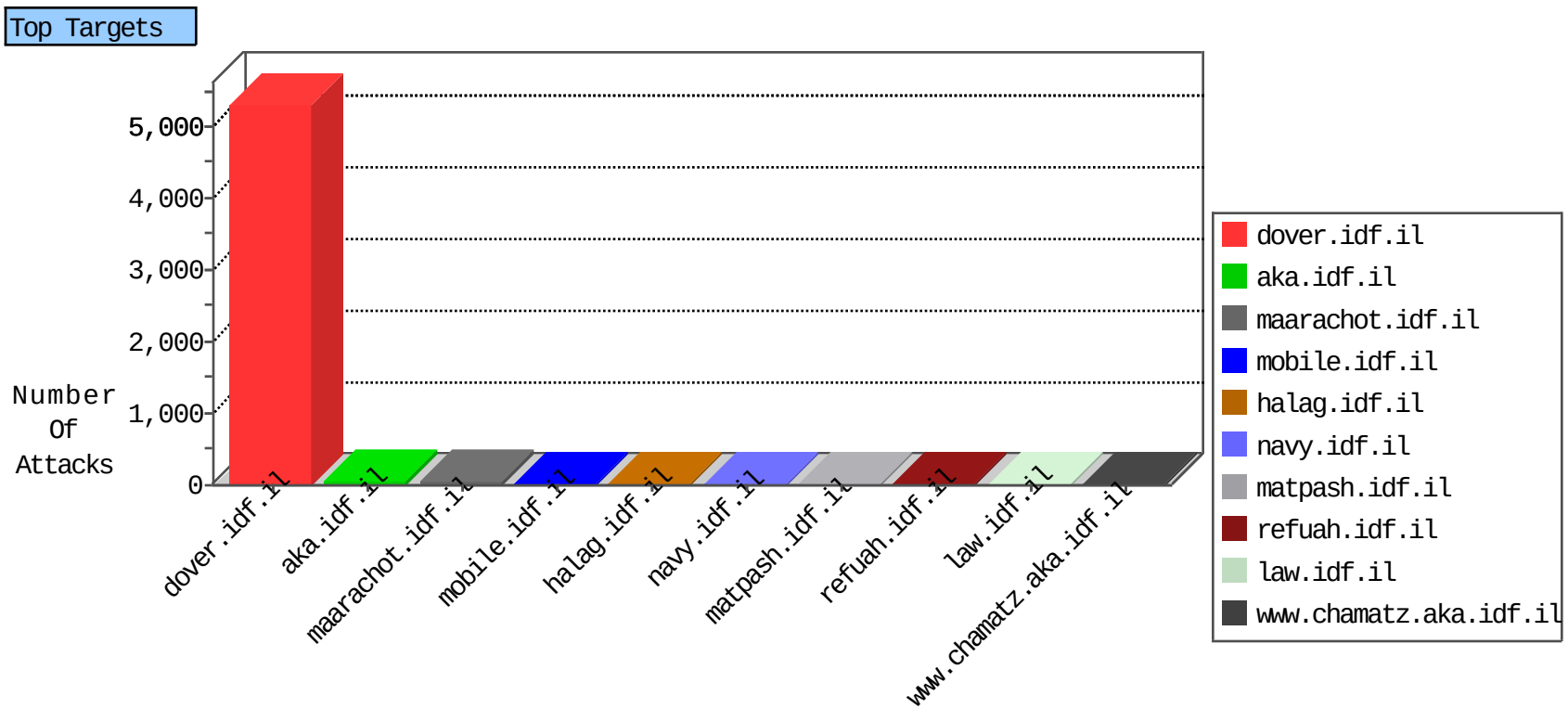
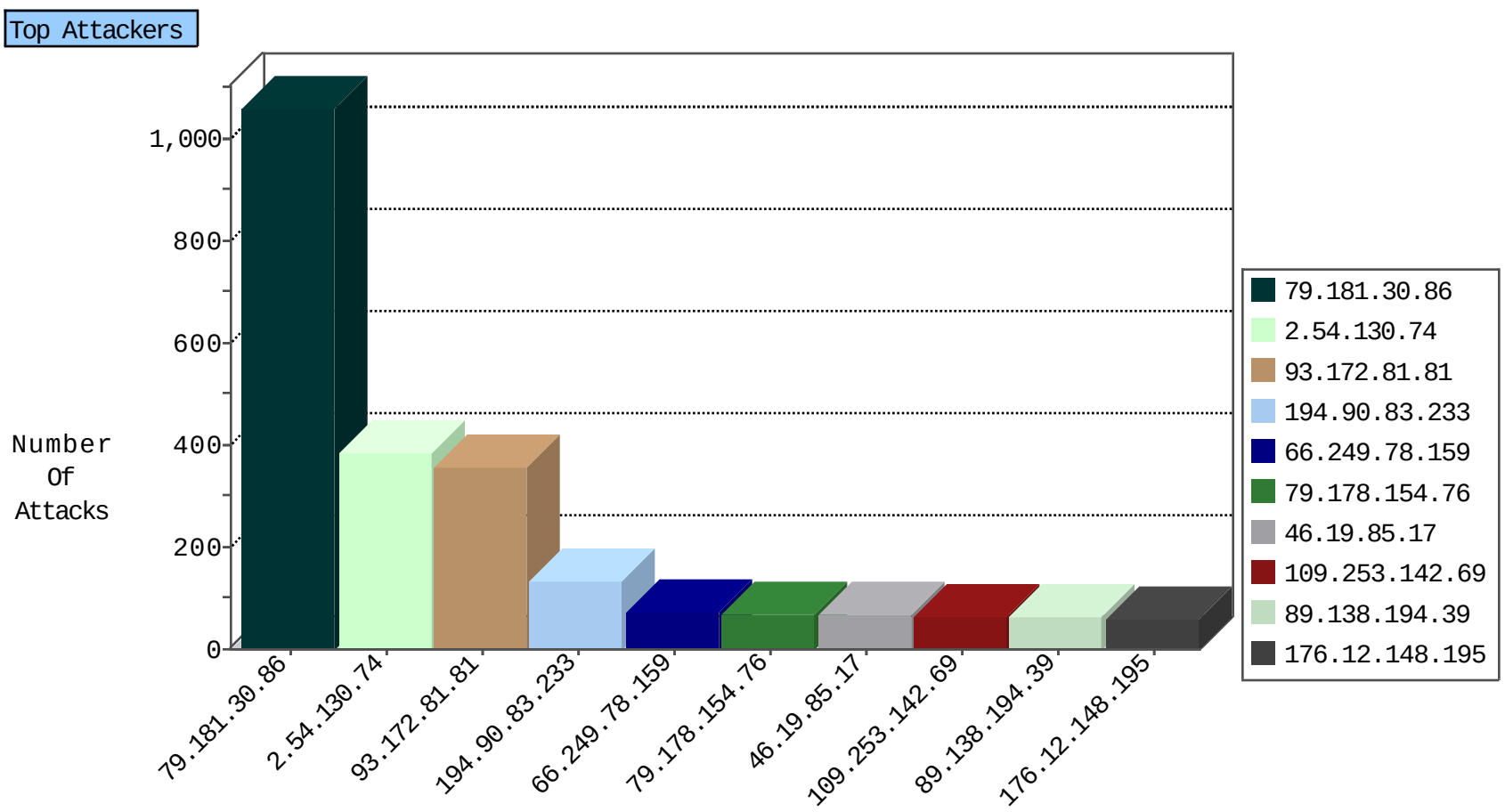
04-19-2015-07:03:03 to 04-19-2015-08:03:03

IDF Under Attack
04-19-2015-07:03:03



Top Target



Top Attackers

04-19-2015-07:03:03 to 04-19-2015-08:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	657
194.90.83.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
109.64.103.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
193.242.218.6	Switzerland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
82.166.140.117	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
95.172.79.244	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-19-2015-07:03:03 to 04-19-2015-08:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.64.168.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
109.65.27.5	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.26.147.233	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1

04-19-2015-07:03:03 to 04-19-2015-08:03:03

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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.212	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.156	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.190.163	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
216.178.244.38	United States	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.147.56.190	Switzerland	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
200.107.233.92	Honduras	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.63.178.190	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
59.63.178.190	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	1
216.178.244.38	United States	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.67	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
212.147.56.190	Switzerland	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
212.147.56.190	Switzerland	147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.63.178.190	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.63.178.190	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1

04-19-2015-07:03:03 to 04-19-2015-08:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.181.30.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1061
2.54.130.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	383
93.172.81.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	355
194.90.83.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	128
79.178.154.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
46.19.85.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
176.12.148.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
194.9.253.237	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
89.138.194.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
62.0.102.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
2.54.44.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
108.49.197.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
149.88.82.254	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
173.192.170.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
213.151.32.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
212.143.191.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
5.29.64.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
2.52.58.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	43
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
193.34.57.101	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
109.253.146.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.19.85.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
46.120.231.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
109.253.131.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
109.253.142.69	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
176.12.143.235	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
46.19.85.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
2.52.52.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
95.86.125.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
147.236.238.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
109.253.142.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
168.63.137.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
37.26.147.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
37.26.147.158	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
77.127.147.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
176.12.150.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
109.253.157.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
46.19.85.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
37.26.147.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
157.55.39.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
176.12.136.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
62.0.101.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
79.170.54.64	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22

04-19-2015-07:03:03 to 04-19-2015-08:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.87.95	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
79.176.134.118	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
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	4
118.123.8.135	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 118.123.8.135	Block	4
37.26.148.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.177.115.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.66.38.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
2.54.177.52	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.134.118	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.176.134.118	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/bi1.stm	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/gene ral.aspx	Block	1
54.157.198.18	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx	Block	1
80.246.130.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0208-2.stm	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/maabada.stm	Block	1
188.165.15.27	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.27	Block	1
109.253.132.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.170.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
62.219.238.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter c... in aka.idf.il/miluim/templates/inner.asp	None	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
118.123.8.135	China	147.237.77.170	maarachot.idf.il	Admin Blocking	Block	1
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-id.stm	Block	1
66.249.64.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
176.12.138.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
89.139.30.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl01 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.127.210.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
37.26.147.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
79.177.136.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ie-index02.stm	Block	1
66.249.64.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
176.12.151.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
93.173.28.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.253.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6264-he/patzar.aspx	Block	1
79.179.120.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.81.233	Israel	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../favicon.ico	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
180.76.6.37	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/clientscripts/{1}	Block	1

04-19-2015-07:03:03 to 04-19-2015-08:03:03