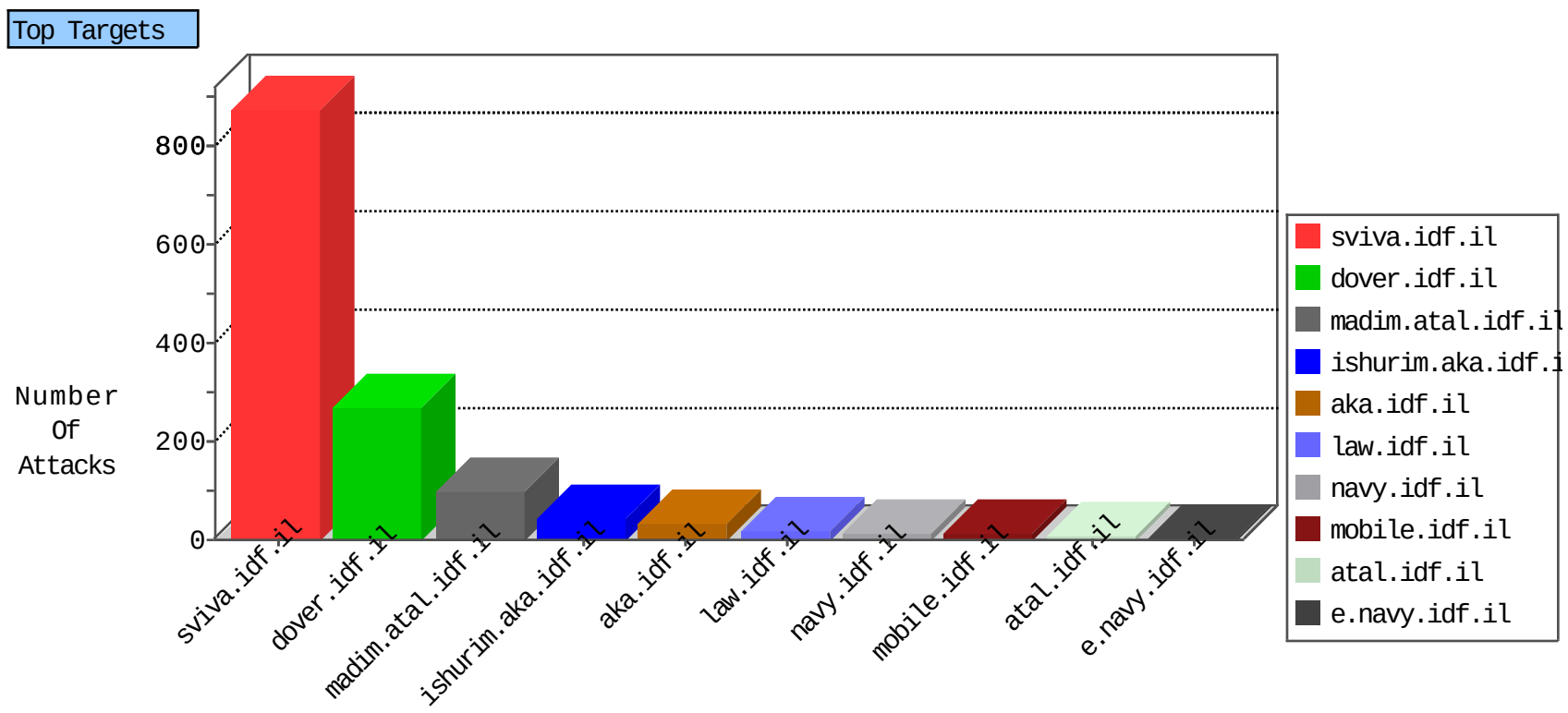
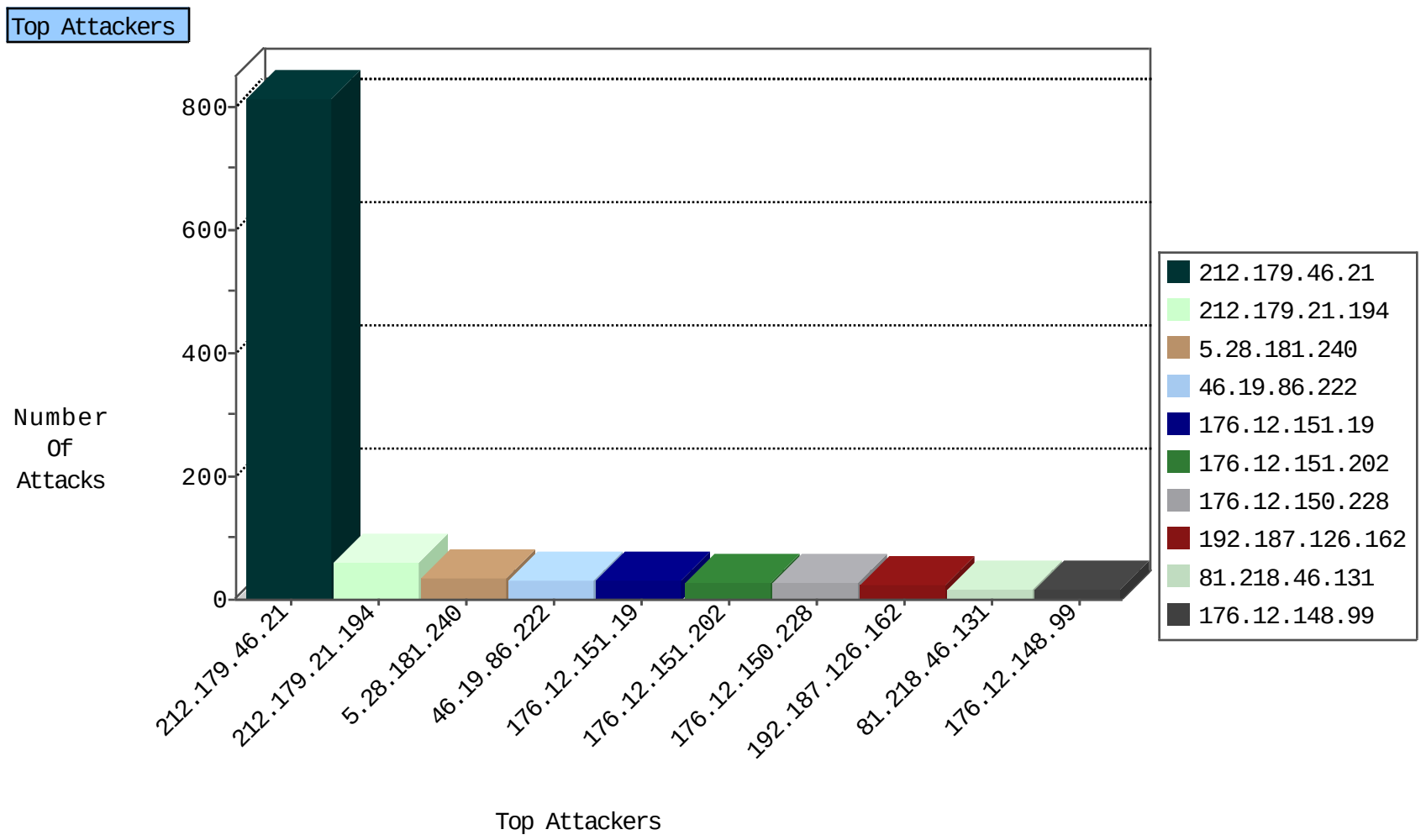
04-02-2015-08:03:09 to 04-02-2015-09:03:09

IDF Under Attack
04-02-2015-08:03:09

Top Targets



Top Attackers



04-02-2015-08:03:09 to 04-02-2015-09:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
5.28.181.240	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	411
31.168.136.9	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
89.248.160.196	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
46.174.83.38	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.196	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
46.28.204.46	Switzerland	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
198.48.92.104	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.196	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
46.174.83.38	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.196	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.196	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
46.174.83.38	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.196	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

04-02-2015-08:03:09 to 04-02-2015-09:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
91.200.12.52	Ukraine	147.237.77.216	dover.idf.il	C1000196: HTTP: Block admin login to gov.il sites	Block	1
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
91.200.12.52	Ukraine	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1

04-02-2015-08:03:09 to 04-02-2015-09:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.240.144.66	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
58.65.152.129	Pakistan	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.117.158.142	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.35	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.138.9.51	Germany	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.161	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
176.12.148.19	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
84.228.87.182	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.156.120	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.164.86	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.239.3	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
222.69.94.13	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.218.245	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.168	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.161	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
176.12.140.160	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.102.145.121	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

04-02-2015-08:03:09 to 04-02-2015-09:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.46.21	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	813
212.179.21.194	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	61
176.12.151.19	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.148.99	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
81.218.46.131	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
64.233.173.151	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
176.12.145.145	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
64.233.173.161	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
65.55.210.124	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
5.22.129.198	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	8
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
192.187.126.162	United States	147.237.76.86	navy.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	7
192.187.126.162	United States	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	7
213.55.107.75	Ethiopia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.139.158	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
80.74.116.135	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.64.166.245	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
188.165.15.198	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.64.166.245	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
176.12.140.211	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.141.197	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
37.247.36.102	Netherlands	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.86	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
195.200.205.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
61.135.190.201	China	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
31.186.228.170	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
207.46.13.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
155.94.254.133		147.237.0.35	akaws.idf.il		drop	drop	2
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
38.99.240.148	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
141.212.121.154	United States	147.237.0.35	akaws.idf.il		drop	drop	1
2.54.177.181	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
82.81.193.82	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
74.82.47.6	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
61.135.190.197	China	147.237.0.35	akaws.idf.il		drop	drop	1
91.227.164.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
80.179.114.27	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.19	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.228.230.32	Bulgaria	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
212.143.138.230	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
176.12.151.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
176.12.150.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
176.12.144.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
192.187.126.162	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.187.126.162	Block	6
17.142.152.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.114	Block	5
17.142.151.198	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.198	Block	4
17.142.151.243	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
81.218.0.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.0.130	Block	3
176.12.144.19	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	2
17.142.151.243	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.243	Block	2
84.108.233.206	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
17.142.151.198	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.52.58.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	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
207.46.13.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.117.62.87	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
113.91.166.126	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
81.218.0.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
216.218.206.67	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
188.138.17.205	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.75.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/march/6.stm	Block	1
176.12.137.103	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
17.142.152.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/048.stm	Block	1
17.142.151.71	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
89.234.68.86	Ireland	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/modiin/default.aspx	Block	1
77.125.167.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
192.187.126.162	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	1
61.135.190.68	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
113.174.191.6	Vietnam	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/1354-he/cogat.aspx	Block	1
222.70.169.100	China	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0304-2.stm	Block	1
66.249.75.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	1
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.141.170	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
91.200.12.52	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
61.135.190.70	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/scriptresource.axd	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/statistics/chiefs.stm	Block	1
17.142.151.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0817-1.stm	Block	1
85.64.150.105	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/faq.aspx	None	1
188.165.15.238	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9237-he/refuah.aspx	Block	1
38.99.240.148	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
176.12.141.197	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il//categorytemplates/listchilddocuments/1071	Block	1
107.168.64.186	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1563-en/dover.aspx/rk=0/rs=ljkgko_v2qmfqdfelm4yqyr76mq-	Block	1
80.179.225.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
192.187.126.162	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/manage/fckeditor/editor/	Block	1
61.135.190.200	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
157.55.39.156	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1

04-02-2015-08:03:09 to 04-02-2015-09:03:09