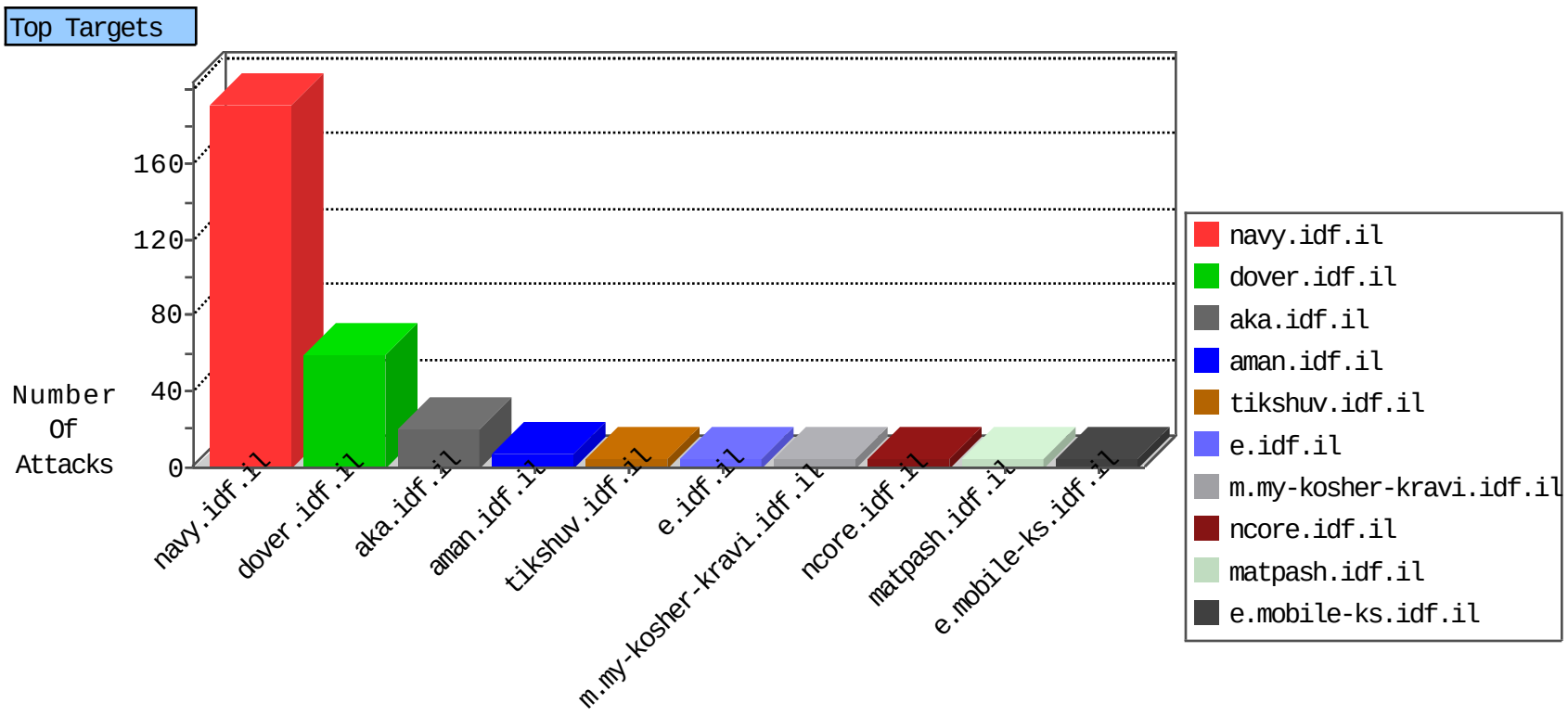
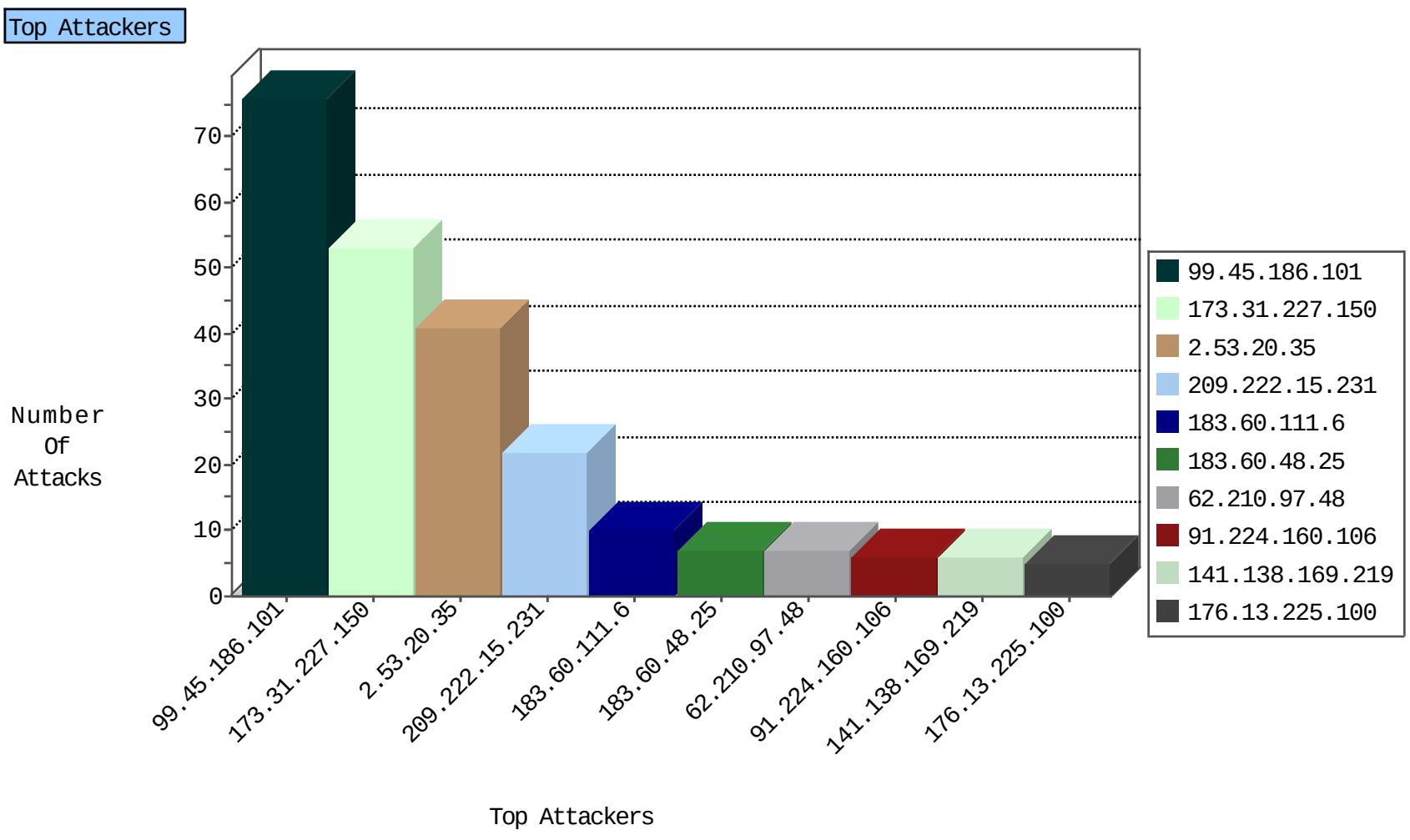
09-22-2016-03:04:06 to 09-22-2016-04:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-22-2016-03:04:06 to 09-22-2016-04:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.236.86.32	Netherlands	147.237.72.156	aman.idf.il	network flood IPv4 TCP-SYN	drop	1
123.151.42.61	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

09-22-2016-03:04:06 to 09-22-2016-04:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.97.48	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
62.210.97.48	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.97.48	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
141.138.169.219	Netherlands	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
82.98.176.41	Spain	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
5.196.64.151	France	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
89.163.213.89	Germany	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
103.27.238.178	Vietnam	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

09-22-2016-03:04:06 to 09-22-2016-04:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
200.241.137.4	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.60.111.6	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
163.172.213.241	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
66.102.6.19	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
183.60.111.6	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
113.105.246.214	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.111.6	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
107.6.179.132	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
183.60.111.6	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.144.3.207	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.111.6	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
212.144.3.207	147.237.72.166	Germany	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
212.92.127.172	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
211.149.201.80	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.154.13.71	147.237.0.34		tikshuv.idf.il	SERVER-WEBAPP backup access	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
74.82.47.12	147.237.77.205	United States	prisha.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
183.60.111.6	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
118.103.126.194	147.237.76.147	Japan	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.111.6	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
113.105.246.214	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.111.6	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.144.3.207	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.49.92	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.111.6	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
212.144.3.207	147.237.72.217	Germany	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
183.60.111.6	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.144.3.207	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.149.222.5	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

09-22-2016-03:04:06 to 09-22-2016-04:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
209.222.15.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	22
99.45.186.101	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
99.45.186.101	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
99.45.186.101	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
99.45.186.101	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
99.45.186.101	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
173.31.227.150	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
2.53.20.35	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
2.53.20.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
173.31.227.150	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
173.31.227.150	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
173.31.227.150	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
173.31.227.150	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
2.53.20.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.225.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.53.20.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.20.35	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	4
82.81.214.189	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.66	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.196.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.228.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.20.35	Israel	147.237.77.216	dover.idf.il	drop		drop	2
189.220.21.156	Mexico	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.67.97.222	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
5.22.134.199	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
104.35.141.143	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
97.106.111.25	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.136	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.112	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.108.21.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.19	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.169	Japan	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.92.127.172	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
97.106.111.25	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
46.116.194.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.16	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.120	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
87.69.224.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.20	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.92.127.172	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
97.106.111.25	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
50.88.124.88	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.16	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
87.69.224.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.26	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
110.5.109.236	Indonesia	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-22-2016-03:04:06 to 09-22-2016-04:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.196.64.151	France	147.237.76.86	navy.idf.il	Parameter Type Violation UncleTypesToIgnore in navy.idf.il/navy/general.aspx	Block	2
50.62.160.139	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	2
82.98.176.41	Spain	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	2
141.138.169.219	Netherlands	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	2
103.27.238.178	Vietnam	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	2
89.163.213.89	Germany	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
41.13.0.128	South Africa	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
149.210.239.204	Netherlands	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
103.27.238.178	Vietnam	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.i	Multiple Unauthorized URL Access from 66.249.79.58	Block	1
141.138.169.219	Netherlands	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
89.163.213.89	Germany	147.237.76.86	navy.idf.il	Parameter Type Violation catId in navy.idf.il/navy/general.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
172.56.12.159	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
104.157.23.184	Canada	147.237.77.216	dover.idf.i	Multiple Untraceable SSL Sessions from 104.157.23.184 (Open Mode)	None	1
66.249.79.58	Israel	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
141.138.169.219	Netherlands	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	1
89.163.213.89	Germany	147.237.76.86	navy.idf.il	Parameter Type Violation docId in navy.idf.il/navy/general.aspx	Block	1
180.76.15.24	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
108.60.209.91	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UpperCatId	Block	1
5.196.64.151	France	147.237.76.86	navy.idf.il	Parameter Type Violation UpperCatId in navy.idf.il/navy/general.aspx	Block	1
103.27.238.178	Vietnam	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
50.62.160.139	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
180.94.113.57	Australia	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
108.60.209.91	United States	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
82.98.176.41	Spain	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
5.196.79.214	France	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
141.138.169.219	Netherlands	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
66.249.66.190	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
207.46.13.63	United States	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
139.162.13.205	Singapore	147.237.77.234	halag.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

09-22-2016-03:04:06 to 09-22-2016-04:04:06