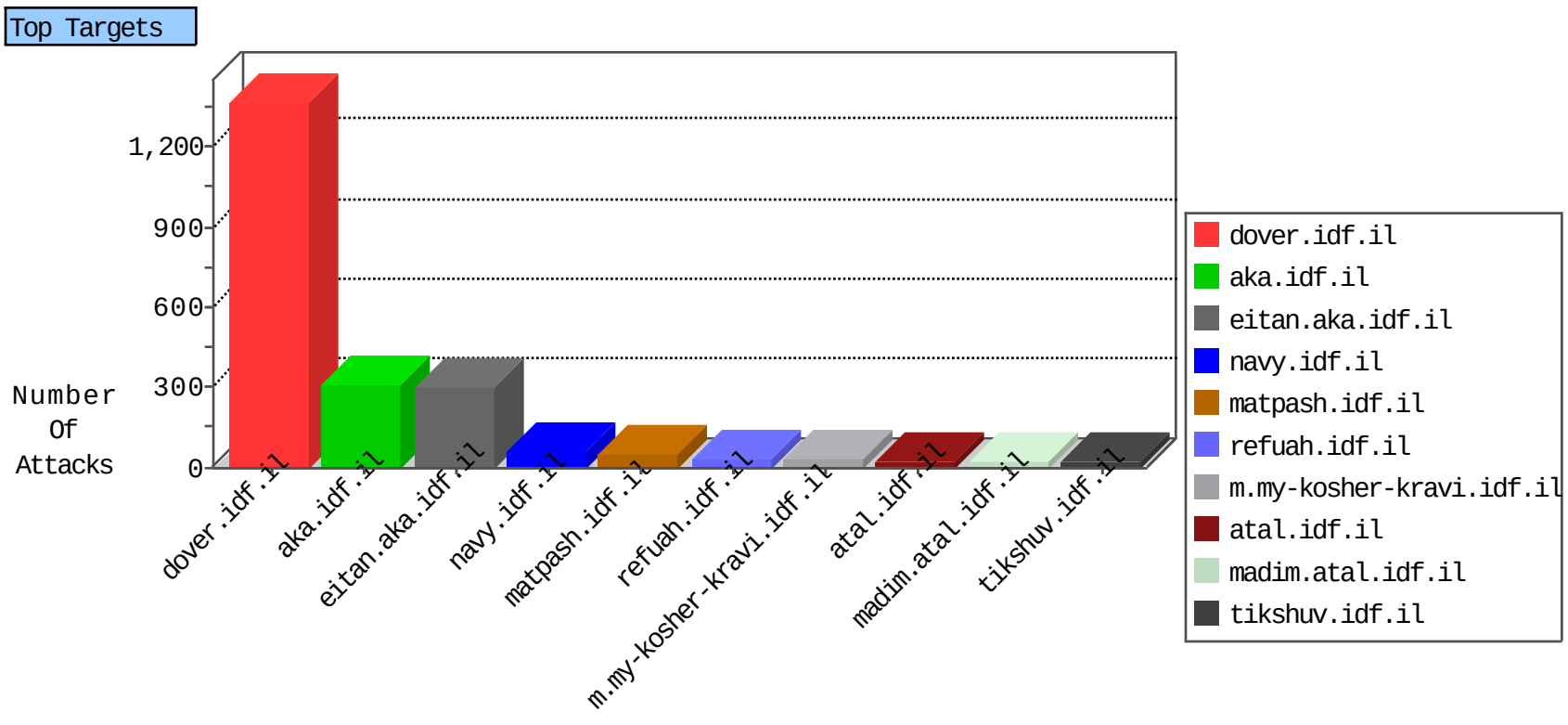
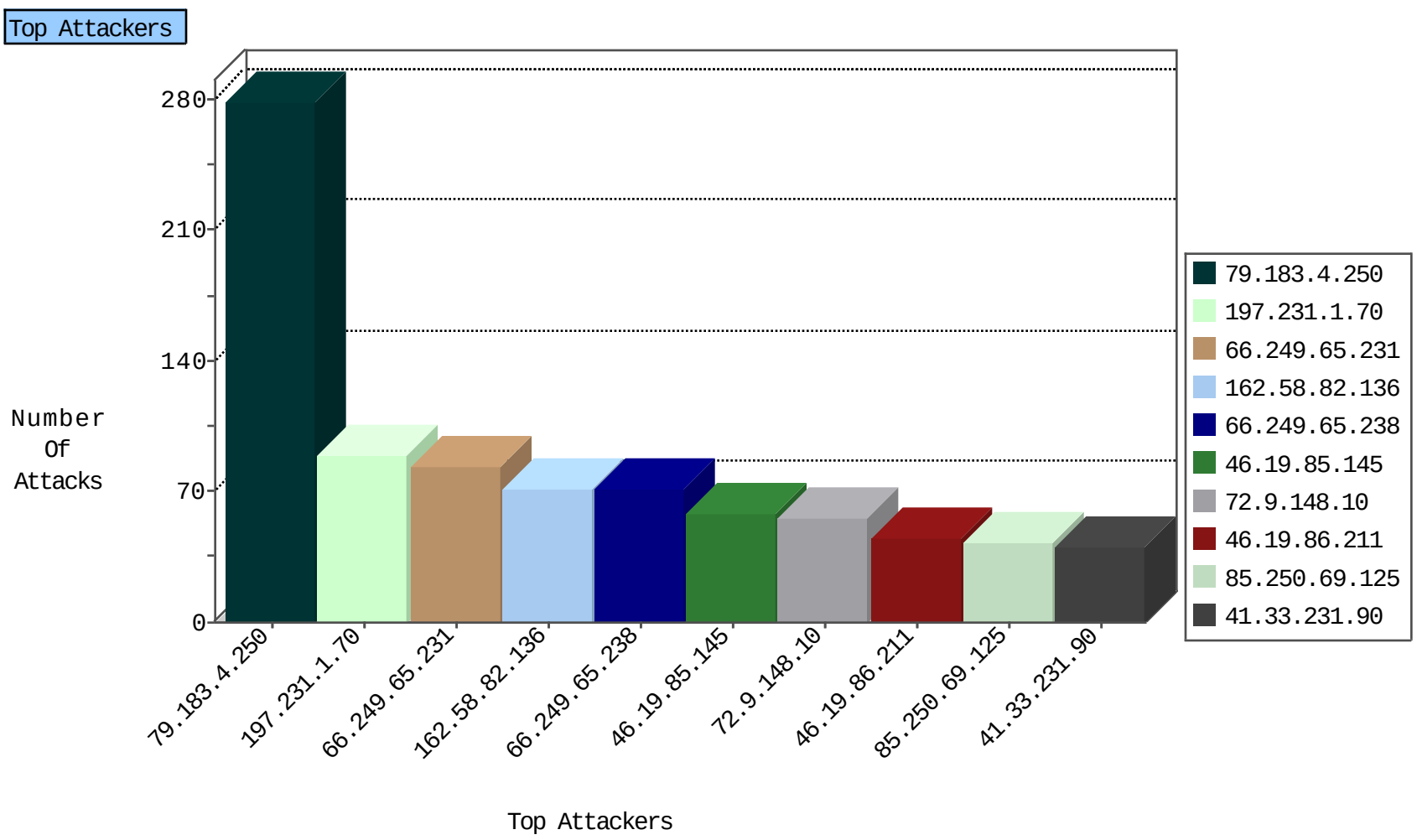
10-23-2015-22:04:00 to 10-23-2015-23:04:00

IDF Under Attack
Daily Report





10-23-2015-22:04:00 to 10-23-2015-23:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.194.104	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	146
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
109.65.57.119	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
192.168.201.252		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
46.19.85.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.182.185.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.110.33.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
68.32.50.150	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
79.181.2.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
172.19.3.107		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
77.125.72.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.12.139.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.110.208.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
37.142.68.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
50.242.46.1	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.22.129.152	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	3
84.228.13.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.22.129.152	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
37.26.147.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.176.225.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.67.180.13	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.180.185.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.67.180.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.86.217	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.183.43	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.179.102.94	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
192.116.177.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
45.32.68.116		147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
2.54.157.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.110.208.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-23-2015-22:04:00 to 10-23-2015-23:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-22:04:00 to 10-23-2015-23:04:00

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	5
5.143.82.242	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
210.61.150.154	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.98	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
37.143.82.50	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
210.61.150.154	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
210.61.150.154	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
185.100.85.71	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 4096	1

10-23-2015-22:04:00 to 10-23-2015-23:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.4.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	276
197.231.1.70	Mauritania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
162.58.82.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
46.19.85.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
85.250.69.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
100.100.72.222		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
149.78.202.17	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
105.158.38.74	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
80.246.133.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
100.100.105.185		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.125.212		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	14
100.100.125.212		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.102.170.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.42.64		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
84.229.49.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.57.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.167.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.182.117.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.12.139.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.100.24.155		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
203.6.176.20	Australia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
94.230.86.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
134.152.194.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.116.177.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.12.139.234	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.110.208.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.230.39.50	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
85.255.232.37	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.217.216.76	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.169.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

10-23-2015-22:04:00 to 10-23-2015-23:04:00

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	56
85.65.50.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	28
46.19.86.211	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 46.19.86.211	Block	28
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
207.46.13.149	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.aspx	Block	14
79.182.164.152	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
213.8.247.86	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
85.65.174.184	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9711-he/refuah.aspx	Block	14
46.19.86.211	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method undefined in URL www.aka.idf.il/main/giyus/api/api/professiondescription/5316	Block	14
115.230.126.48	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckfinder	Block	14
81.223.254.34	Austria	147.237.77.234	halag.idf.il	Unauthorized URL Access to /robots.txt	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	14
213.57.216.150	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	14
89.138.77.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
54.179.134.216	Singapore	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	14
141.212.122.160	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	14
84.228.207.30	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	14
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
217.69.133.224	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/faq/default.asp	Block	14
93.173.148.91	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
79.111.218.222	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
207.46.13.132	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/dynamic_map.aspx	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
94.23.30.222	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
79.180.185.191	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	14
84.228.207.30	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	13
109.65.177.204	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	8

10-23-2015-22:04:00 to 10-23-2015-23:04:00