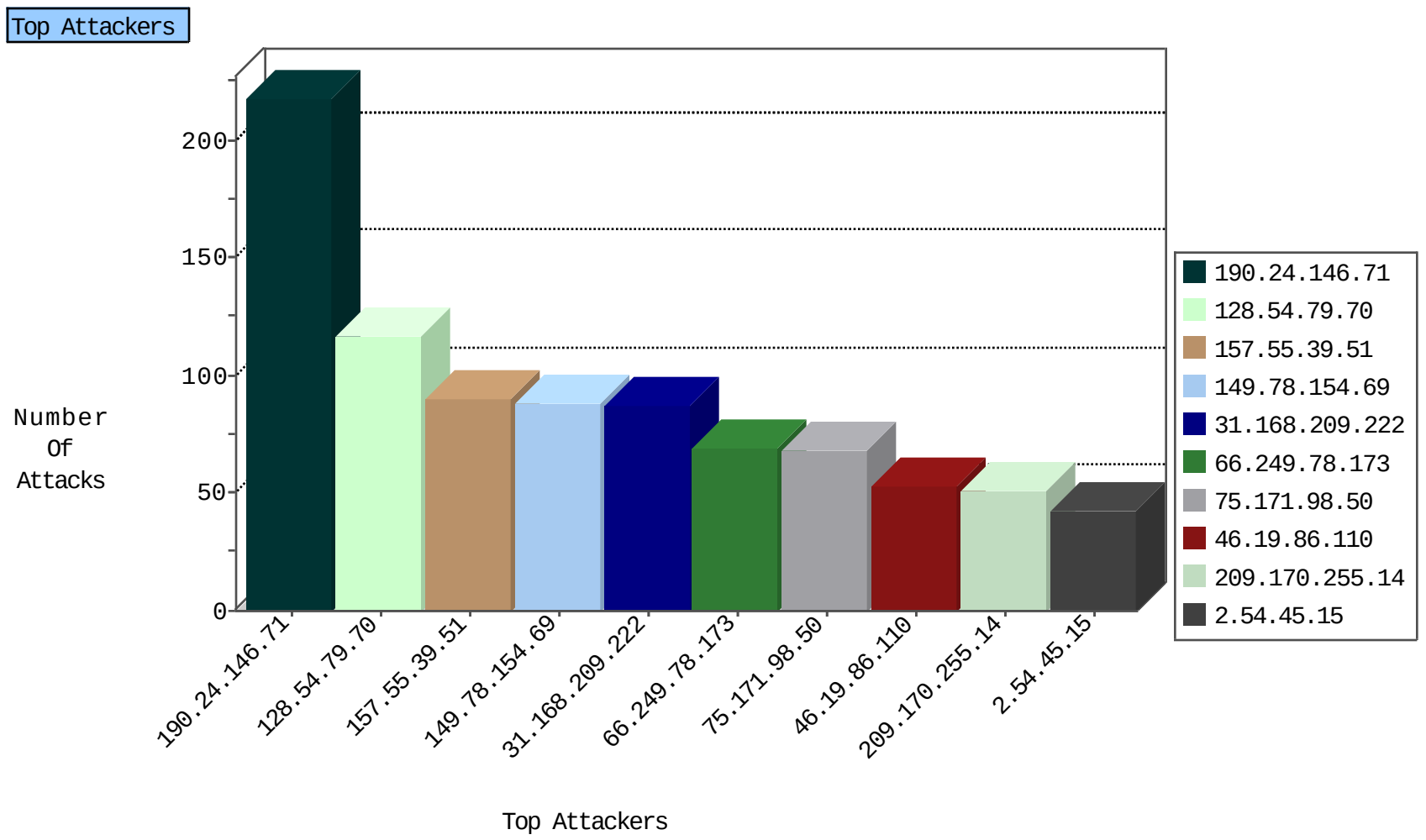
10-31-2015-01:04:01 to 10-31-2015-02:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-31-2015-01:04:01 to 10-31-2015-02:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8173
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3876
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2729
128.54.79.70	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	858
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	674
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	537
213.139.53.147	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	95
31.168.209.222	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	54
84.111.4.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
2.52.148.8	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24
176.13.7.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
31.168.209.222	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
79.181.97.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
46.19.86.110	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
213.57.190.150	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
209.170.255.14	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
17.142.152.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
90.214.125.65	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
46.120.115.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
176.106.226.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
17.142.152.94	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.86.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
17.142.145.3	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
146.185.239.100	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
2.241.209.173	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-31-2015-01:04:01 to 10-31-2015-02:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-31-2015-01:04:01 to 10-31-2015-02:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.60	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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
112.171.173.85	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
112.171.173.85	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
62.212.230.9	147.237.76.197	Azerbaijan	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
186.147.233.160	147.237.76.39	Colombia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
186.147.233.160	147.237.76.39	Colombia	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
12.216.138.71	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
118.244.216.171	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
112.171.173.85	147.237.8.46	Korea, Republic of	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
112.171.173.85	147.237.8.27	Korea, Republic of	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
112.171.173.85	147.237.8.14	Korea, Republic of	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.166	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
62.212.230.9	147.237.76.177	Azerbaijan	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
186.147.233.160	147.237.76.39	Colombia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
12.216.138.71	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
118.244.216.171	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
118.244.216.171	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -f -sS	1

10-31-2015-01:04:01 to 10-31-2015-02:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	218
128.54.79.70	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
31.168.209.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
75.171.98.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
209.170.255.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
12.9.250.183	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
99.17.228.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
187.50.199.66	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
17.142.152.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
17.142.152.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
176.12.138.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
176.12.141.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
17.142.145.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
17.142.152.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.13.7.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
40.77.167.71	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
24.182.106.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
17.142.152.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
17.142.152.111	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
90.214.125.65	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
17.142.152.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
17.142.152.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.101.179		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.54.45.15	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.241.209.173	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.67.41	United States	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.117.108.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.120.22.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
177.41.75.205	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.33	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
17.142.152.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	30
2.54.45.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
178.255.215.87	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	15
109.145.248.250	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation catId in www.navy.idf.il/navy/articles.aspx	Block	15
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	15
192.99.20.92	Canada	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	15
157.55.39.51	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/eitan/listpage/default.asp	None	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan.	Block	15
5.254.65.183	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	15
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8896-he/refuah.aspx	Block	15
209.249.157.69	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/sendtofriend/sendtofriend.aspx	Block	15
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1237-he/atal.aspx	Block	15
179.223.121.108	Brazil	147.237.77.74	law.idf.il	PHP Attempt	Block	15
110.45.135.229	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/giyus/forum/asp/showforum.asp	None	15
193.143.77.22	Poland	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.143.77.22	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/108997.pdf	Block	15
157.55.39.51	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/sites/miktzoa/default.asp	None	15
58.210.44.162	China	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	15
79.180.221.148	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.180.221.148	Block	15
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8769-he/refuah.aspx	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	15
179.223.121.108	Brazil	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	15
157.55.39.51	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/news/default.asp	None	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	15
2.11.140.151	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	15
75.171.98.50	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17329.jpg	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/9/107389.pdf	Block	15
157.55.39.51	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/kurs/default.asp	None	15
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on www.navy.idf.il/navy/articles.aspx parameter catId	Block	15
85.143.24.70	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	15
183.245.77.242	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx	Block	15
157.55.39.51	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
2.52.148.8	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	15
77.6.140.80	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	15
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17344.jpg	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
177.21.255.18	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	15
108.227.98.31	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	15
66.249.65.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	15