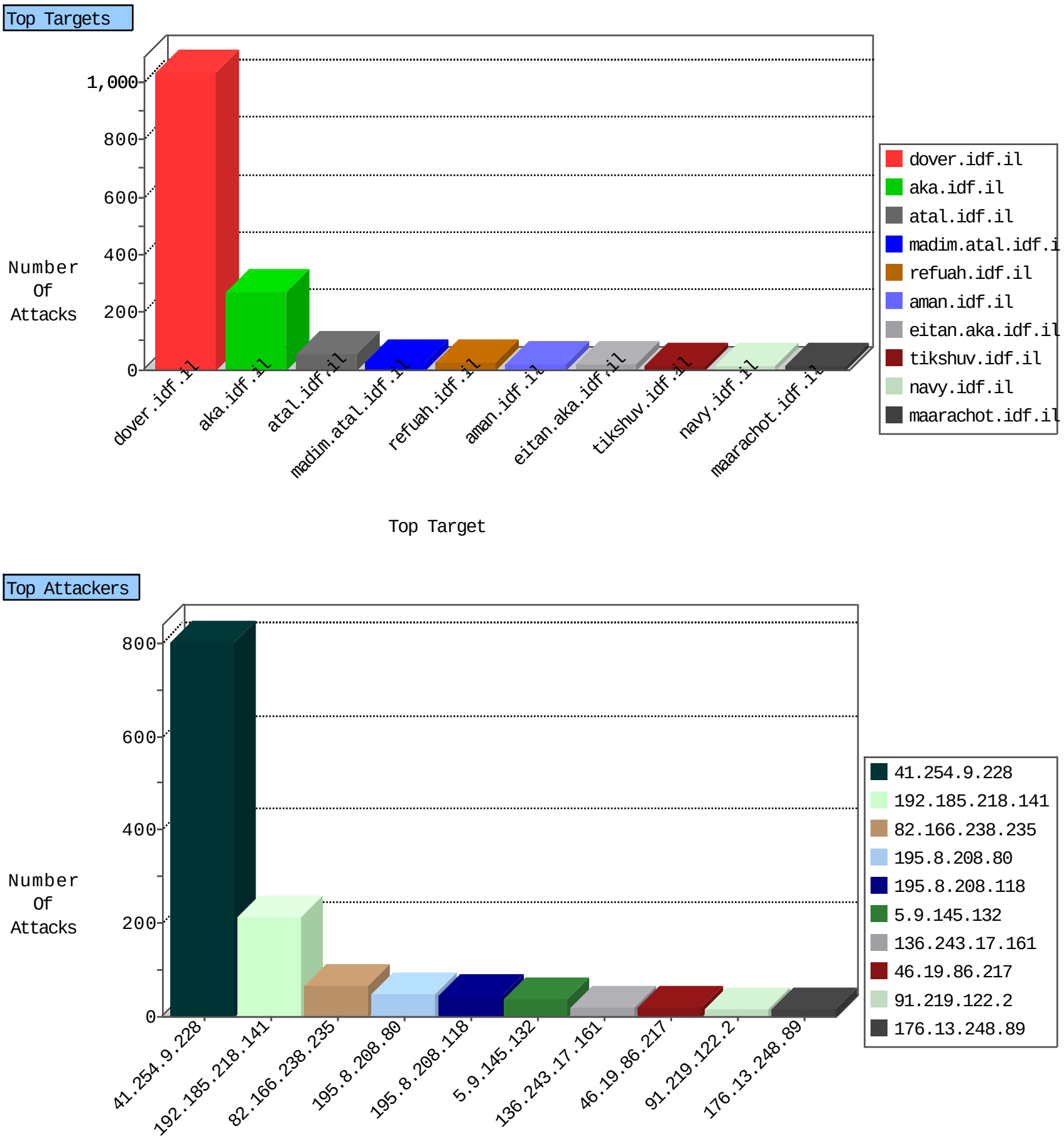
09-10-2016-14:04:08 to 09-10-2016-15:04:08

IDF Under Attack Daily Report



09-10-2016-14:04:08 to 09-10-2016-15:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.254.9.228	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	68
41.254.9.228	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
71.6.146.185	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
173.242.116.60	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1

09-10-2016-14:04:08 to 09-10-2016-15:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.8.208.80	Netherlands	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
195.8.208.118	Netherlands	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
195.8.208.130	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.8.208.80	Netherlands	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.8.208.118	Netherlands	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
179.43.141.208	Switzerland	147.237.76.38	e.e.meitav.idf.i	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

09-10-2016-14:04:08 to 09-10-2016-15:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.8.208.80	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	26
195.8.208.118	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	26
91.219.122.2	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	11
195.8.208.130	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	8
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
200.195.135.82	147.237.77.233	Brazil	atal.idf.il	ET SCAN NMAP -sS window 4096	1
52.166.130.115	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
104.167.6.84	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
69.24.208.162	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
52.166.130.115	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
200.195.135.82	147.237.77.233	Brazil	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.63.2	147.237.77.170	Germany	maarachot.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
163.172.129.15	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1

09-10-2016-14:04:08 to 09-10-2016-15:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.254.9.228	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	717
5.9.145.132	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
82.166.238.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	19
136.243.17.161	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
84.111.160.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
82.166.238.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
192.185.218.141	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
82.166.238.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
192.185.218.141	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
82.166.238.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
82.166.238.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.185.218.141	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
82.166.238.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.185.218.141	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.185.218.141	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
78.46.156.169	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
144.76.71.83	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.9.94.207	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.13.162.183	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.166.238.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.185.218.141	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
192.185.218.141	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.89	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
85.232.60.142	United Kingdom	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
184.168.193.34	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.166.75.214	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
84.229.54.244	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.53.14.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.57.136.12	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.145.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
87.253.153.38	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

09-10-2016-14:04:08 to 09-10-2016-15:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.254.9.228	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.254.9.228	Block	14
79.182.53.151	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
84.109.49.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.103.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.254.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
109.66.126.123	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
5.29.229.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.39.104	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
79.177.51.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
41.254.9.228	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Malformed URL aaaaaaaa	Block	1
176.13.17.184	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
82.166.75.214	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
79.178.215.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.248.89	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 176.13.248.89	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
31.168.219.155	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 31.168.219.155 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.67.5.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
176.13.248.89	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
107.178.35.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/saiarotflash.aspx	Block	1
77.138.54.197	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
31.168.219.155	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
157.55.39.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.181.216.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.235	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
2.53.143.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
192.169.7.223	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
107.178.39.104	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 107.178.39.104	Block	1
77.138.225.200	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
37.26.149.190	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
68.180.229.181	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
207.46.13.93	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16602-en/dover	Block	1

09-10-2016-14:04:08 to 09-10-2016-15:04:08