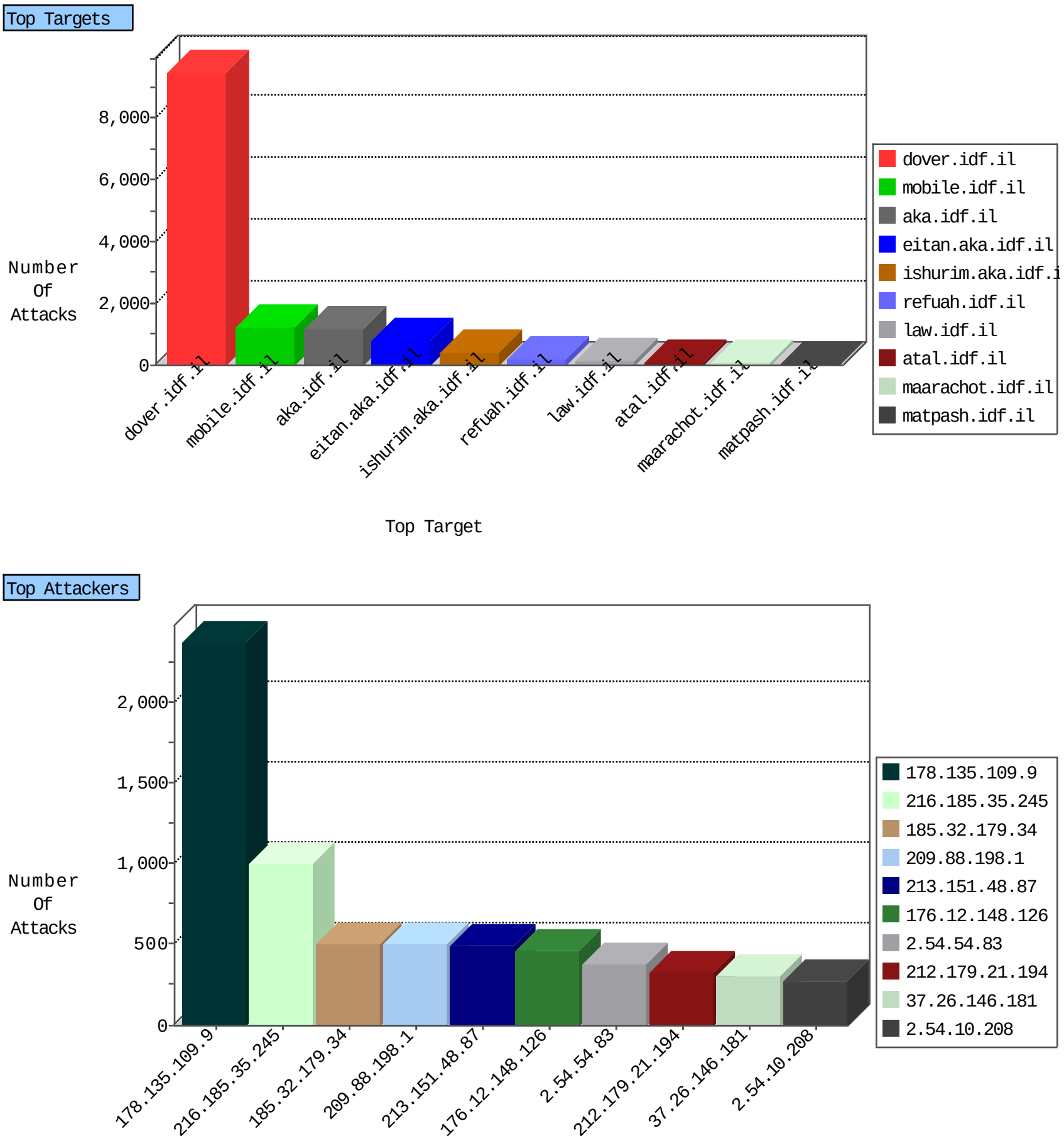
11-01-2015-12:04:05 to 11-01-2015-13:04:05

IDF Under Attack
Daily Report



11-01-2015-12:04:05 to 11-01-2015-13:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.8.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1512
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	376
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	330
80.246.138.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	41
85.65.49.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	41
176.12.141.217	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	40
212.150.171.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
84.94.21.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
2.54.162.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
93.173.22.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
178.135.109.9	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23
109.67.21.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
79.183.60.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
80.246.139.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
79.179.104.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
41.109.57.127	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	11
176.12.151.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
2.54.164.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
37.26.147.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.86.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
216.185.35.245	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.i	Block_Udp_All_Nets	drop	6
46.19.86.69	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.176.136.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.186.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.67.21.56	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
176.106.46.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.117.103.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.12.151.171	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
185.32.179.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.183.56.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.64.246.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.22.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
94.13.184.241	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
91.199.69.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
80.246.136.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.64.130.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
88.103.90.45	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.12.211	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
31.168.81.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.80.17.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.104	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
81.218.37.2	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4

11-01-2015-12:04:05 to 11-01-2015-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.33.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-01-2015-12:04:05 to 11-01-2015-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
192.115.248.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.5.9.227	147.237.0.33	Turkey	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.233.64.64	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN Potential SSH Scan	1
85.65.103.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
217.147.86.8	147.237.76.39	United Kingdom	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
37.26.149.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.101.186.134	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
192.117.12.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.233.64.64	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN Potential SSH Scan	1
94.233.64.64	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
79.177.207.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.123.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.147.86.8	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.134	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1

11-01-2015-12:04:05 to 11-01-2015-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.135.109.9	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2337
216.185.35.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	996
209.88.198.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	499
213.151.48.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	491
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	317
37.26.146.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	309
2.54.10.208	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	276
108.59.8.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	200
37.26.146.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	150
31.168.81.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
89.138.216.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	137
31.154.91.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
82.166.22.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
46.19.86.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
37.26.148.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
109.67.115.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
37.26.146.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
79.176.209.89	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
84.228.8.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
50.118.196.232	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
178.77.185.181	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
88.64.13.246	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
176.13.13.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.86.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
79.178.200.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
81.218.37.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
82.80.28.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
213.151.48.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
100.100.37.123		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
178.79.187.60	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
37.26.146.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.147.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
207.46.13.23	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	22
2.54.159.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.166.137.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.166.24.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.12.151.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
77.125.83.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.34	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	480
176.12.148.126	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	449
95.86.68.149	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
2.54.54.83	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	210
2.54.54.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	165
46.116.167.188	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	90
176.12.142.44	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	60
176.12.151.171	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	60
176.13.12.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
212.199.251.227	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	45
199.203.215.1	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
212.92.237.8	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	30
84.109.32.240	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/drushim	Block	30
37.26.149.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	30
176.12.138.195	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	30
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	30
2.52.7.241	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
91.135.102.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	30
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
31.154.161.250	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 31.154.161.250	Block	30
46.118.155.220	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	30
84.108.177.123	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/giyus/	None	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/rabanut/general.aspx	Block	15
46.19.86.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
77.126.186.141	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	15
31.168.31.150	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	15
149.78.246.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/family	Block	15
2.54.50.1	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
89.138.216.73	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	15
81.218.165.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	15
66.249.65.18	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	15
185.45.192.227	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/__	Block	15
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	15
46.19.85.161	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	15
176.12.150.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
2.54.159.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.75.60	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.75.60	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
46.19.86.227	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
176.13.16.189	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	15
79.177.147.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
89.139.16.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 82.80.17.163	Block	15
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/links.aspx	Block	15
185.45.192.227	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/__	Block	15