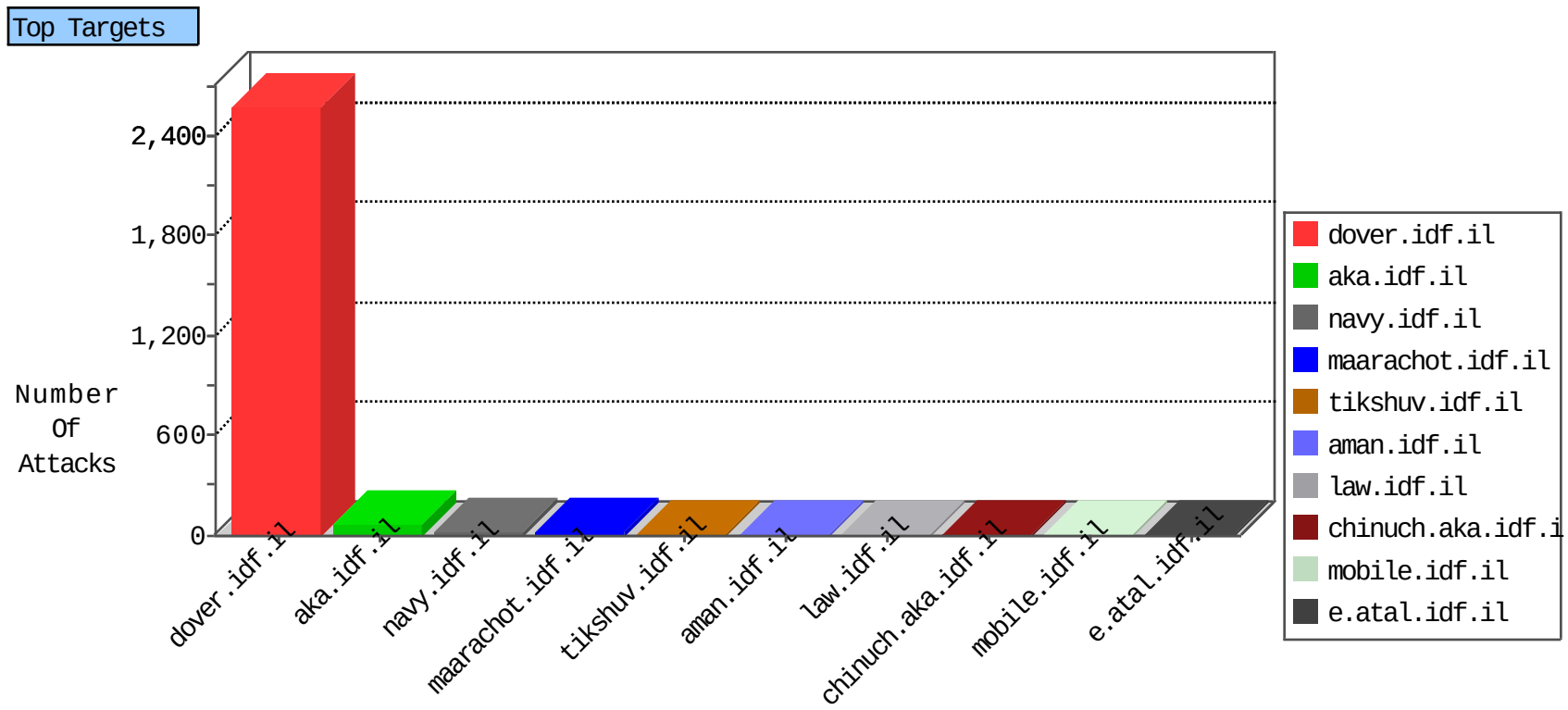
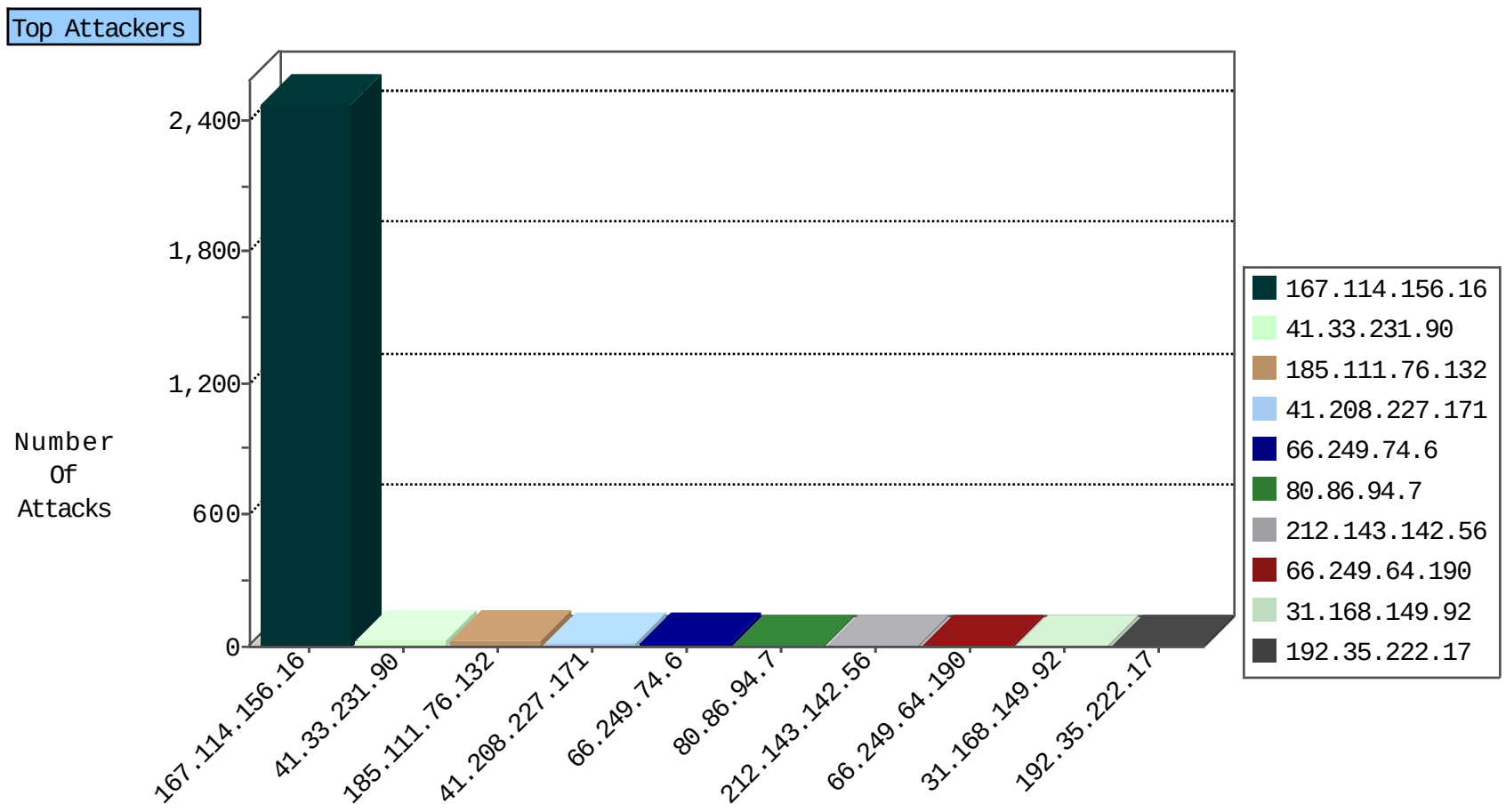
12-11-2015-02:04:06 to 12-11-2015-03:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-11-2015-02:04:06 to 12-11-2015-03:04:06

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	DOS-Tool-SwitchbladG	dest-reset	3358
66.249.79.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	55
61.183.118.225	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
60.189.70.32	China	147.237.72.167	ishurim.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
111.122.42.143	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

12-11-2015-02:04:06 to 12-11-2015-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.117	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.35.180.120	United States	147.237.76.86	navy.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1

12-11-2015-02:04:06 to 12-11-2015-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
185.111.76.132	147.237.77.243		mobile.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.6	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
185.111.76.132	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	2
185.111.76.132	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	2
185.111.76.132	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
185.111.76.132	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
125.65.97.66	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
185.111.76.132	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.164.54	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.8.45		e.eitan.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.8.24		e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.66	147.237.77.216		dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.111.76.132	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.10.66.60	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
185.106.94.66	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.111.76.132	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
175.143.53.17	147.237.8.14	Malaysia	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
185.111.76.132	147.237.76.39		mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
125.65.97.66	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
202.98.157.52	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
185.111.76.132	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.218.246.103	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
185.111.76.132	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	147.237.0.15	Hong Kong	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.111.76.132	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
185.111.76.132	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
221.10.66.60	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
185.106.94.66	147.237.76.196		e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.111.76.132	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
218.161.111.51	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.143.53.17	147.237.8.14	Malaysia	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
185.111.76.132	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1
175.143.53.17	147.237.8.14	Malaysia	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
202.98.157.52	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1

12-11-2015-02:04:06 to 12-11-2015-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
41.208.227.171	South Africa	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.168.149.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.49	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.183.10.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.167.180	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.55	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.247.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.189.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.29.110.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
148.177.129.212	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
87.195.152.102	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.74.12	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.35.222.17	United States	147.237.77.216	dover.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
208.115.113.88	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
141.212.122.127	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.100	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.35	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.112	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.66	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
122.204.139.210	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
202.98.157.52	China	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.100	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
221.10.66.60	China	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.54.17.213	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
186.45.170.116	Trinidad and Tobago	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.121.139.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.113	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.67	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
125.65.97.66	China	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
202.98.157.52	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.101	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
221.10.66.60	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.54.17.213	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
108.244.66.196	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.86.94.7	Germany	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 80.86.94.7	Block	8
66.33.212.131	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.33.212.131	Block	3
41.208.227.171	South Africa	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	3
37.142.184.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
37.142.231.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
40.77.167.16	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.200.24.232	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	2
66.249.69.8	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
176.13.22.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.247.30.234	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	2
150.70.173.5	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
52.35.180.120	United States	147.237.76.86	navy.idf.il	Multiple Illegal Byte Code Character in Method from 52.35.180.120	Block	1
104.131.14.193	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on /	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/	Block	1
207.46.13.49	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.0.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.56.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.86.94.7	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/general/general.aspx	Block	1
220.166.62.101	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2826.jpg	Block	1
150.70.173.40	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
52.35.180.120	United States	147.237.76.86	navy.idf.il	Multiple NULL Character in Method from 52.35.180.120	Block	1
104.131.14.193	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9014-he/refuah.aspx	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/rights/asp/searchresults.asp	Block	1
207.46.13.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
141.212.122.97	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1
87.69.105.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.35.180.120	United States	147.237.76.86	navy.idf.il	NULL Character in Method	Block	1
40.77.167.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/form.asp	Block	1
104.131.14.193	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on /	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	1
207.46.13.144	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.210.150.253	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
93.172.164.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.17	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
54.153.32.246	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/kkkkkkk=cd078036kkkkkkk_cd078036	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
150.70.97.86	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
52.35.180.120	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method	Block	1
95.65.34.177	Moldova, Republic of	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
54.153.32.246	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
207.46.13.17	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opmissingperson/opmissingperson.in.aspx	Block	1
45.55.223.101		147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on /	Block	1