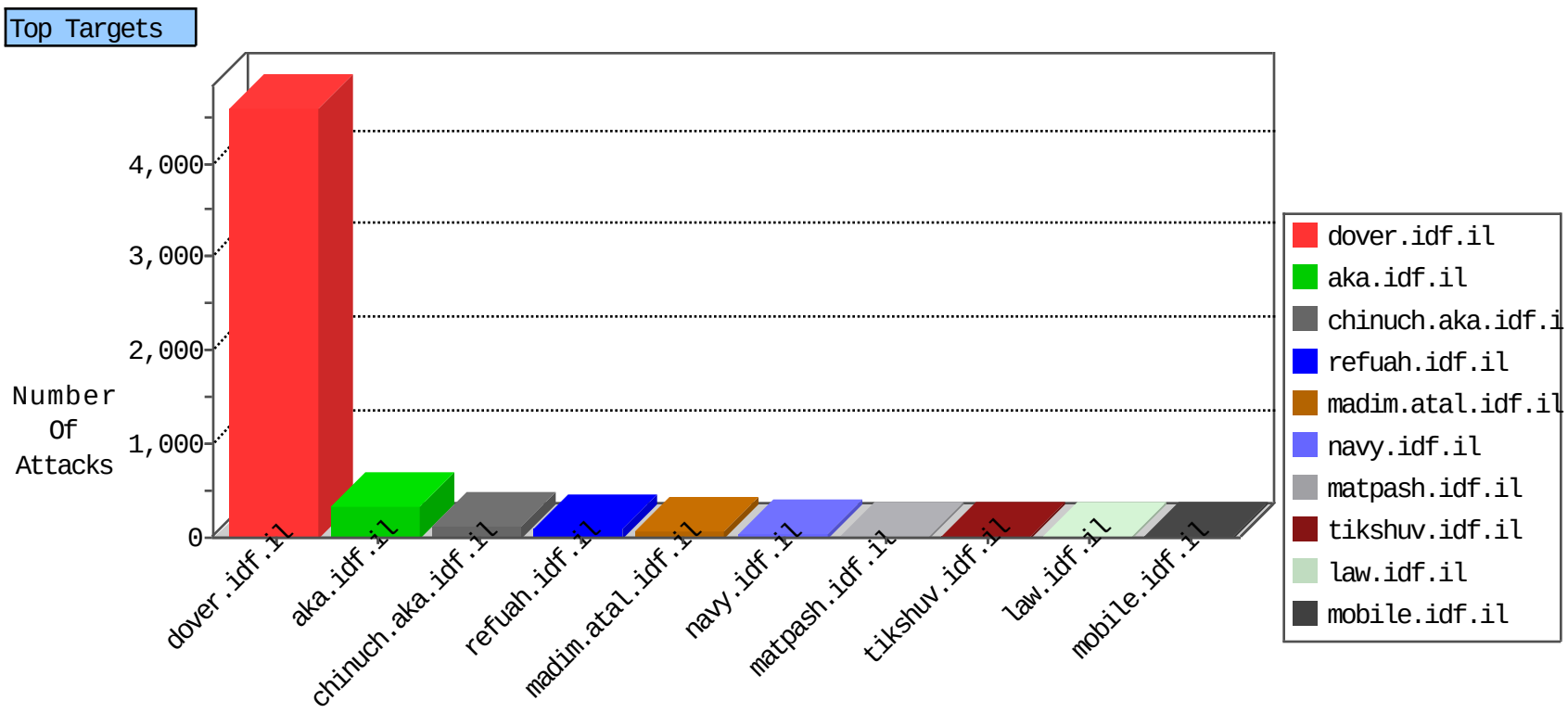
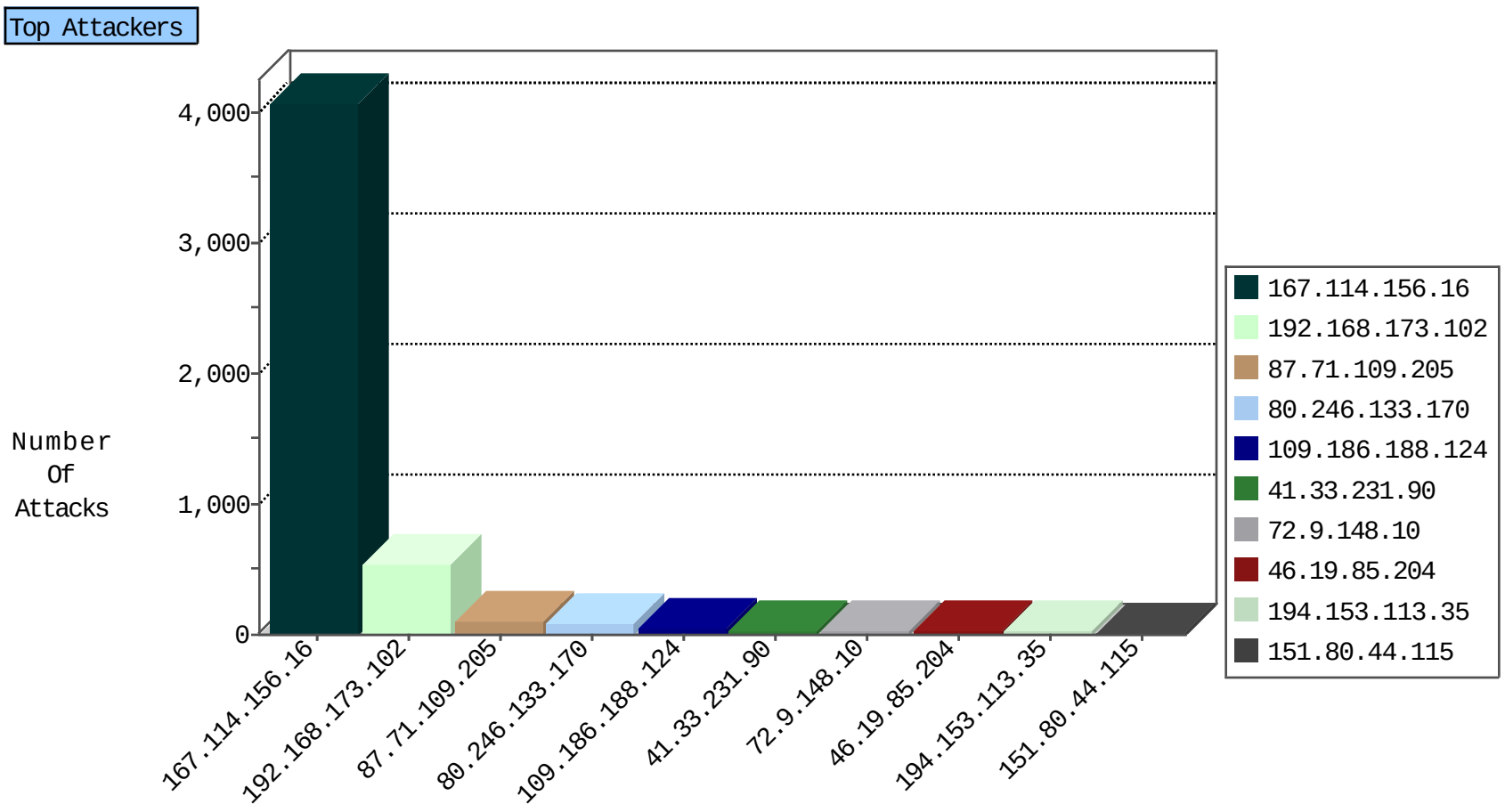
04-08-2016-18:04:00 to 04-08-2016-19:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-08-2016-18:04:00 to 04-08-2016-19:04:00

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	Block_Ip_Web_In	drop	4077
79.177.181.5	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	85
123.59.59.52	China	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
209.126.110.228	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
209.126.110.228	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1

04-08-2016-18:04:00 to 04-08-2016-19:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.1.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
151.80.44.115	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
151.80.44.115	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.149.230	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.44.115	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.86.58	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.44.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.44.115	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.44.115	France	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.62	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
162.250.190.142	Canada	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-08-2016-18:04:00 to 04-08-2016-19:04:00

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	4
66.249.69.93	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.20	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
193.201.227.65	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
173.88.225.181	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
161.18.128.22	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.204.187.90	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN NMAP -sS window 2048	1
84.200.15.174	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
195.154.54.169	147.237.72.217	France	e.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.65	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
173.88.225.181	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
173.88.225.181	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
106.184.2.29	147.237.77.235	Japan	sviva.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN NMAP -f -sS	1
84.200.15.174	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

04-08-2016-18:04:00 to 04-08-2016-19:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	361
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	178
87.71.109.205	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
80.246.133.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	81
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.210.219.210	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
37.142.209.124	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.204	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.210.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
201.240.135.175	Peru	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.14.140.99	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.204	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.14.140.99	United Kingdom	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
2.54.156.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.3.147.130	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.218.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
5.102.98.41	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
194.153.113.35	Germany	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.102.254.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
201.240.135.175	Peru	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
207.46.13.36	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.229.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
87.71.124.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.153.113.35	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
84.229.49.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.250.85.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.120.126.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.179.116.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.141	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	3
46.19.85.80	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
37.46.41.69	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.129.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.179.183.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
201.240.135.175	Peru	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
169.254.221.157		147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
188.120.148.140	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.186.188.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
79.170.44.111	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.170.44.111	Block	5
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.179.68.209	Block	4
109.65.252.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.57.209.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.97	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.138.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.171.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.43.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.102.98.41	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	2
94.194.155.204	United Kingdom	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 94.194.155.204	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
123.59.59.52	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.elong.com/894-he/cogat.aspx	Block	1
212.76.112.159	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method HEAD for www.chinuch.aka.idf.il/1145-he/chinuch.aspx	None	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18907-en/dover.aspx <a href=	Block	1
5.28.144.44	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.133.170	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
54.153.33.145	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
198.209.13.56	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.53.43.46	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
94.194.155.204	United Kingdom	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /english/@[[#22]]o[[#2]]	Block	1
185.92.72.33	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
82.205.10.17	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
54.153.33.145	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
131.253.25.237	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.170.44.111	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
185.92.72.33	Netherlands	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.hagnas.atal.idf.il/hnap1/	Block	1
37.187.114.171	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /irj/portal	Block	1
109.253.139.86	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8990	Block	1
87.69.216.59	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.36	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
131.253.25.241	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.207.248	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.16.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
194.153.113.35	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
109.253.210.108	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.105	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/general/	Block	1
131.253.25.247	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.22.129.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
109.65.105.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspx/	Block	1
80.246.133.8	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
46.117.232.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
194.153.113.35	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1