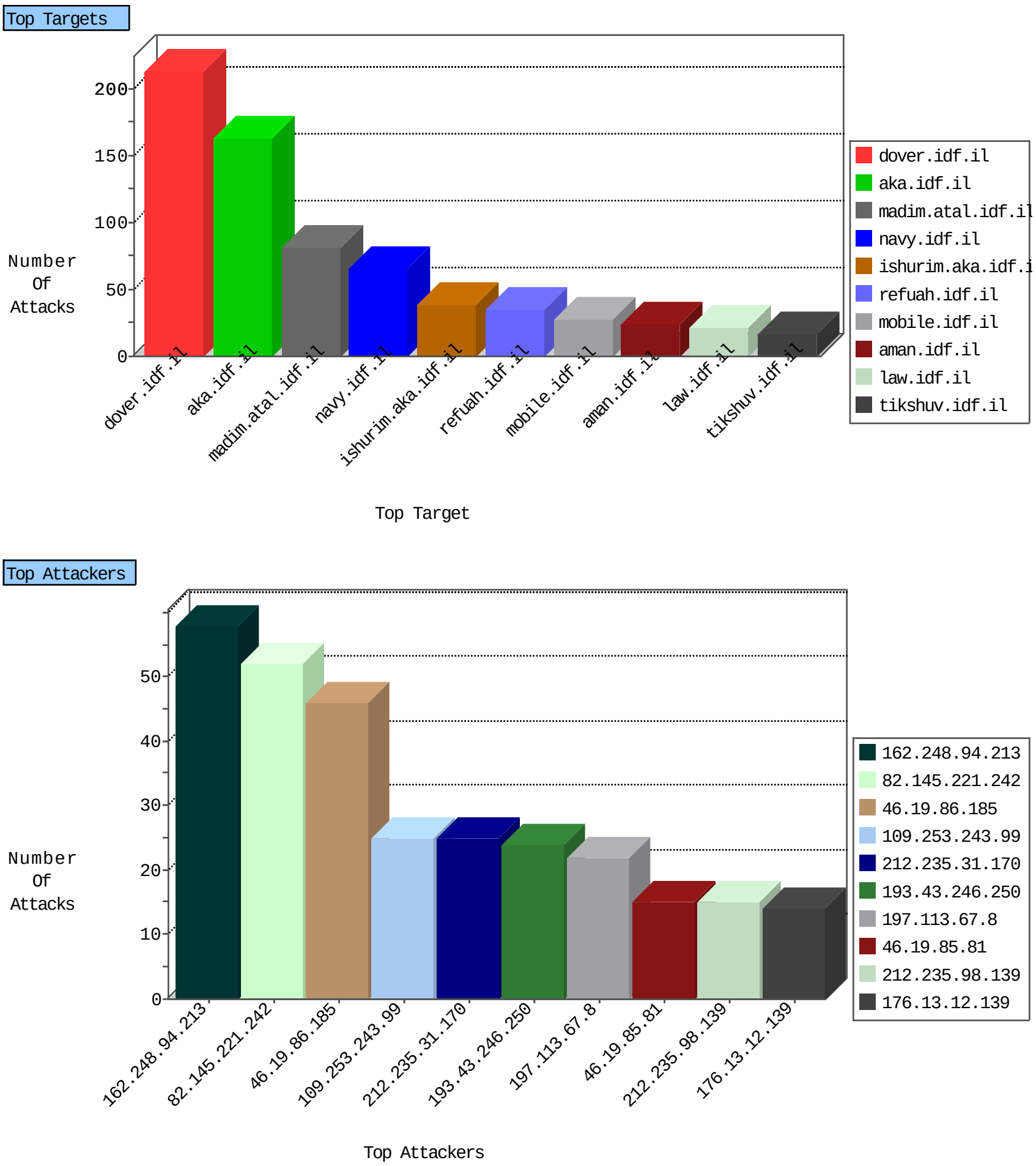
09-06-2016-13:04:01 to 09-06-2016-14:04:01

IDF Under Attack
Daily Report



09-06-2016-13:04:01 to 09-06-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.245.51	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
37.48.83.137	Netherlands	147.237.76.176	test.ncore.idf.i	Black List	drop	1
37.48.83.137	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
79.176.57.186	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-06-2016-13:04:01 to 09-06-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-06-2016-13:04:01 to 09-06-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.150.11.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
109.253.138.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.121.144.42	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
79.183.55.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.155.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.53.232	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.135.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.10	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.172.71.251	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.16.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
150.242.238.99	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.131.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.201.254.246	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.163.3	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
79.179.26.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.42.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.203.63.71	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -f -sS	1
66.249.93.158	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
208.100.26.228	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.181.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.33.63.5	147.237.77.212	Colombia	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.86.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.44.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-06-2016-13:04:01 to 09-06-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.221.242	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
197.113.67.8	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
162.248.94.213	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
162.248.94.213	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
162.248.94.213	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
37.26.146.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
212.235.31.170	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.140.104	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
162.248.94.213	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.81	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.3.147.133	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.177.223	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.165.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.81	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.245.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.14	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.14	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.41	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.90.153.242	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
212.235.31.170	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	5
109.253.200.67	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
37.247.36.94	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
109.253.208.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
212.235.31.170	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
37.26.148.161	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.235.31.170	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.213.48.202	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.12.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.235.31.170	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.12.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.176.57.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.32.179.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.208.233	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
31.210.186.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.136.96	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.209.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.237.248	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.163	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

09-06-2016-13:04:01 to 09-06-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
109.253.243.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
31.168.170.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.170.190	Block	6
31.168.15.54	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	3
82.81.137.131	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.90.2.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	3
109.253.156.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.65.222	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/926-he/refuah.aspx	Block	3
188.166.186.43	Singapore	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.146.217	Block	2
72.199.248.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	2
37.26.147.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/geneal.aspx	Block	2
46.116.202.38	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	2
136.179.21.78	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 136.179.21.78	Block	1
46.19.85.14	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
52.16.137.212	Ireland	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on /	Block	1
91.231.193.150	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
46.19.86.41	Israel	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
79.178.188.209	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
212.199.226.66	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.86.125	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
136.179.21.78	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	1
82.166.97.173	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.166.97.173	Block	1
31.168.15.54	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
109.253.134.240	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.19.86.41	Israel	147.237.77.233	atal.idf.il	Distributed Malformed URL	Block	1
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
79.180.215.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.215.55	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/70224.pdf	Block	1
157.55.39.115	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/general/general.aspx	Block	1
82.166.97.173	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
46.19.85.183	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version sdch	Block	1
77.138.150.168	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
194.83.40.1	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.19.86.41	Israel	147.237.77.233	atal.idf.il	Distributed Unknown HTTP Request Method	Block	1
80.246.133.0	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.76.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
2.53.139.50	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
176.13.10.205	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	1
46.19.85.183	Israel	147.237.76.31	nakchal.idf.il	Malformed URL deflate,	Block	1
31.168.170.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
77.139.30.108	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.69.10	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/540-en/patzar.aspx	Block	1

09-06-2016-13:04:01 to 09-06-2016-14:04:01