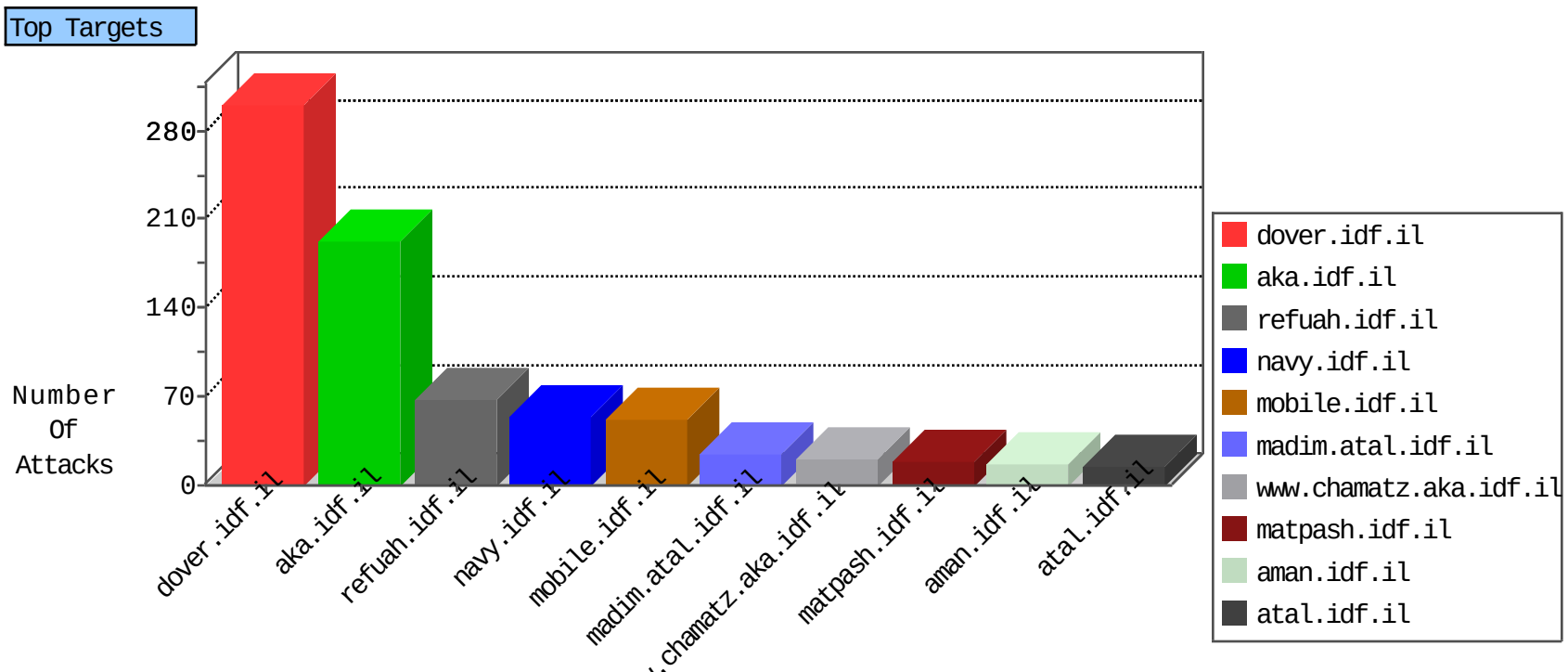
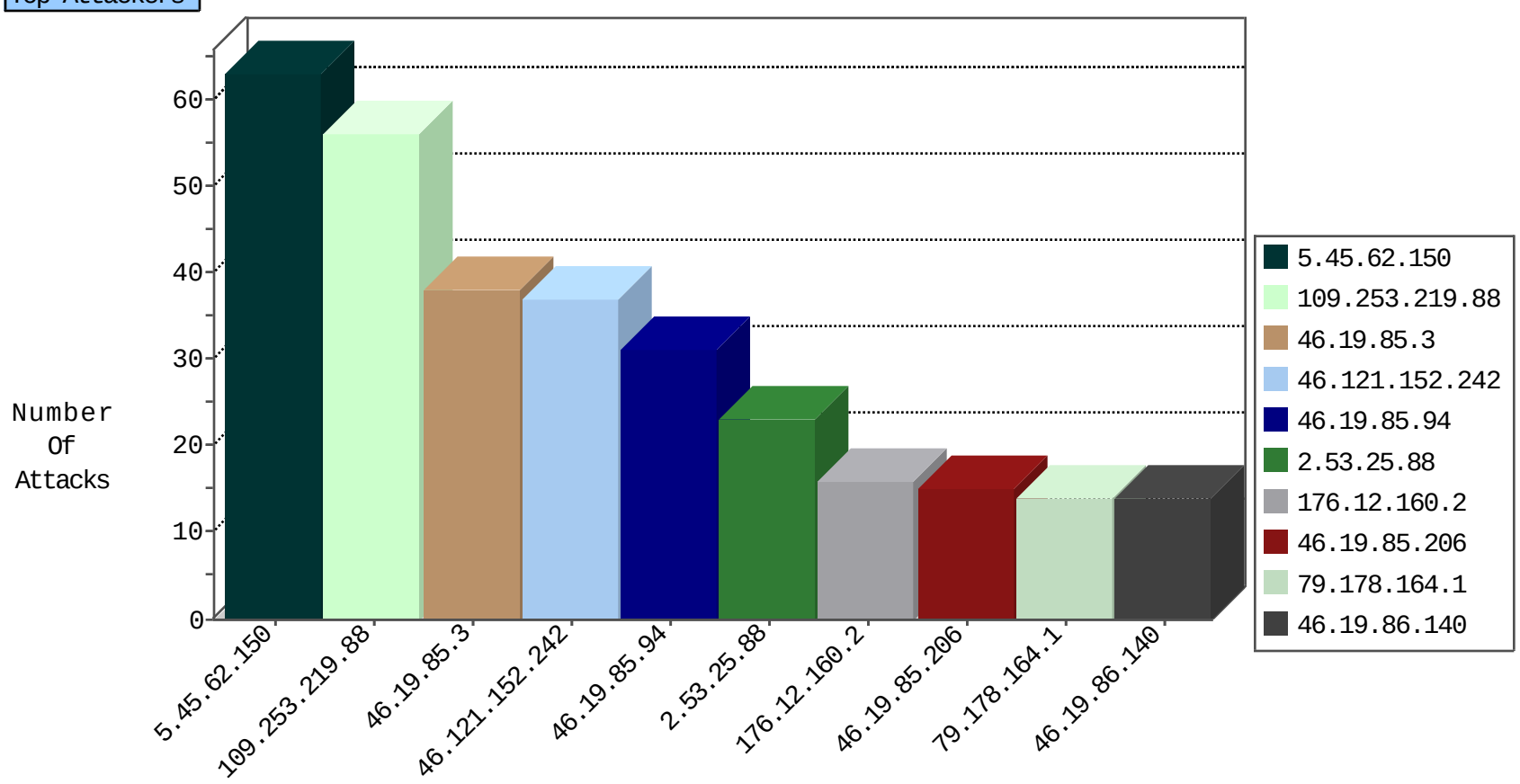
09-21-2016-19:04:06 to 09-21-2016-20:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-19:04:06 to 09-21-2016-20:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.219.88	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
77.138.26.130	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.65.192.59	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	6
109.65.192.59	Israel	147.237.77.216	dover.idf.il	Black List	drop	5
5.29.247.41	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
173.208.197.205	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
89.138.107.66	Israel	147.237.76.42	refuah.idf.il	Black List	drop	2
63.141.231.194	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
63.141.242.194	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
196.200.16.203	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
46.19.85.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
69.30.193.251	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
204.12.220.82	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
173.208.197.206	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
91.230.121.158	Ukraine	147.237.76.44	e.refuah.idf.il	Black List	drop	1
69.30.226.218	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
41.206.63.130	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
139.167.186.232	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.130.255.129	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
63.141.231.197	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
69.30.226.219	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
41.206.63.132	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
142.54.174.82	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
87.69.118.82	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

09-21-2016-19:04:06 to 09-21-2016-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-21-2016-19:04:06 to 09-21-2016-20:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.65.77.214	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
109.65.77.214	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
108.52.13.168	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.93.202	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	1
94.102.56.151	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.149.219.167	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.140.252.90	147.237.76.200	India	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
94.102.56.151	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.140.252.90	147.237.76.176	India	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
128.199.207.123	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.56.151	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.140.252.90	147.237.76.44	India	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
128.199.83.245	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.56.151	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.140.252.90	147.237.76.34	India	yohalan.idf.il	ET SCAN Potential SSH Scan	1
110.5.109.236	147.237.77.170	Indonesia	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
109.65.174.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.25.57	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
100.13.130.4	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
94.102.56.151	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.97.106.37	147.237.76.38	China	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
41.251.250.250	147.237.77.216	Morocco	dover.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.56.151	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.140.252.90	147.237.76.198	India	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
139.167.186.232	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.56.151	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
14.140.252.90	147.237.76.86	India	navy.idf.il	ET SCAN Potential SSH Scan	1
128.199.167.194	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.56.151	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.140.252.90	147.237.76.38	India	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
128.199.81.128	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.56.151	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.140.252.90	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.253.219.88	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1

09-21-2016-19:04:06 to 09-21-2016-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.121.152.242	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
5.45.62.150	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
109.253.219.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
5.45.62.150	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
46.19.85.206	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.3	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.140	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
80.246.139.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
178.137.153.235	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.170.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.164.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.43.101.227	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.12.160.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.194	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
109.253.156.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
104.179.115.161	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
207.241.226.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.85.3	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.219.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.25.88	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence		monitor	5
46.19.86.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
85.130.255.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.71.48.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.46.39.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.5.104	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.12.160.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
85.130.255.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.160.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.255.129	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.66.26.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.207.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.25.88	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.3.147.210	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
5.45.62.150	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
85.64.6.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.55.12.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.139.51.92	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
134.35.143.3	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.25.88	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.45.62.150	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

09-21-2016-19:04:06 to 09-21-2016-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.196.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
189.212.232.21	Mexico	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 189.212.232.21	Block	4
213.57.187.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
77.139.85.105	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.85.105	Block	4
79.178.250.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.207.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.49.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.160.243	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
2.53.135.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.85.105	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
185.32.179.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.5.82	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.77.214	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal	Block	1
79.179.147.136	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
77.138.121.76	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
207.46.13.31	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
2.53.183.242	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
176.13.12.212	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
84.108.127.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.226.111	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
185.120.124.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.86.175	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
2.53.25.0	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
79.183.42.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/null	Block	1
77.139.34.105	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.34.105	Block	1
207.46.13.93	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.47.169.77	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
77.139.232.45	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.232.45	Block	1
46.121.152.242	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
2.53.25.88	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.179.9.7	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
77.139.34.105	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
181.215.117.117	United States	147.237.77.234	halag.idf.il	Distributed PHP Attempt	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
109.65.77.214	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/edim	Block	1
77.139.232.45	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
189.212.232.21	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
80.179.9.115	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
181.215.117.117	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/blog/wp-login.php	Block	1
46.19.85.68	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
109.65.77.214	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.65.77.214	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
192.116.52.137	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
2.53.136.224	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc	Block	1
157.55.39.195	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
82.102.169.113	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1

09-21-2016-19:04:06 to 09-21-2016-20:04:06