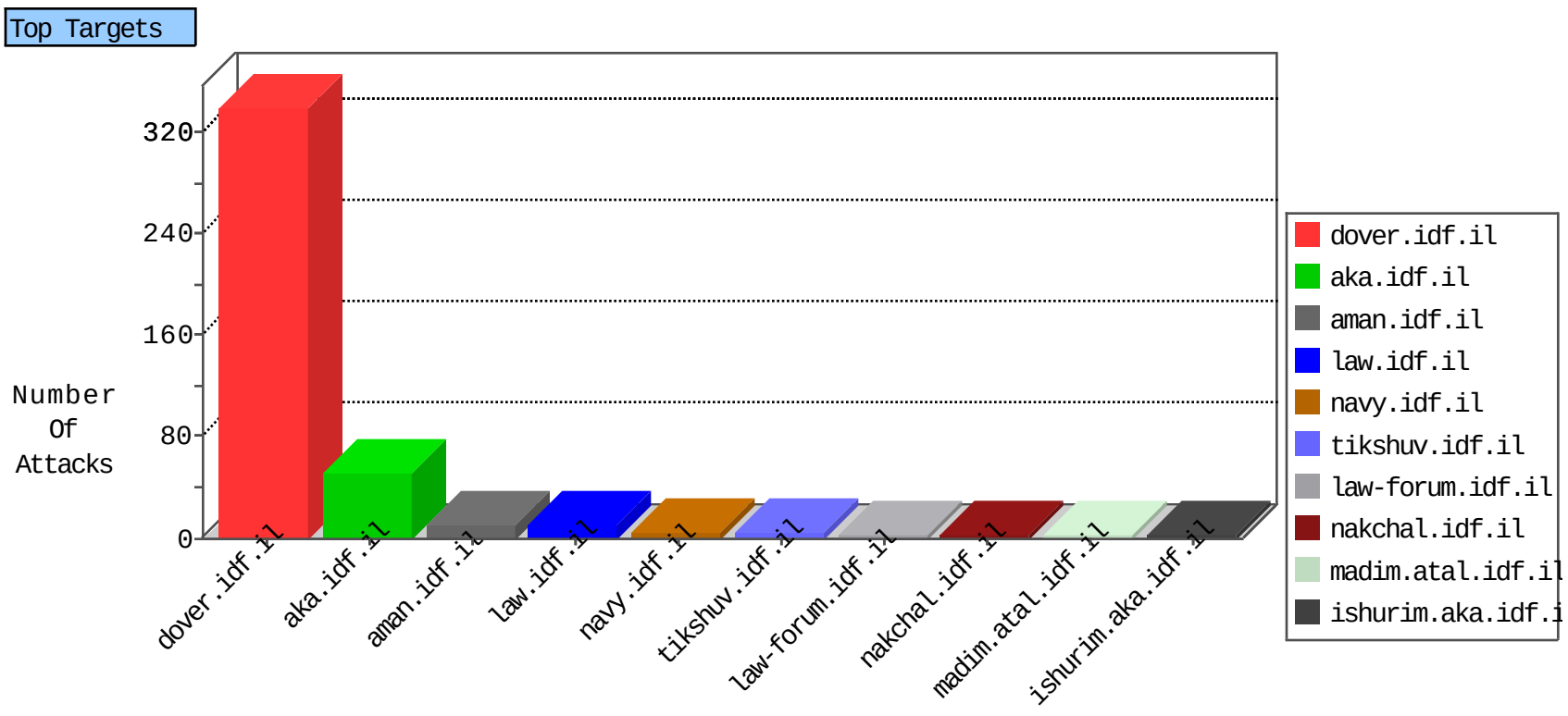
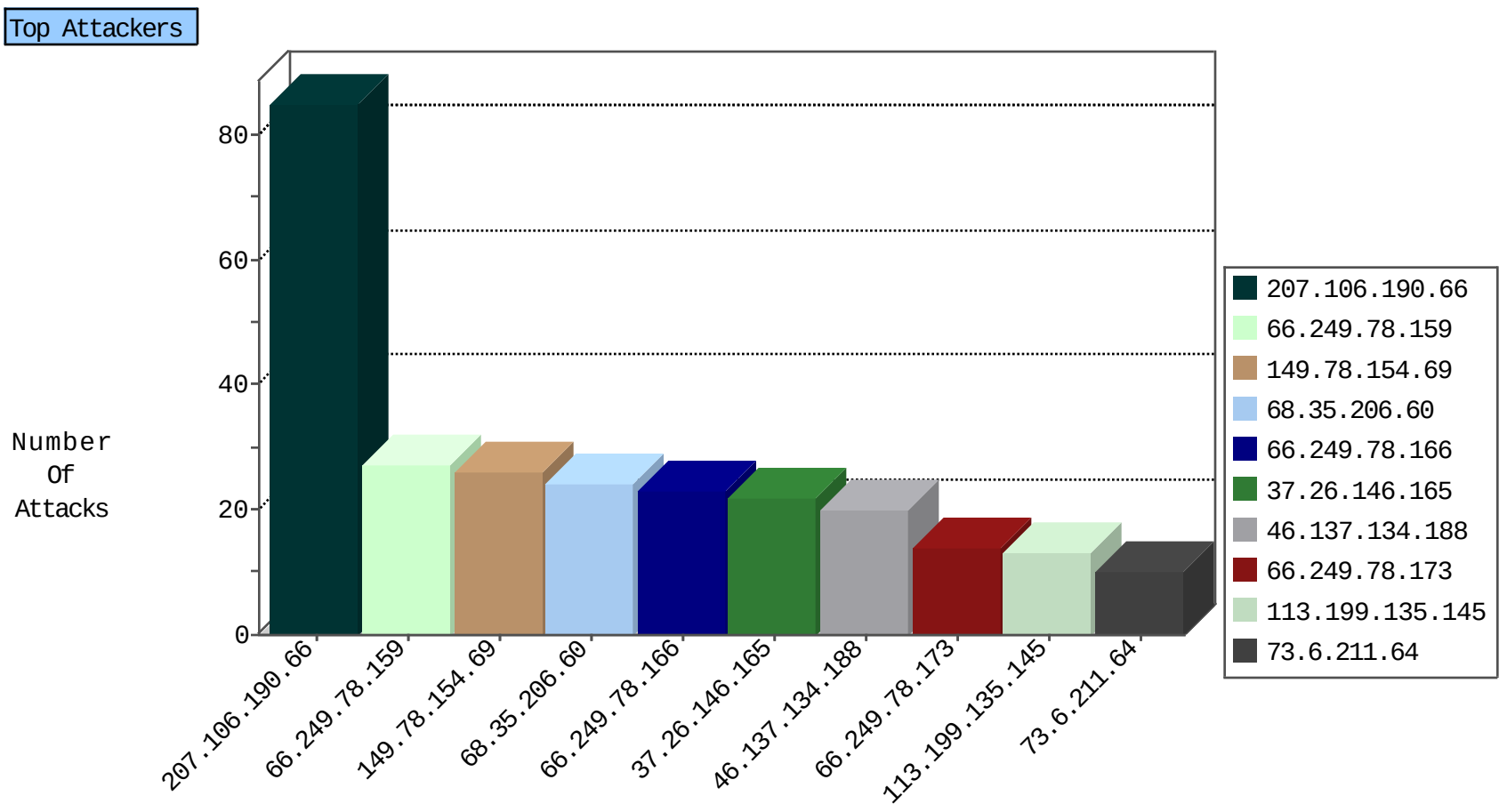
05-06-2015-05:03:02 to 05-06-2015-06:03:02

IDF Under Attack
05-06-2015-05:03:02

Top Targets



Top Attackers



05-06-2015-05:03:02 to 05-06-2015-06:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.156	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2104
220.181.108.82	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	101
74.82.47.3	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.216.41	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

05-06-2015-05:03:02 to 05-06-2015-06:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
85.25.43.94	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	2
37.46.39.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.i	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
36.231.145.10	Taiwan	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
101.251.236.90	China	147.237.76.30	himush.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
36.231.145.10	Taiwan	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
112.111.189.8	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
89.248.160.192	Netherlands	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
89.248.160.192	Netherlands	147.237.0.35	akaws.idf.il	DVRep_P-N_40-59	Permit	1

05-06-2015-05:03:02 to 05-06-2015-06:03:02

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	5
66.249.64.148	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.245	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.208.209.74	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	1
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
66.249.73.217	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
221.235.189.245	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
157.55.39.248	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
80.82.78.27	Netherlands	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1

05-06-2015-05:03:02 to 05-06-2015-06:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
68.35.206.60	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
37.26.146.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
207.106.190.66	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
113.199.135.145	Nepal	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
131.194.104.100	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
85.114.106.243	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
73.6.211.64	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
68.180.229.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
5.102.254.158	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
188.165.15.99	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.64.178	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
73.6.211.64	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	2
66.249.65.65	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
37.46.39.17	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
73.6.211.64	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
197.237.112.175	Kenya	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
65.19.138.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
37.46.39.17	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
73.6.211.64	United States	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	2
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
77.125.150.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.220.156.118	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.78.95	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	1
77.126.90.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
67.183.70.127	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
66.249.78.95	Israel	147.237.77.216	dover.idf.i	Unexpected post SYN packet - RST or SYN expected	drop	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
84.228.227.39	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
113.199.135.145	Nepal	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	1
84.228.227.39	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.78.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
173.68.9.153	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
113.199.135.145	Nepal	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	1
66.220.156.116	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
69.30.240.46	United States	147.237.0.33	idf.il		drop	drop	1
66.249.78.95	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	1
177.16.219.239	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
207.106.190.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.106.190.66	Block	64
207.106.190.66	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
32.215.162.246	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
112.90.231.100	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
66.249.65.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//giyus/forum/asp/showforum.asp	Block	1
157.55.39.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/contactus/www.idf.il/1395-en/dover.aspx forcerecrawl: 0	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
66.249.73.217	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/kkkkkkk=166321a5kkkkkkk_166321a5	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
66.249.65.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;amp;catId in www.aka.idf.il/giyus/general/default.asp	None	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/994-8121-he/hamaz.aspx	Block	1
180.76.6.55	China	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.65.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19781-he/dover.aspx	Block	1
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
180.76.6.57	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Unknown Parameter m in www.aka.idf.il/main/drushim/drushim/general.aspx	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/armored7.stm	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.190	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/general/general.aspx	Block	1
79.178.60.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17558-he/dover.aspx	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
203.198.29.198	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
207.106.190.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/text/javascript	Block	1
66.249.67.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	1