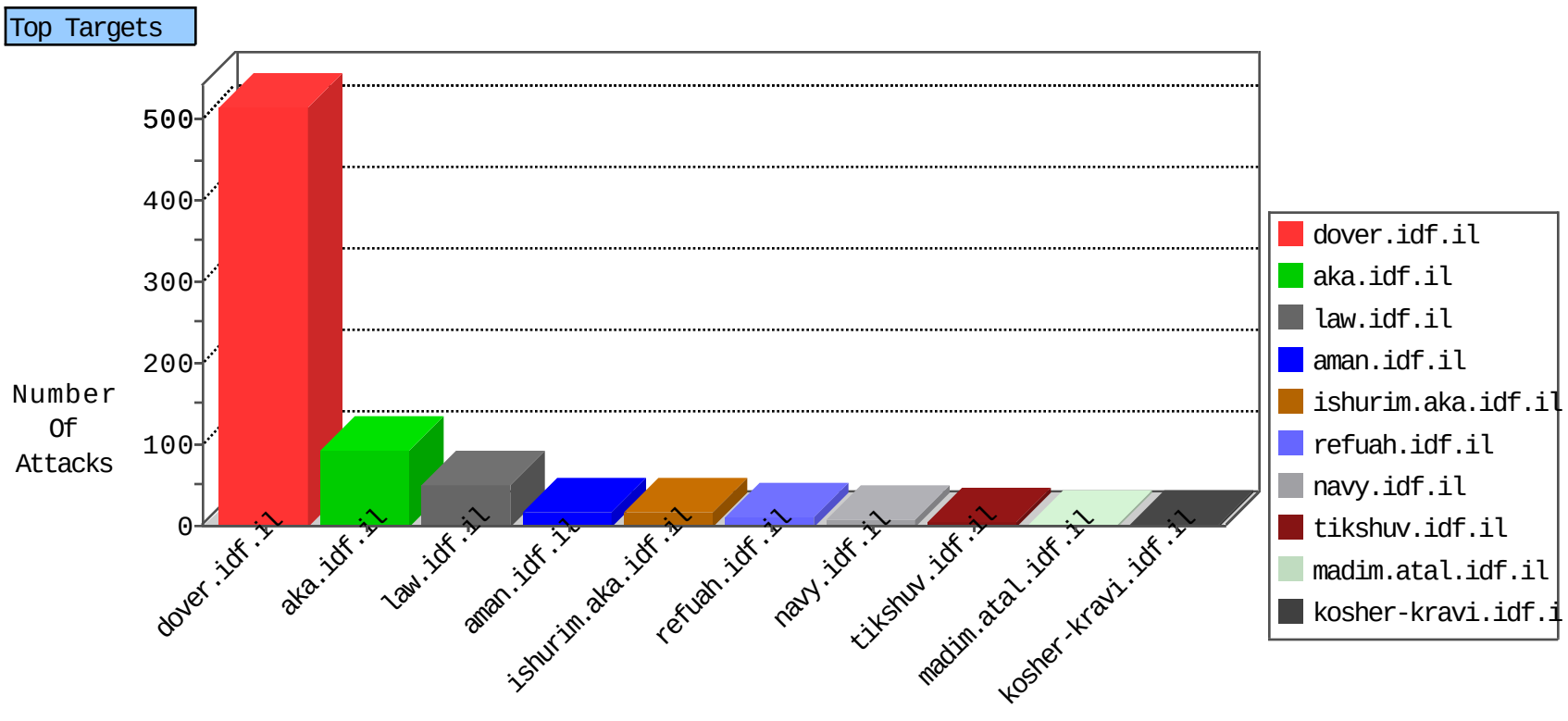
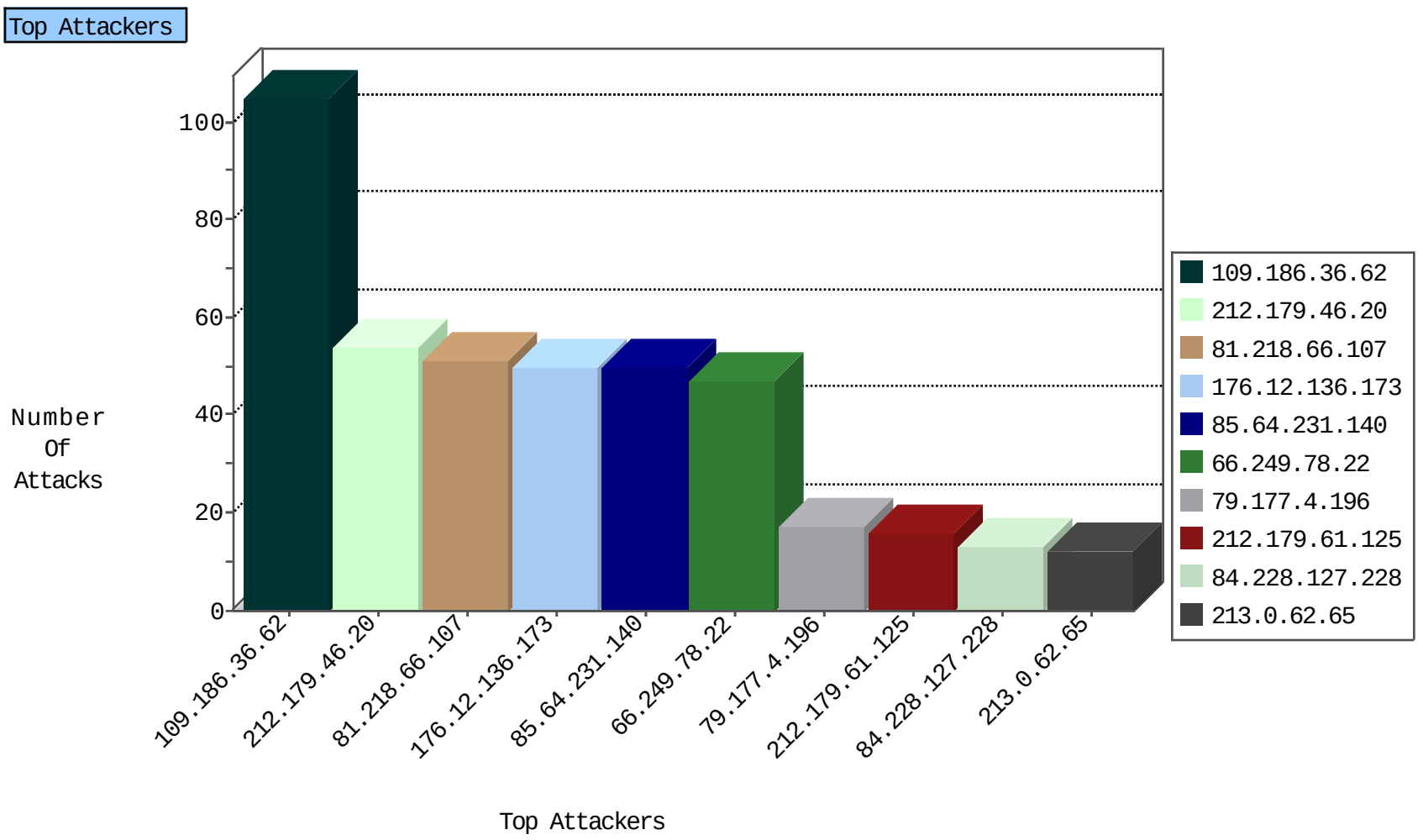
04-26-2015-13:03:09 to 04-26-2015-14:03:09

IDF Under Attack
04-26-2015-13:03:09

Top Targets



Top Attackers



04-26-2015-13:03:09 to 04-26-2015-14:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	896
79.177.4.196	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
84.228.127.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
199.199.0.101	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
193.43.244.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
84.228.201.235	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
132.68.205.93	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
89.138.74.135	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.108.111.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.228.126.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.186.36.62	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
2.54.4.193	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.116.71.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
31.168.209.183	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
109.226.13.51	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.108.204.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
213.57.80.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.85.13	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
81.218.241.26	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.46.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
176.12.148.19	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
194.90.254.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.120.97.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.114.105.254	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
87.69.58.232	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
81.218.58.54	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.94	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
62.219.137.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.77	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.146.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.179.61.125	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.155	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.48.92.104	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
62.90.251.149	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.118.36.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-26-2015-13:03:09 to 04-26-2015-14:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.0.62.65	Spain	147.237.0.15	kosher-kravi.idf.il	0932: HTTP: Shell Command Execution (bash)	Block	1
46.19.86.94	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
213.0.62.65	Spain	147.237.0.17	m.my-kosher-kravi.idf.il	0932: HTTP: Shell Command Execution (bash)	Block	1
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
213.0.62.65	Spain	147.237.0.19	madim.atal.idf.il	0932: HTTP: Shell Command Execution (bash)	Block	1
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.19	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1

04-26-2015-13:03:09 to 04-26-2015-14:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	47
132.74.56.24	Israel	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	3
213.0.62.65	Spain	147.237.0.15	kosher-kravi.idf.i	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
31.168.197.78	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.150.239	France	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
193.254.206.6	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
176.12.140.143	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.97.114	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.227	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.97.130	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
78.166.132.56	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	1
213.0.62.65	Spain	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
46.117.128.187	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	India	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
5.29.0.20	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.12.148.50	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
147.236.50.178	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.207.234	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.66.107	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.217.73	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
213.0.62.65	Spain	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1

04-26-2015-13:03:09 to 04-26-2015-14:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.186.36.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
176.12.136.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
81.218.66.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
85.64.231.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
147.236.50.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
95.86.113.136	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
31.168.244.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.29.237.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.183.48.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
194.90.254.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.13.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.133.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
62.0.102.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.199.53.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.250.159.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
91.135.111.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.144.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
94.188.161.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.94.205.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.48.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.64.57.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
162.243.210.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
87.68.214.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.93.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.120.97.29	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.54.55.184	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	1
109.64.149.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
62.219.161.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.178.189.43	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
65.19.138.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.120.148.176	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
79.178.189.43	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
193.34.57.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-26-2015-13:03:09 to 04-26-2015-14:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.142.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
93.173.250.127	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.160.160.214	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//console/core/doc_mgr/doc_mgr.asp	Block	3
81.218.33.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	3
82.166.20.48	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.0.62.65	Spain	147.237.0.34	tikshuv.idf.il	Multiple URL worm attacks from 213.0.62.65	Block	2
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	2
46.117.63.114	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.29.97.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.239.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.142.49.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.200.12.139	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	2
77.125.135.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.111.220	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
84.229.135.100	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//console/core/doc_mgr/doc_mgr.asp	Block	2
46.117.124.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.151.56	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 01024D0375E5254ED208FE4D7BB6B0284ED208000932003000360038003600310031003700310000012F00FF, Observed 0102AD3F7304404DD208FEADB7B4CF424DD208000932003000360038003600310031003700310000012F00FF	None	2
77.127.97.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
31.168.243.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
109.253.158.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.67.160.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
213.0.62.65	Spain	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
85.65.110.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//lomdim/forum/	Block	1
37.142.255.87	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.133.201	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
5.22.130.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/resource/userfollowresource/create/	Block	1
109.253.131.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/information_archive.stm	Block	1
66.249.64.27	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.97	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.19.86.97	Block	1
192.116.98.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
82.166.53.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl05 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.180.123.34	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
37.26.146.141	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.253.159.46	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12463-he/dover.aspx	Block	1
85.250.27.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.120.120.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
207.232.29.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.166	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
81.218.33.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.33.77	Block	1
5.22.130.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.141.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-26-2015-13:03:09 to 04-26-2015-14:03:09