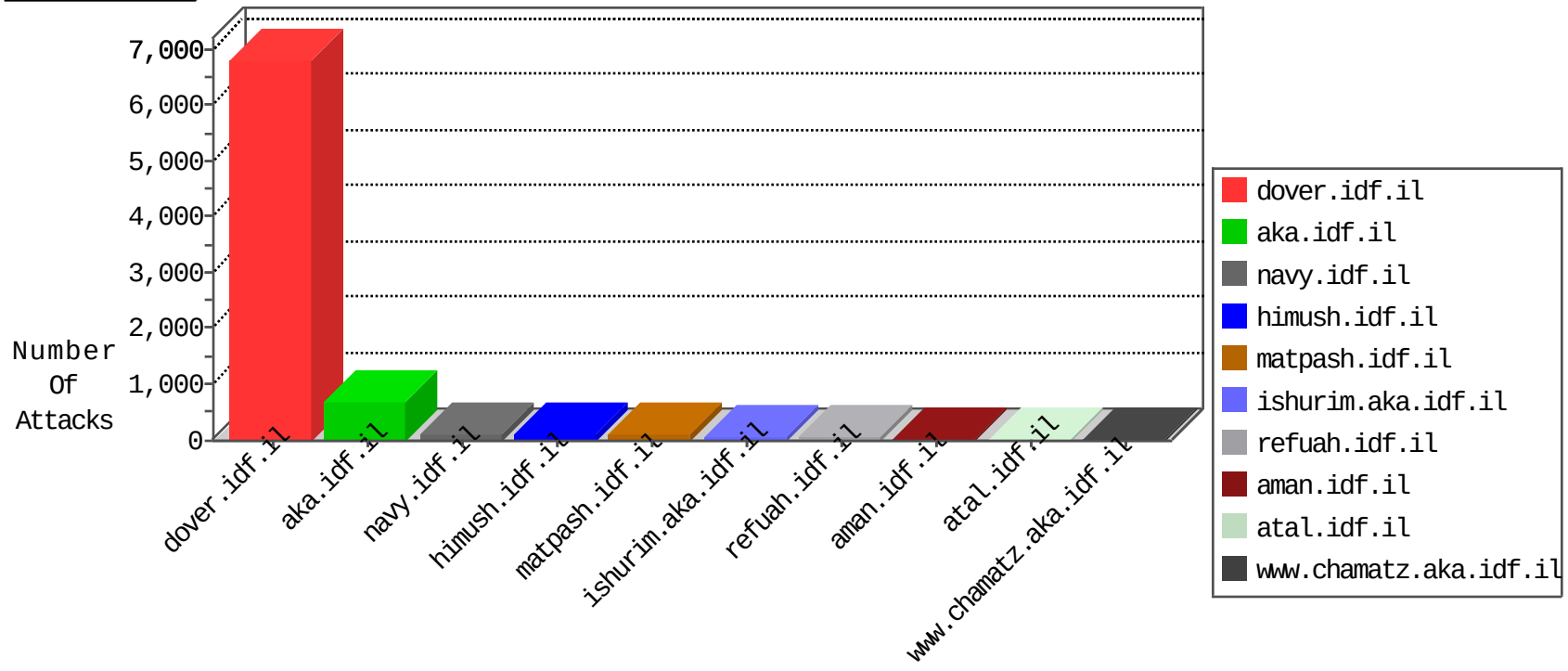
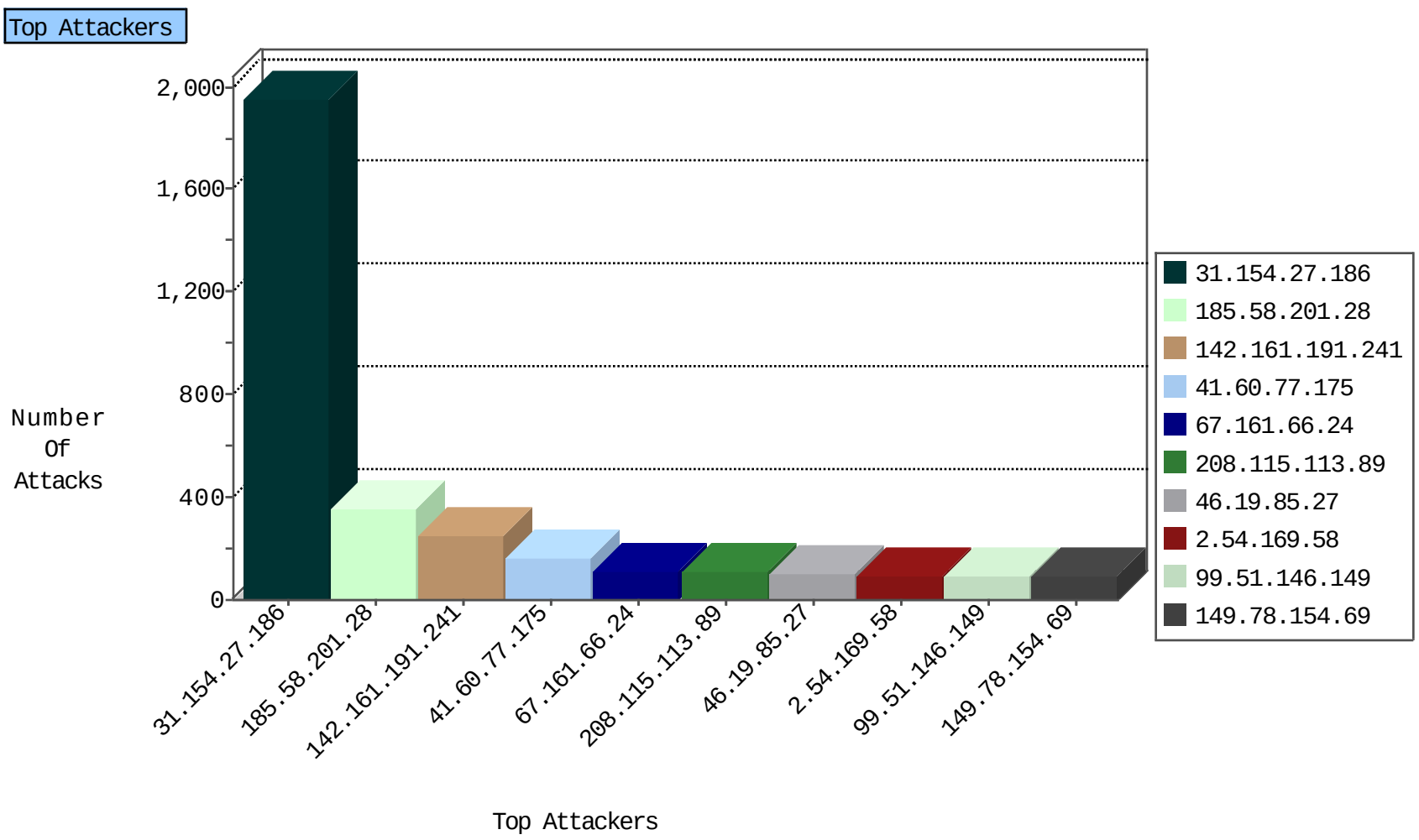
10-19-2015-08:04:04 to 10-19-2015-09:04:04

IDF Under Attack Daily Report





10-19-2015-08:04:04 to 10-19-2015-09:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.214	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	108
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
93.173.182.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
80.246.136.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
79.177.216.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
37.26.148.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
212.199.239.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.168.138.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
89.139.16.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.67.138.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.108.160.36	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
94.230.93.159	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
81.218.48.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
5.102.254.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
138.134.102.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
94.230.93.191	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
94.230.93.223	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.139.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
84.228.169.119	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.52.171.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
165.225.72.81	United States	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
2.54.139.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
82.80.56.21	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
186.81.3.109	Colombia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-19-2015-08:04:04 to 10-19-2015-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.52.148	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
82.80.41.242	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

10-19-2015-08:04:04 to 10-19-2015-09:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
185.58.201.28	147.237.76.30	Lebanon	himush.idf.il	ET SCAN NMAP -sA (2)	2
210.61.150.154	147.237.0.33	Taiwan	idf.il	ET SCAN NMAP -sS window 4096	1
210.61.150.154	147.237.0.33	Taiwan	idf.il	ET SCAN NMAP -f -sS	1
183.83.17.54	147.237.76.44	India	e.refuah.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
76.78.130.9	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.32	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.61.150.154	147.237.0.33	Taiwan	idf.il	ET SCAN NMAP -sS window 2048	1
195.68.62.253	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
171.249.219.247	147.237.0.33	Vietnam	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.184.195.114	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-19-2015-08:04:04 to 10-19-2015-09:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.154.27.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1956
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	285
142.161.191.241	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	249
41.60.77.175	Zambia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	162
67.161.66.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
46.19.85.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
2.54.169.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
99.51.146.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
149.78.181.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	69
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
46.19.86.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
212.25.84.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
95.211.226.36	Netherlands	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	56
46.117.77.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
46.19.85.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
62.219.146.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
46.19.86.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
176.13.5.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
37.16.138.214	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
109.64.11.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
1.47.170.178	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
31.154.254.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
82.145.219.146	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
212.34.11.99	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
176.13.16.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
176.12.148.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
85.250.91.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
84.228.3.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
176.13.16.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
194.90.191.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
81.218.48.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
100.100.116.195		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
46.19.86.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
37.26.146.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
89.139.16.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.126.122.176	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	78
199.188.204.160	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 199.188.204.160	Block	52
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	39
193.169.71.243	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.169.71.243	Block	26
141.0.12.203	Norway	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
2.52.56.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
80.178.213.134	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	26
176.13.8.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	26
62.128.48.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	13
46.19.85.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
79.181.124.153	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.124.153	Block	13
2.52.16.27	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	13
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/kkkkkkk=44a4b8f5kkkkkkk_44a4b8f5	Block	13
5.100.249.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	13
95.35.199.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	13
62.219.175.68	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	13
193.169.71.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	13
144.76.129.242	Germany	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../shared/usercontrols/headerupper/	Block	13
46.19.85.129	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	13
79.181.124.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/https:/aka.idf.il/	Block	13
202.102.99.102	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/webresource.axd%3fd	Block	13
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
180.153.186.47	China	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../shared/clientscripts/jquery.plugins/jquery.cycle.all.min.js	Block	13
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	13
31.154.151.30	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 31.154.151.30	Block	13
109.65.2.73	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	13
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	13
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
195.159.233.44	Norway	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	13
147.236.16.190	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	13
46.19.85.129	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
2.54.149.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
213.57.105.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	13
185.32.179.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
37.46.39.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
109.67.21.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	13
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
195.159.233.44	Norway	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unsupported Legacy SSL Version	None	13
46.19.86.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
2.54.179.91	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
80.246.137.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qr/	Block	13
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
192.115.85.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
46.19.85.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
132.70.66.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13