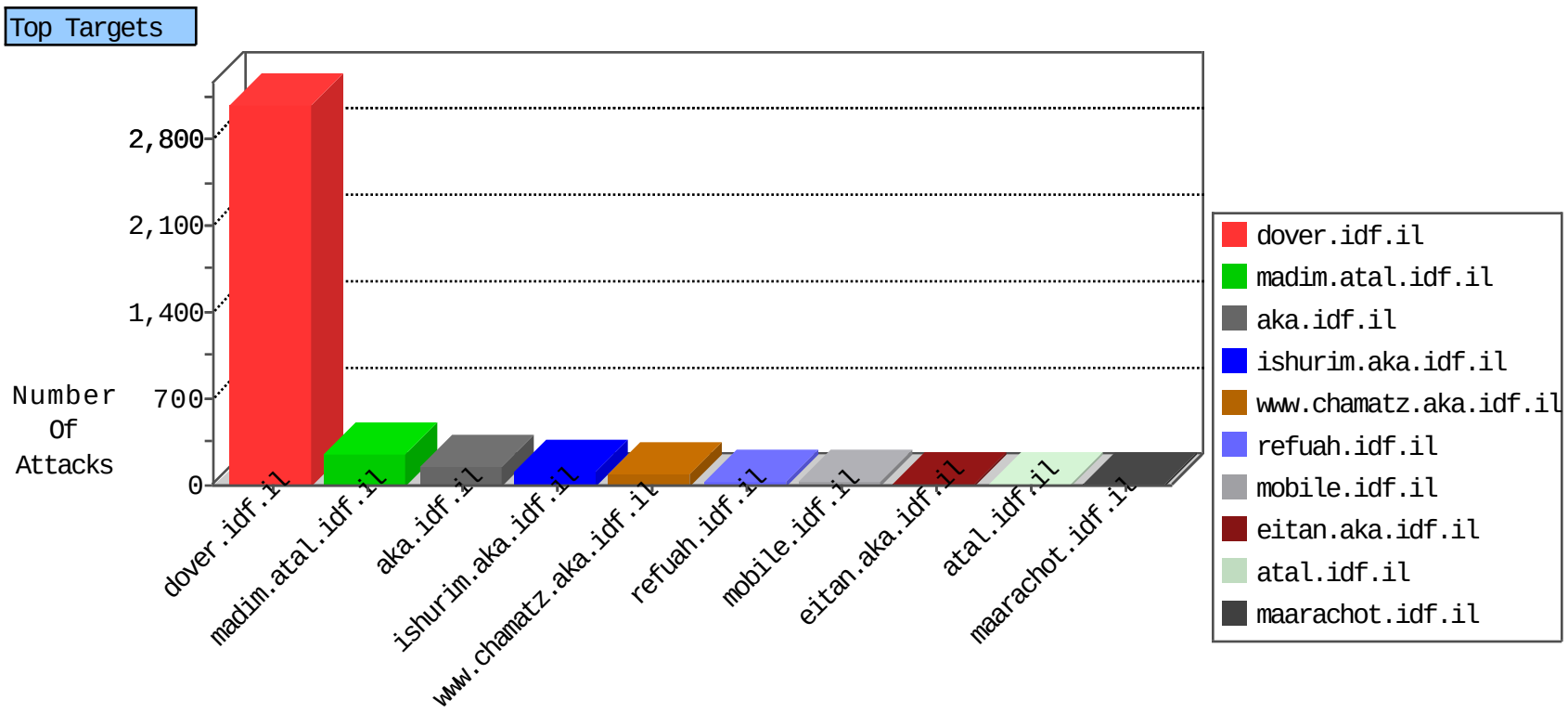
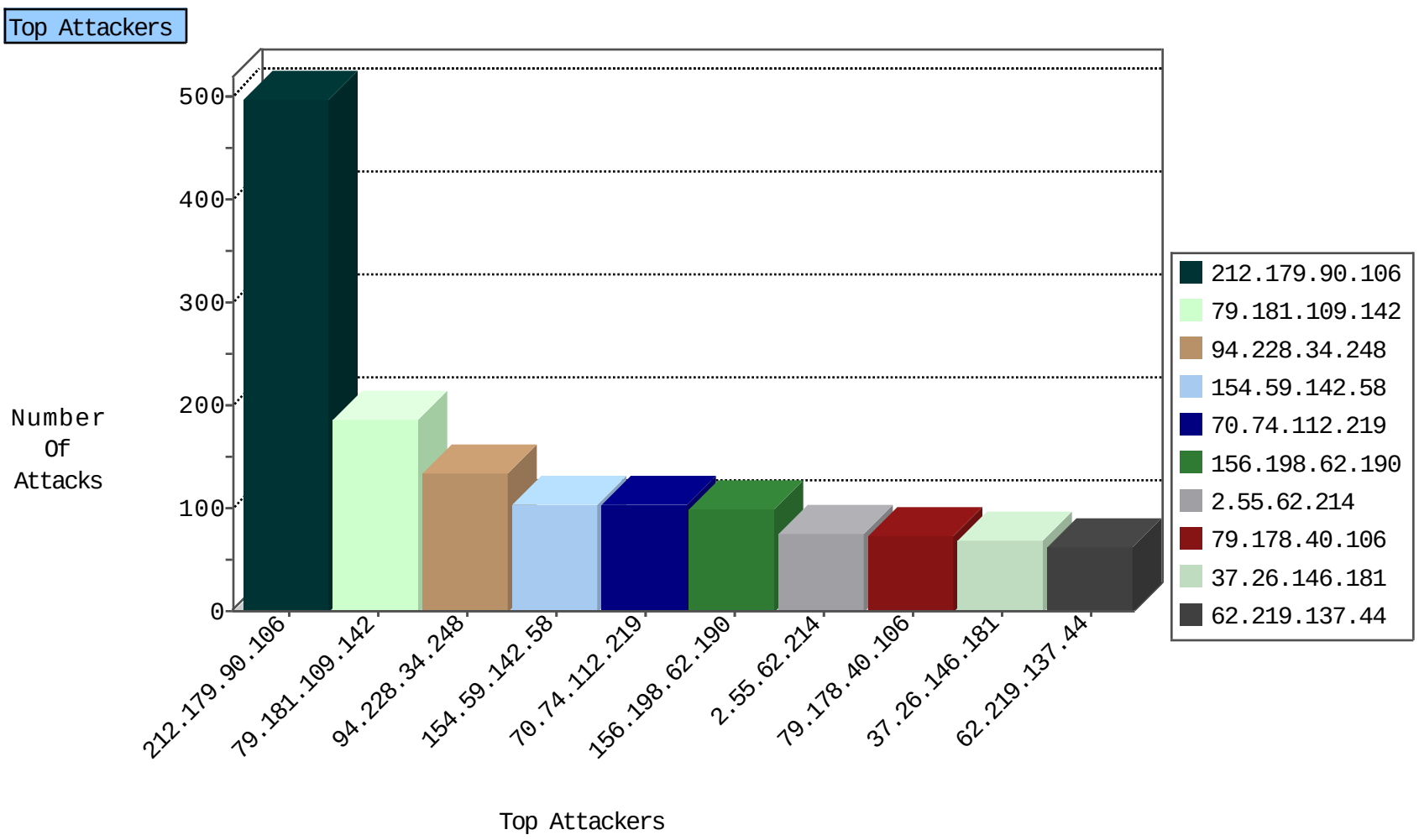
05-04-2016-08:04:06 to 05-04-2016-09:04:06

IDF Under Attack Daily Report





05-04-2016-08:04:06 to 05-04-2016-09:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6448
156.198.62.190	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	421
212.235.77.210	Israel	147.237.76.42	refuah.idf.il	ICMP-Frag-Needed-Storm	drop	13
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
113.123.48.185	China	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.74	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
210.195.113.183	Malaysia	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

05-04-2016-08:04:06 to 05-04-2016-09:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.198.62.190	Egypt	147.237.77.216	dover.idf.i	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2

05-04-2016-08:04:06 to 05-04-2016-09:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.177.214.30	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	4
115.47.12.162	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.214.34.99	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
104.192.0.19	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.230.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.159	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
208.100.26.228	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.53.163.68	147.237.72.166	Israel	aka.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
117.34.70.143	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.214.34.99	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
104.214.34.99	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
104.192.0.19	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.29.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.212	United States	e.dover.idf.il	ET DROP Dshield Block Listed Source	1
180.94.87.162	147.237.0.16	Afghanistan	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

05-04-2016-08:04:06 to 05-04-2016-09:04:06

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	487
79.181.109.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
70.74.112.219	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
154.59.142.58	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	84
79.178.40.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
37.26.146.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
91.231.193.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
134.222.104.250	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
213.57.251.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
156.198.62.190	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
176.13.6.105	Israel	147.237.72.166	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	29
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
65.254.225.176	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
188.120.148.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
82.166.91.198	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
62.219.137.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
178.20.190.114	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.55.26.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
156.198.62.190	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
154.59.142.58	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
79.183.207.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
45.49.135.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
195.50.126.101	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
217.132.149.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
192.115.252.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
91.197.61.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.235.77.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
81.218.251.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.108.233.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
31.154.41.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.181.49.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.79.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.181.65.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.62.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
132.70.66.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
37.26.147.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
156.198.62.190	Egypt	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 156.198.62.190	Block	31
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
176.13.10.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
176.13.21.204	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.21.204	Block	12
2.53.176.97	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.53.176.97	Block	6
176.13.21.204	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
2.53.11.112	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
2.53.154.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.221	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	3
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.185.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.41.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.32.143	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	2
172.56.3.69	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 172.56.3.69	Block	2
62.90.35.105	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.168.175.226	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	2
2.53.12.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.10.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1845-he/dover.aspx-	Block	1
85.250.180.130	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2308.jpg	Block	1
37.26.146.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/schar	Block	1
195.154.199.235	France	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
79.179.139.19	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opmissingperson/mobile	Block	1
2.55.27.127	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/darom/site/he/main.asp	Block	1
130.160.195.8	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsnite/english/0402	Block	1
195.154.199.235	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
176.213.8.3	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/16919.pdf.	Block	1
2.53.0.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.230.120	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
212.235.56.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
172.56.3.69	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	1
80.246.137.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2424.jpg	Block	1
192.115.252.2	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Unknown SSL Session	None	1
24.124.5.101	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	1
212.235.77.210	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.176.97	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.73.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
132.70.66.12	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.126.151.144	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1

05-04-2016-08:04:06 to 05-04-2016-09:04:06