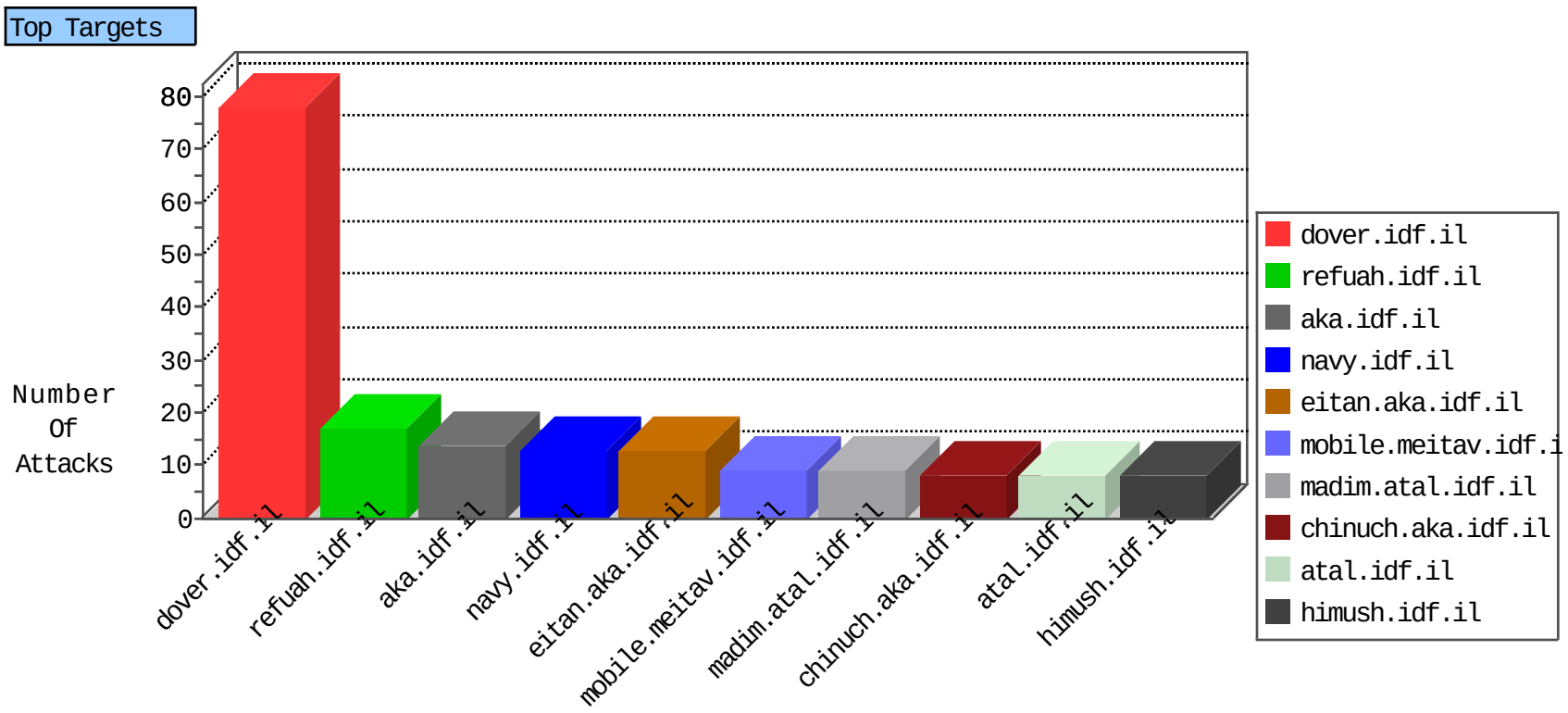
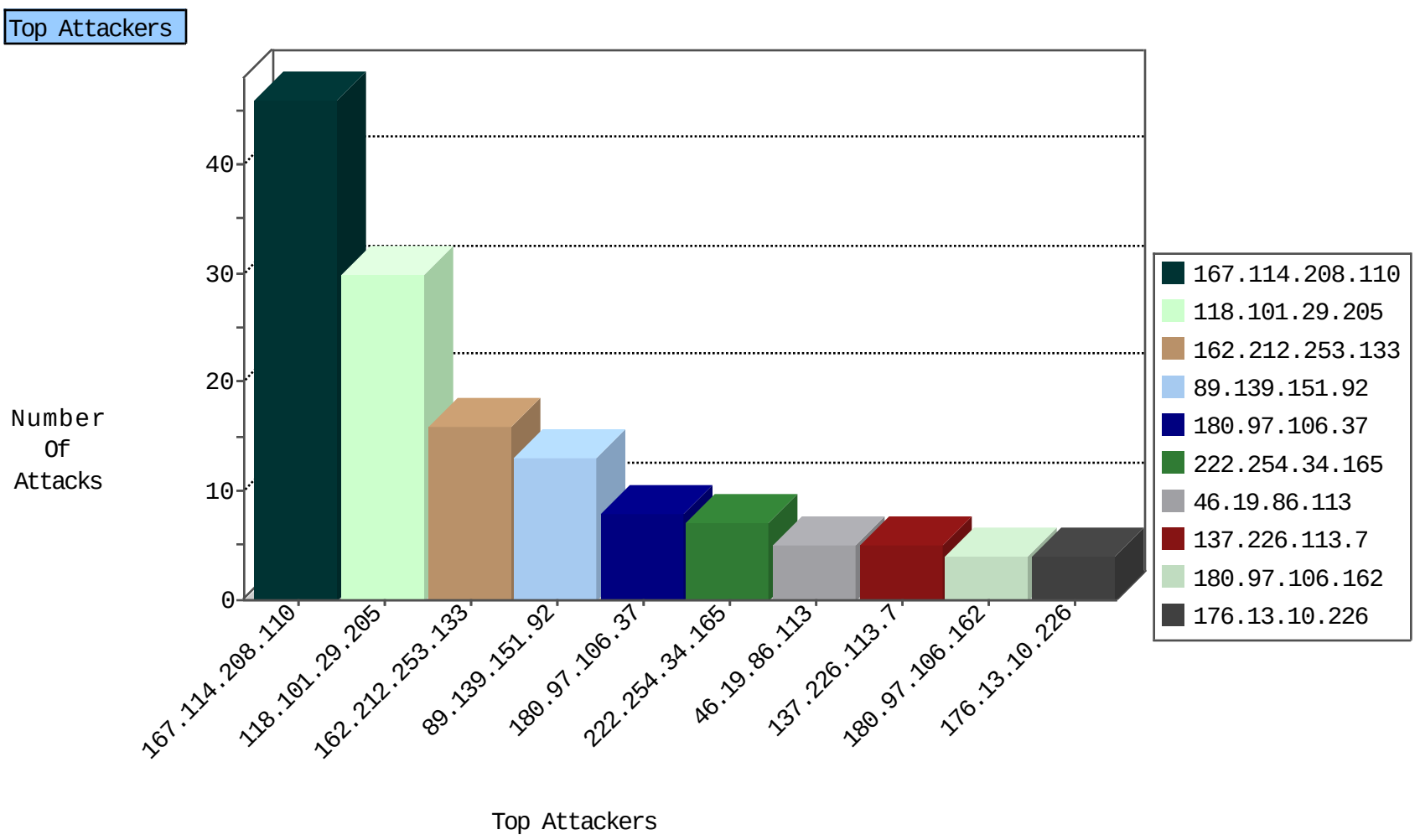
09-01-2016-06:04:05 to 09-01-2016-07:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-01-2016-06:04:05 to 09-01-2016-07:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.221.105.7	Iceland	147.237.76.197	e.himush.idf.il	Black List	drop	1
91.230.121.156	Ukraine	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-01-2016-06:04:05 to 09-01-2016-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-01-2016-06:04:05 to 09-01-2016-07:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.112.208.26	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
79.177.118.165	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
50.245.143.138	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
193.201.225.149	147.237.77.74	Ukraine	law.idf.il	ET SCAN Potential SSH Scan	1
23.82.46.210	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
178.220.165.231	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
122.72.53.188	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
103.207.36.84	147.237.77.212	Vietnam	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 1024	1
222.254.34.165	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
216.81.230.167	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
50.245.143.138	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
178.220.165.231	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
122.224.250.234	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.36.84	147.237.77.212	Vietnam	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
222.254.34.165	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

09-01-2016-06:04:05 to 09-01-2016-07:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
118.101.29.205	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
167.114.208.110	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
167.114.208.110	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
167.114.208.110	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
167.114.208.110	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
167.114.208.110	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
167.114.208.110	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
167.114.208.110	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
167.114.208.110	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.10.226	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
101.184.140.221	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
197.48.157.2	Egypt	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.113	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
172.56.6.136	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
128.250.0.213	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
68.180.228.87	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
89.139.151.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
49.231.145.50	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.113	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	2
207.46.13.64	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
137.226.113.7	Germany	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
162.212.253.133	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.75	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
62.138.2.83	Germany	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
162.212.253.133	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.228.75.121	Hungary	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.35	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
222.254.34.165	Vietnam	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.113.119.13	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
162.212.253.133	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
208.54.83.217	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
49.148.182.1	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.45	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
179.99.200.39	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
137.226.113.7	Germany	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.132.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
162.212.253.133	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
216.218.206.79	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
162.212.253.133	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.228.75.149	Hungary	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
2.53.30.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.36	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.56.38.243	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
131.253.36.200	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
222.254.34.165	Vietnam	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
162.212.253.133	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
208.54.86.163	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-01-2016-06:04:05 to 09-01-2016-07:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.1.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.95.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	Multiple NULL Character in Method from 180.97.106.37	Block	1
66.249.64.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
180.97.106.37	China	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
131.253.24.152	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
180.97.106.162	China	147.237.77.233	atal.idf.il	Distributed NULL Character in Method	Block	1
31.154.237.163	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.37	Block	1
104.148.201.34	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/01032011beitar.aspx	Block	1
180.97.106.37	China	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
131.253.26.227	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.102	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
37.26.149.170	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	Multiple NULL Character in Method from 180.97.106.37	Block	1
131.253.24.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
216.244.66.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
65.55.212.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.97.106.37	China	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
131.253.24.140	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	Distributed NULL Character in Method	Block	1
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.37	Block	1
77.126.30.87	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
65.55.212.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
180.97.106.37	China	147.237.76.147	chinuch.aka.idf.il	Distributed NULL Character in Method	Block	1
131.253.24.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/70282.pdf	Block	1
180.97.106.162	China	147.237.77.233	atal.idf.il	Distributed Illegal Byte Code Character in Method	Block	1

09-01-2016-06:04:05 to 09-01-2016-07:04:05