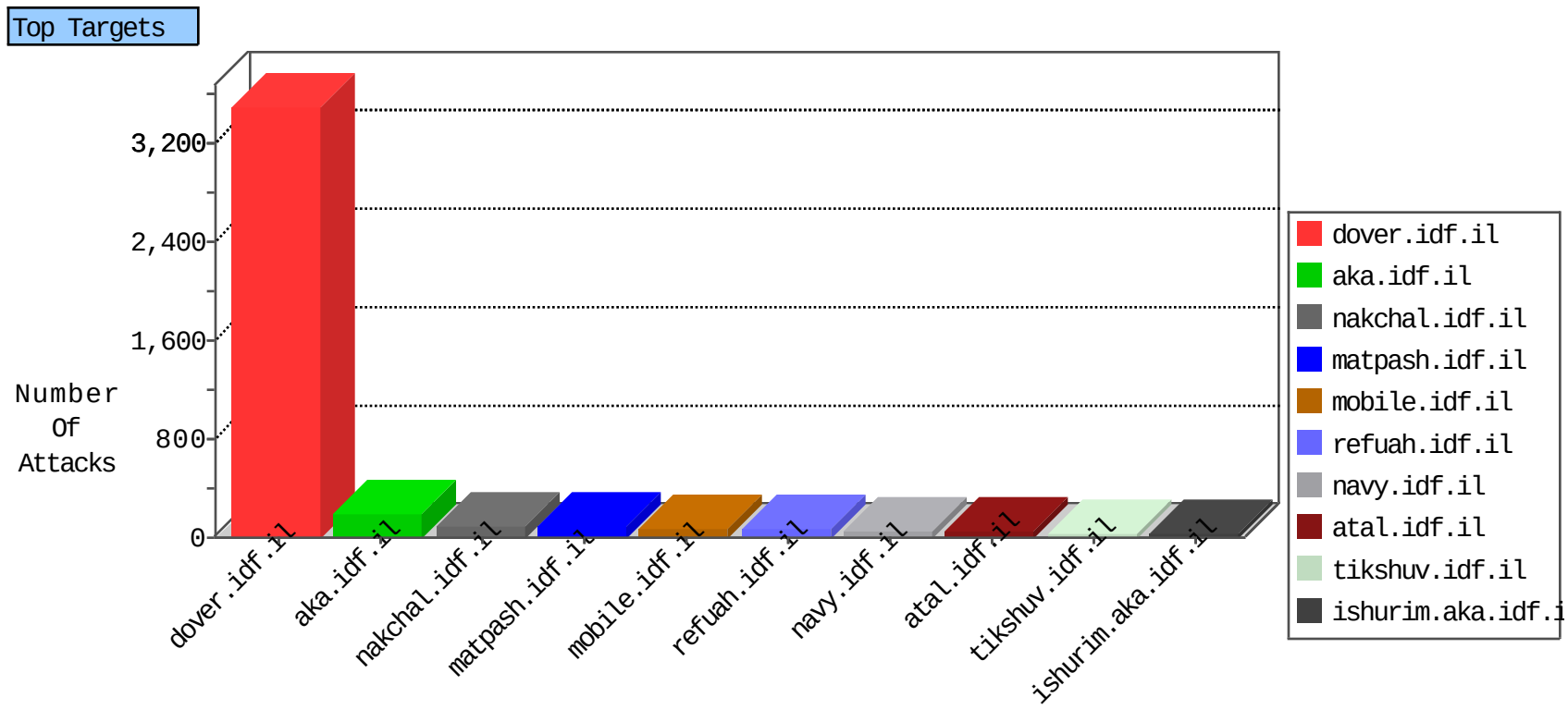
10-22-2015-01:07:21 to 10-22-2015-02:07:21

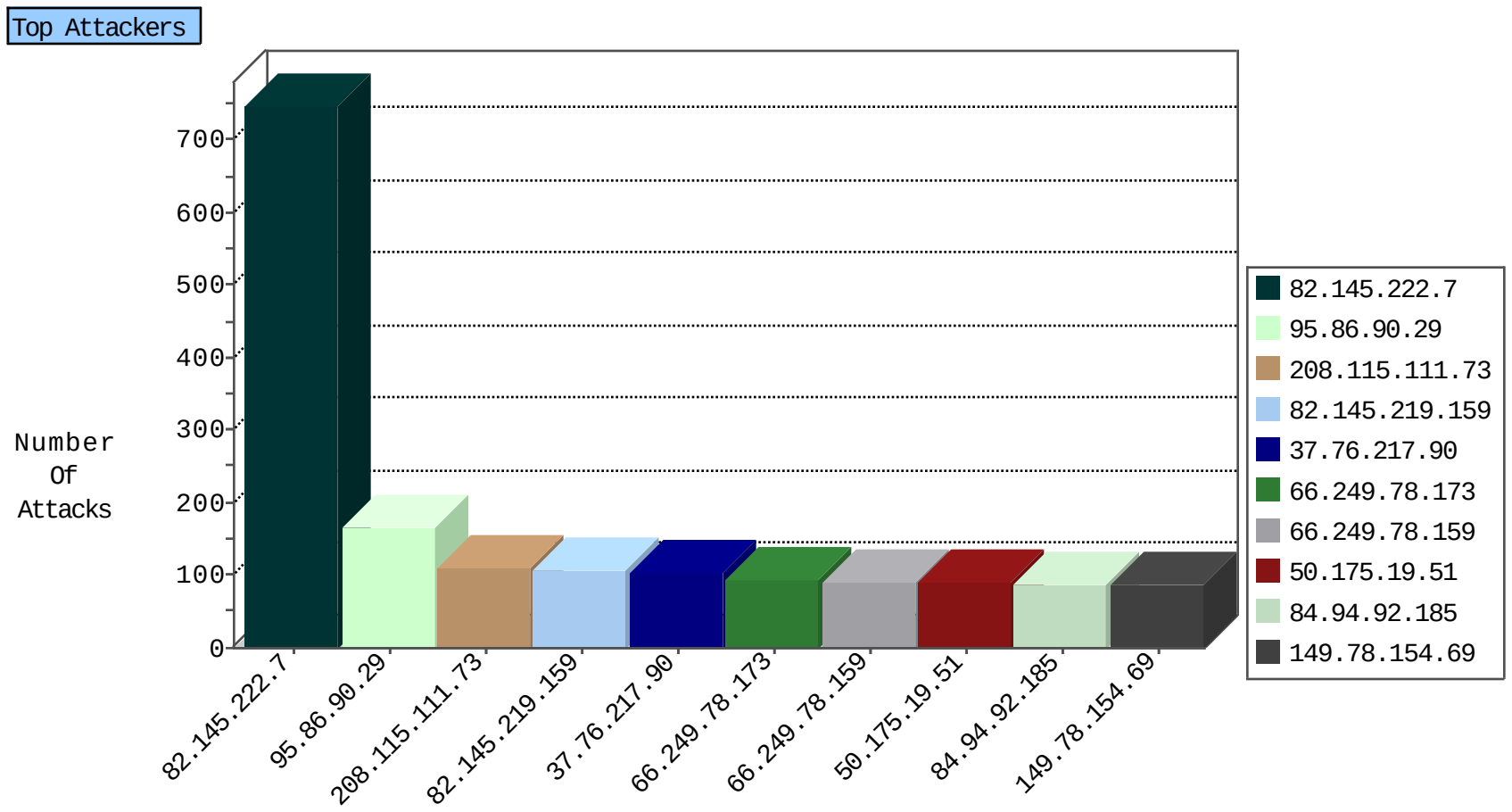
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-22-2015-01:07:21 to 10-22-2015-02:07:21

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.8.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1646
50.175.19.51	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	942
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	434
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	368
220.181.108.100	China	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	244
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	213
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
2.54.45.15	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
66.249.67.59	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
66.102.8.178	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
96.244.132.13	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
197.27.75.124	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-22-2015-01:07:21 to 10-22-2015-02:07:21

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.70	United States	147.237.76.42	refuah.idf.il	C1000106: HTTP: majestic bot	Block	1

10-22-2015-01:07:21 to 10-22-2015-02:07:21

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
176.13.22.68	147.237.76.86	Israel	navy.idf.il	INDICATOR-SCAN myscan	2
176.13.22.68	147.237.76.86	Israel	navy.idf.il	GPL SCAN myscan	2
111.93.198.54	147.237.77.61	India	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
103.232.35.93	147.237.76.202	Hong Kong	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
198.199.65.204	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.114.137.161	147.237.77.74	Germany	law.idf.il	ET SCAN NMAP -sS window 3072	1
185.120.126.49	147.237.72.166		aka.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
85.114.137.161	147.237.77.74	Germany	law.idf.il	ET SCAN NMAP -f -sS	1
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
169.229.3.91	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
168.187.246.41	147.237.77.227	Kuwait	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
139.162.144.227	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.77.61	India	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
103.232.35.93	147.237.76.202	Hong Kong	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
103.232.35.93	147.237.76.202	Hong Kong	e.halag.idf.il	ET SCAN NMAP -f -sS	1
85.114.137.161	147.237.77.74	Germany	law.idf.il	ET SCAN NMAP -sS window 2048	1
185.100.85.71	147.237.76.30		himush.idf.il	ET SCAN NMAP -sS window 1024	1
78.24.220.21	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.79.188.5	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
168.187.246.41	147.237.77.227	Kuwait	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
14.134.164.60	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.187.246.41	147.237.77.227	Kuwait	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
139.162.141.72	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1

10-22-2015-01:07:21 to 10-22-2015-02:07:21

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.222.7	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	746
95.86.90.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	167
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
82.145.219.159	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
37.76.217.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
84.94.92.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
1.144.96.76	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
50.175.19.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
5.254.65.125	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
149.78.145.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
150.108.157.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
5.43.204.36	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
109.66.177.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
37.142.239.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.84.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
176.13.11.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.84.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
5.170.34.80	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
185.88.24.245		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
84.108.75.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
86.91.185.105	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
31.223.176.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
79.255.8.193	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
192.116.162.182	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	16
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.84.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

10-22-2015-01:07:21 to 10-22-2015-02:07:21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	84
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
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	56
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	56
84.228.32.86	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	42
79.177.194.5	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	42
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	28
79.177.194.5	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.177.194.5	Block	28
149.78.221.205	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.221.205	Block	28
149.78.221.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/selectusertype.asp	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/16641.jpg	Block	14
41.238.187.142	Egypt	147.237.77.176	matpash.idf.il	PHP Attempt	Block	14
79.178.36.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	14
68.101.96.250	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	14
157.55.39.9	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
77.237.146.28	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
202.102.99.103	China	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../shared/clientscripts/sidebar/sidebar.js	Block	14
41.238.187.142	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	14
79.180.113.73	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
66.249.67.245	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/haredim/contactus.aspx	Block	14
157.55.39.36	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/	Block	14
77.237.146.28	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
207.46.13.119	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.64.205	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	14
66.249.67.253	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.165.15.138	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	14
37.26.149.135	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_bottom.asp	Block	14

10-22-2015-01:07:21 to 10-22-2015-02:07:21