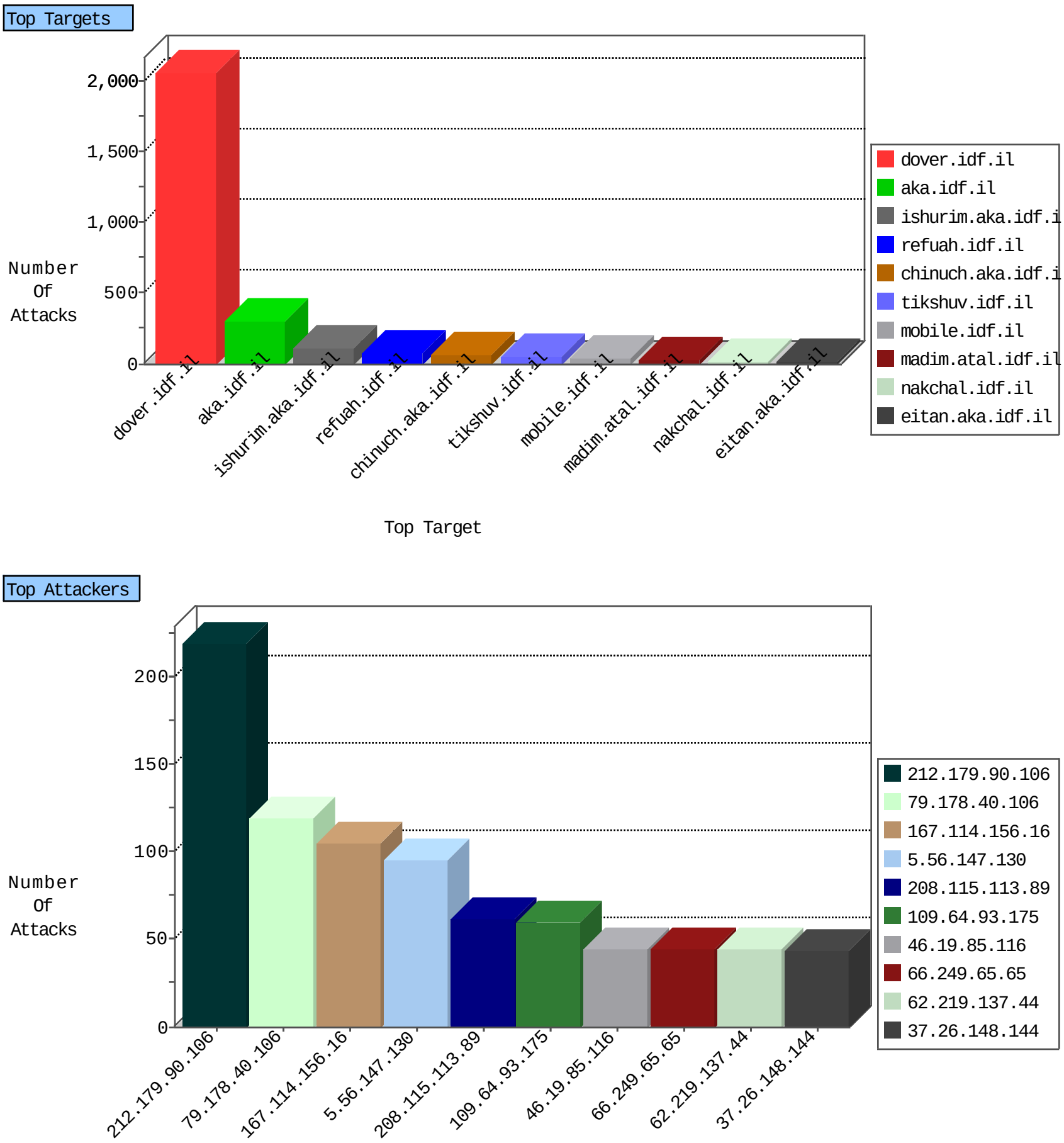
05-04-2016-09:04:07 to 05-04-2016-10:04:07

IDF Under Attack
Daily Report



05-04-2016-09:04:07 to 05-04-2016-10:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.198.62.190	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5886
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4547
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2490
94.102.49.116	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
81.218.56.125	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
94.102.49.116	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

05-04-2016-09:04:07 to 05-04-2016-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.143.180.166	United States	147.237.0.19	madim.atal.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

05-04-2016-09:04:07 to 05-04-2016-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
104.219.238.10	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
76.181.249.213	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
5.56.147.130	147.237.77.216	Denmark	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
104.128.144.131	147.237.0.33	Canada	idf.il	ET SCAN NMAP -sS window 3072	1
79.177.172.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
76.181.249.213	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
2.53.171.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

05-04-2016-09:04:07 to 05-04-2016-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	219
79.178.40.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
5.56.147.130	Denmark	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	78
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
37.26.148.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.85.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
24.217.189.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	31
104.131.147.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
109.64.93.175	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.86.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.253.136.237	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
87.71.22.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
5.56.147.130	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.26.146.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.94.171.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.120.49.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.179.57.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.119	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
65.55.210.210	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.40.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
203.81.85.2	Myanmar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.125.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
84.228.252.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.130.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.39.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.19.191.224	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
82.80.198.164	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.199.165	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
2.53.46.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	6
131.253.25.231	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	6
176.13.7.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.52.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.214	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.15.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.201.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.27	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.201.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.199.165	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
37.115.184.150	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	2
2.53.46.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	2
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.232.27.5	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
2.53.5.44	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
87.69.39.95	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
212.150.65.209	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.116.52.99	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.148.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
203.127.58.235	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.73.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
2.53.39.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.231.61	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
216.218.206.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
46.117.45.175	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1653-he/refuah.aspx	Block	1
109.253.199.165	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.199.165	Block	1
37.26.149.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.81.193.82	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.73.189	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1399-he/atal.aspx	Block	1
203.127.96.231	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.178.24.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
219.74.239.176	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.76.15.22	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	1
46.120.49.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.94.121.159	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
203.127.96.249	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.172	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1653-he/refuah.aspx parameter searchText	Block	1
132.74.210.255	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
104.131.147.112	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
220.255.148.146	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1