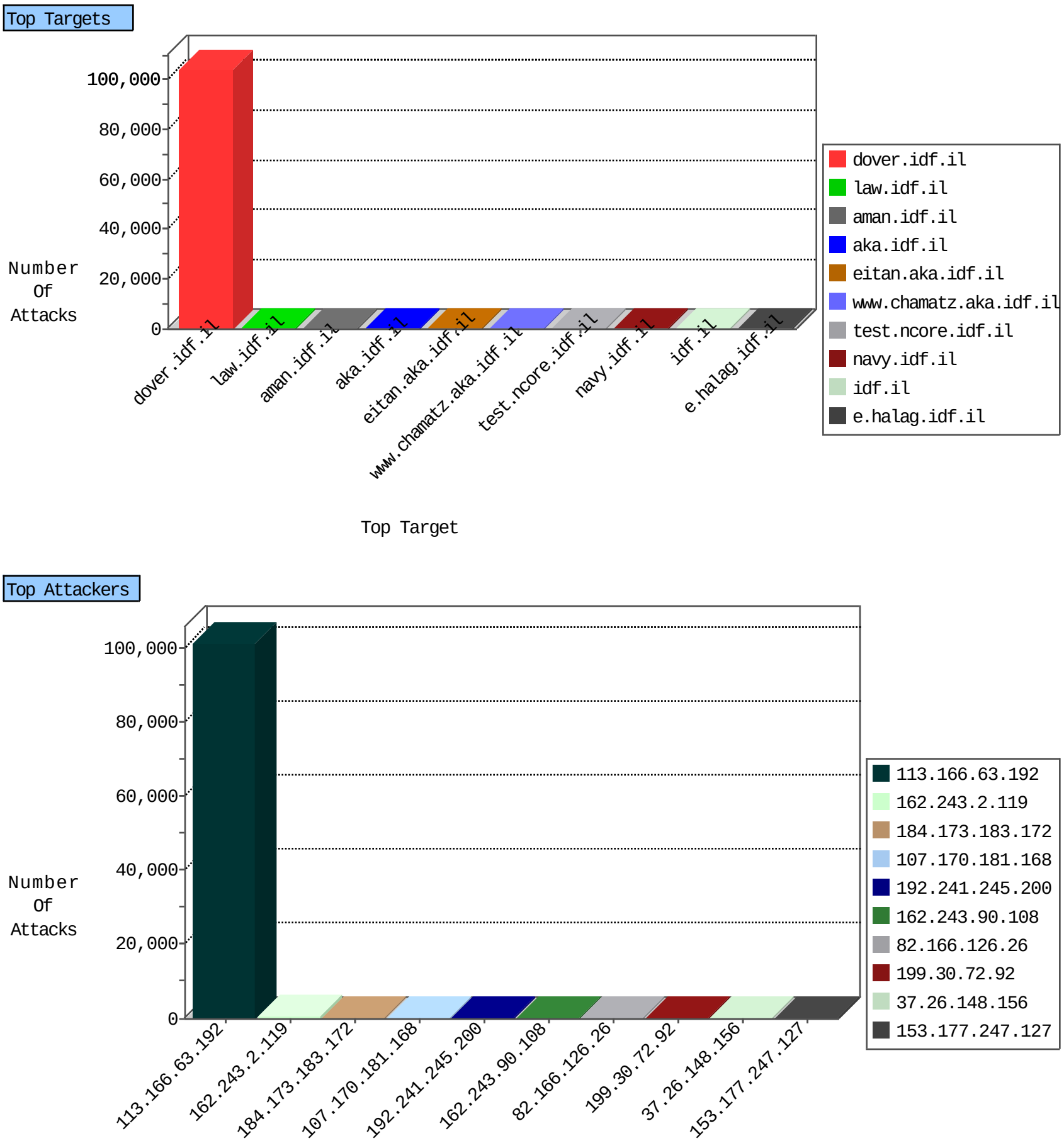
04-21-2015-04:03:02 to 04-21-2015-05:03:02

IDF Under Attack
04-21-2015-04:03:02



04-21-2015-04:03:02 to 04-21-2015-05:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.93	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	193
66.249.79.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
204.42.253.130	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1

04-21-2015-04:03:02 to 04-21-2015-05:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	341
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	49
90.61.124.227	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	15
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1

04-21-2015-04:03:02 to 04-21-2015-05:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	26
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
88.249.106.23	Turkey	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.60.229.45		147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.45		147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.45		147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.45		147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.45		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.60.229.45		147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.45		147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.45		147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.45		147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.45		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-21-2015-04:03:02 to 04-21-2015-05:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
113.166.63.192	Vietnam	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	101479
162.243.2.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	454
107.170.181.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	254
192.241.245.200	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	143
162.243.90.108	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	121
82.166.126.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	112
199.30.72.92	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	69
37.26.148.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	68
153.177.247.127	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
85.72.40.4	Greece	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
140.139.231.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
66.249.79.66	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
73.39.233.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
46.19.86.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
75.115.10.138	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
66.249.79.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
70.199.65.157	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
66.249.79.58	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
46.19.86.138	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
74.65.228.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
12.167.51.34	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
31.116.149.50	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
184.107.255.178	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
70.54.87.155	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
174.234.196.92	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
70.194.72.235	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
75.132.213.140	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
192.34.109.234	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
162.247.73.206		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
212.174.166.140	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
174.234.196.92	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	7
174.234.196.92	United States	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	7
50.190.221.205	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
134.191.232.71	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
181.64.192.188	Peru	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
73.172.169.250	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
174.234.196.92	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	5
46.116.211.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
157.55.39.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5

04-21-2015-04:03:02 to 04-21-2015-05:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	11
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	10
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	7
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	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
66.249.73.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
141.212.121.160	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.65.30	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
202.46.50.160	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
66.249.79.112	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18775-he/dover.aspx	Block	1
45.55.134.10		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/navmenu/undefined	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
202.46.63.115	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.73.219	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/military-police/	Block	1
157.55.39.44	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/	Block	1
66.249.67.143	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-contacts.stm	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/935	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
180.76.5.148	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.79.96	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-15315-en/dover.aspx	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.148	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
82.80.133.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21240-he/idfgdover.aspx/	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
180.76.5.154	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
66.249.79.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-13552-en/dover.aspx	Block	1

04-21-2015-04:03:02 to 04-21-2015-05:03:02