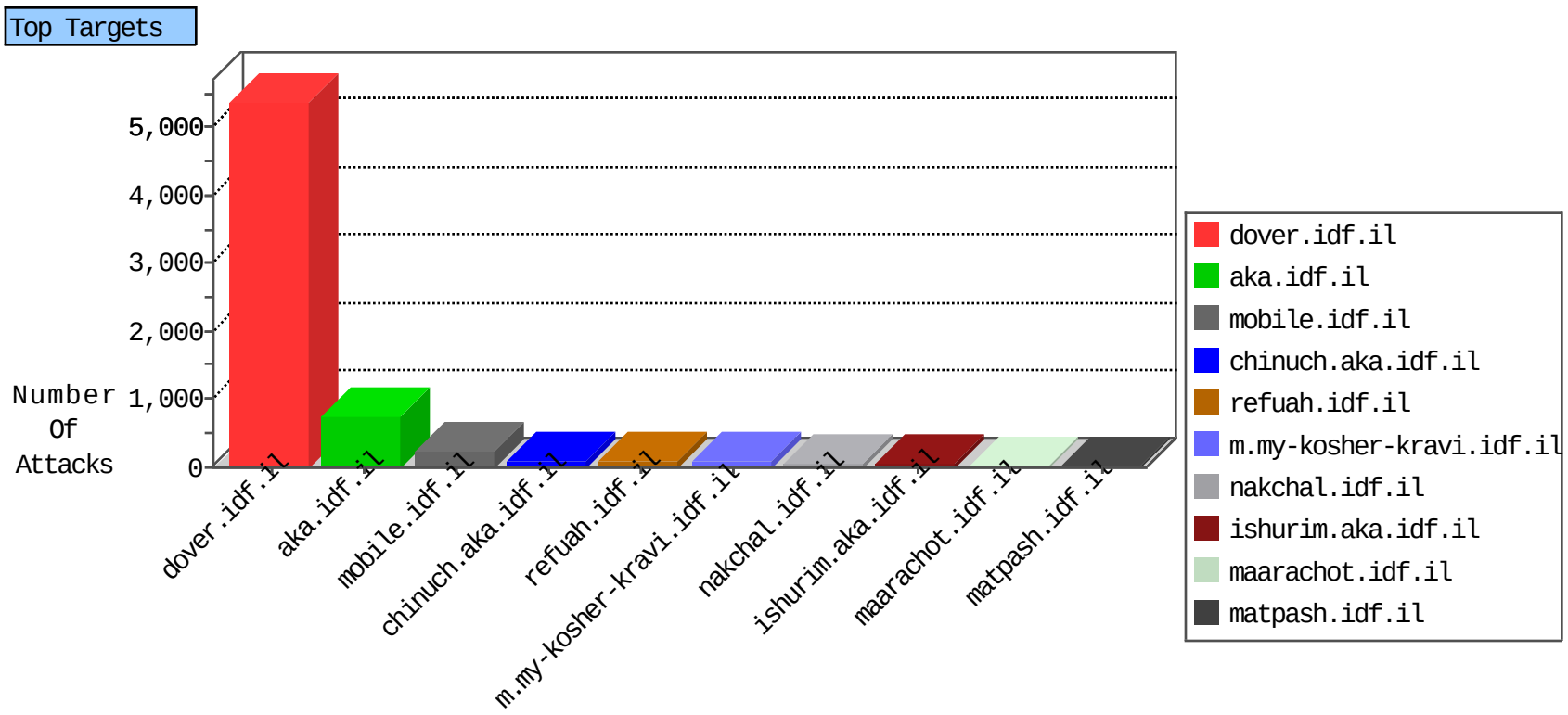
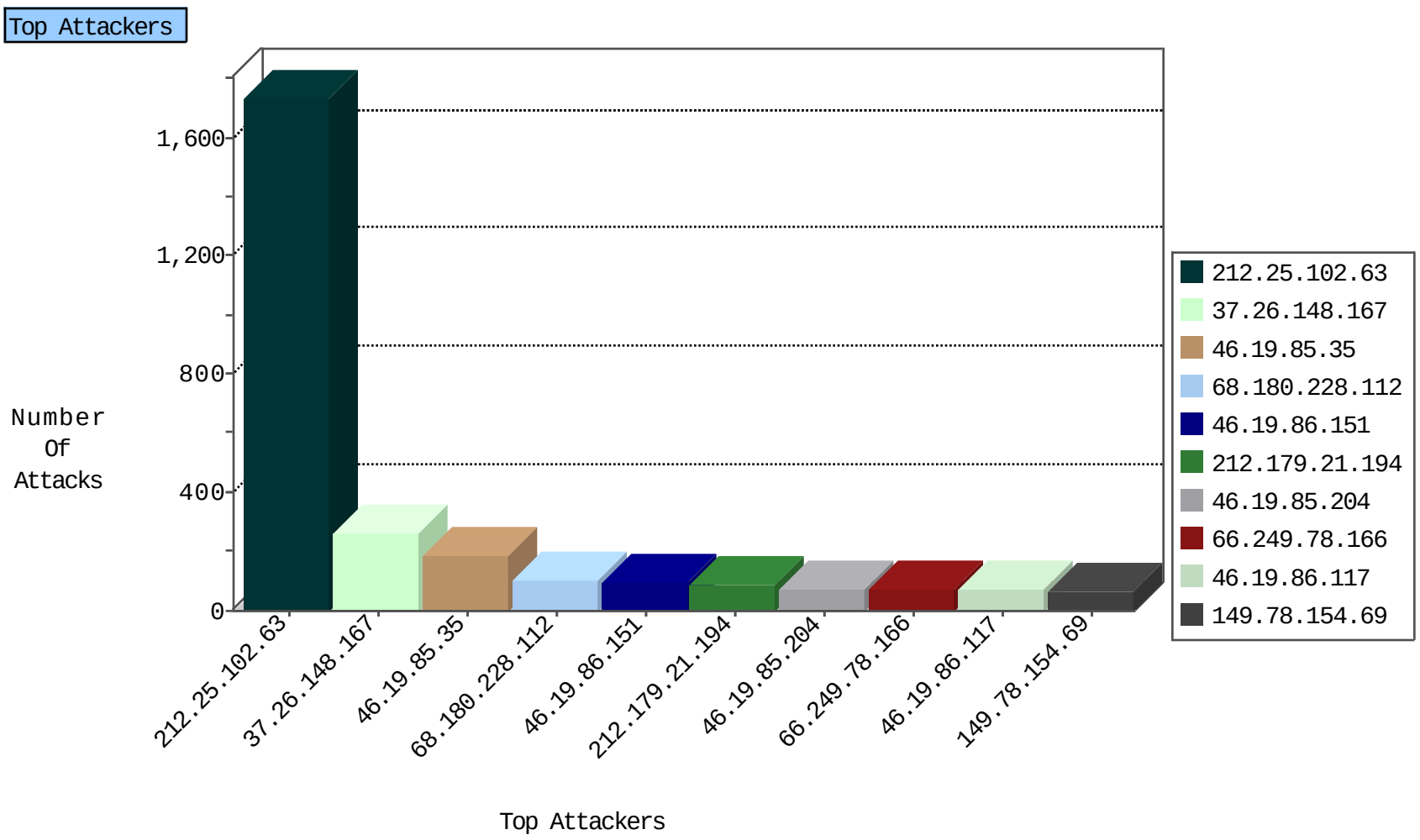
10-28-2015-08:04:07 to 10-28-2015-09:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-28-2015-08:04:07 to 10-28-2015-09:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.203	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	69809
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36792
66.249.64.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34959
106.79.130.100	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34139
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	28675
37.105.195.79	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14788
82.145.210.64	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6974
66.249.64.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5618
2.89.113.46	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4900
66.249.78.109	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4739
5.141.12.212	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4726
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4191
66.249.78.204	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1984
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	558
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
2.54.39.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	61
176.12.147.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	44
184.1.231.192	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
212.143.240.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
176.13.0.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.52.133.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
46.19.86.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
46.19.86.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
46.19.85.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
212.25.102.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
87.68.153.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
37.26.147.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	11
46.116.216.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.12.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.12.148.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
5.29.128.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.85.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
37.26.148.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
213.244.83.2	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.186.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.86.117	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.85.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
2.54.39.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.19.86.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.151.57.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.131.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.95.130.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.168.114.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.171.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.172.0.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
137.95.1.11	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.133.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.186.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4

10-28-2015-08:04:07 to 10-28-2015-09:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
70.35.195.245	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

10-28-2015-08:04:07 to 10-28-2015-09:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.255.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.195.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.106.226.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.57.5.20	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
118.172.198.195	147.237.0.15	Thailand	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.181.126.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.26.147.200	147.237.77.216	Israel	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
2.54.19.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
169.57.5.20	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
137.95.1.11	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.38.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1

10-28-2015-08:04:07 to 10-28-2015-09:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.25.102.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1726
37.26.148.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	265
46.19.86.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
79.182.214.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
46.19.85.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
87.69.195.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
46.19.86.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
46.19.86.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
82.145.210.64	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
2.54.0.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
89.139.41.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
84.108.10.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.143.222.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
181.47.177.97	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
193.104.117.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
132.68.11.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
184.1.231.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.85.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
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
2.54.39.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
87.68.153.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
2.54.10.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
79.177.206.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
77.127.227.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
84.95.130.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.142.118.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
79.134.145.168	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.3.78		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
46.19.86.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
46.116.216.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.77.239.138	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
46.19.85.221	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
84.95.130.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.65.24.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
185.32.179.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17

10-28-2015-08:04:07 to 10-28-2015-09:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.35	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	118
46.19.85.204	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	74
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	56
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906.pdf	Block	56
40.77.167.45	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
2.54.171.214	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	42
62.219.161.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
212.199.108.206	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.108.206	Block	28
176.13.10.165	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	28
82.166.184.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born	Block	28
62.90.35.177	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	22
62.90.35.177	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/ajax/updatestatus.php	Block	16
193.106.54.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
176.12.145.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
69.65.3.173	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	14
40.77.167.44	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	14
95.86.68.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.68.13	Block	14
66.249.93.207	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.93.207	Block	14
46.19.85.35	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	14
176.13.4.66	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	14
79.179.118.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
40.77.167.44	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	14
95.86.68.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ca0qfjaaahukewj98fe2yotiahwdshqkhclmc6w&sig2=myp5ljp-x-4zrufumwre2g&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	14
66.249.93.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/registrationwizard/register.aspx	Block	14
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/iaf.org.il	Block	14
188.165.15.241	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×″×?×ª×¨	Block	14
46.19.86.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
212.199.108.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files	Block	14
176.228.47.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
192.114.105.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
46.19.85.35	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
157.55.39.68	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	14
37.26.147.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
185.32.179.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9680-he/refuah.aspx	Block	12
82.166.239.100	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	11
109.67.210.101	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	10
188.120.148.180	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	7

10-28-2015-08:04:07 to 10-28-2015-09:04:07