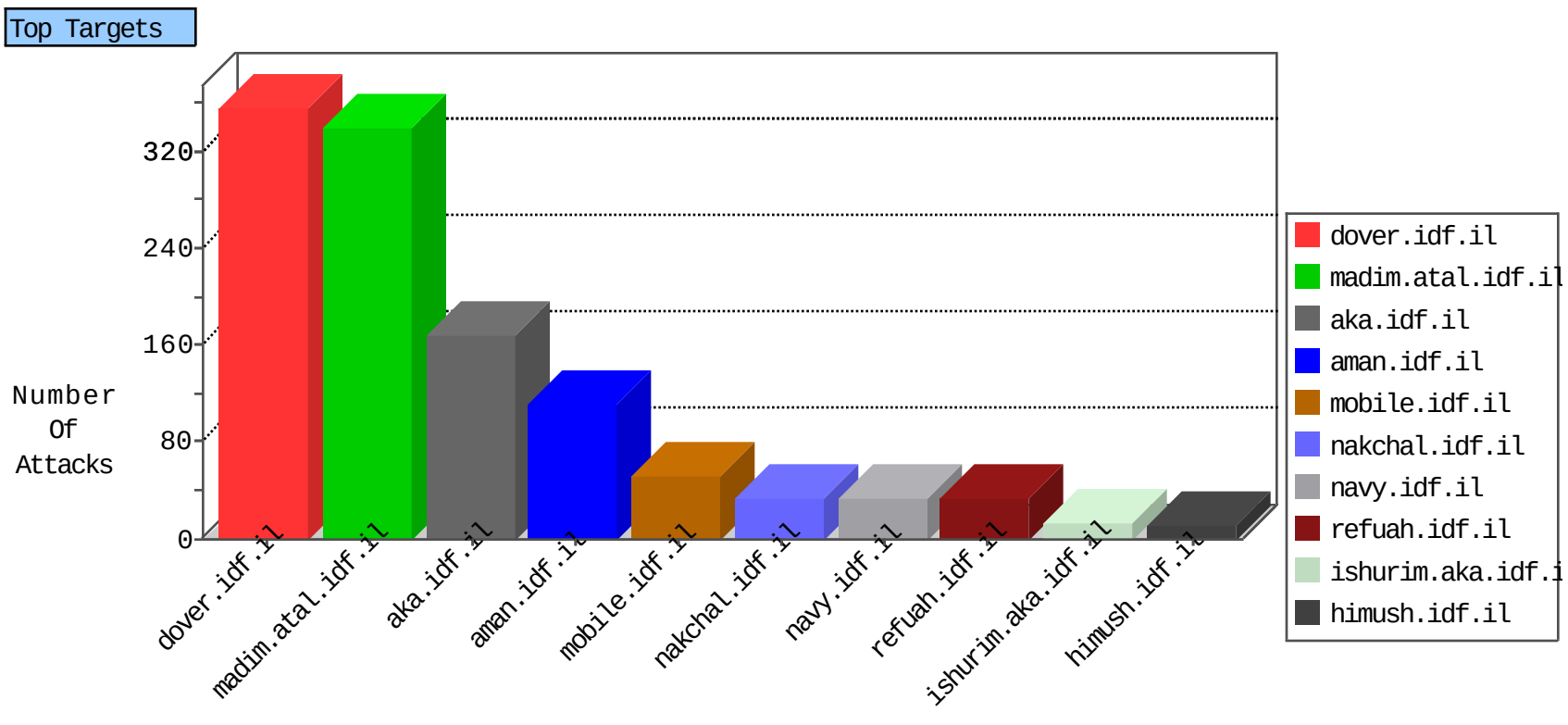
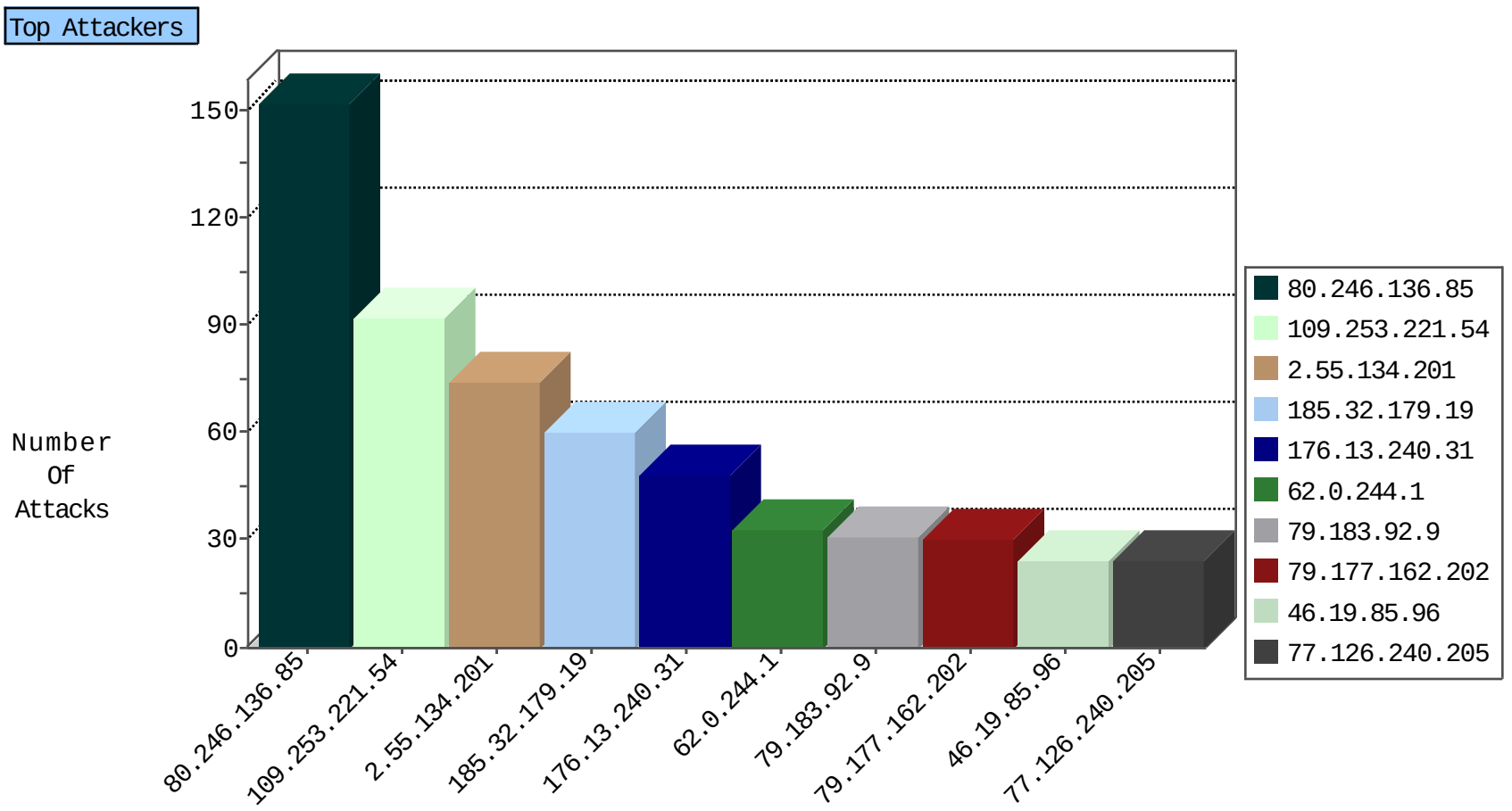
09-20-2016-17:04:02 to 09-20-2016-18:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-17:04:02 to 09-20-2016-18:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.134.201	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	54
93.192.105.18	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	42
46.19.85.99	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	30
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
185.24.207.117	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
157.55.39.37	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
62.0.244.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
173.208.150.116	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
142.54.174.83	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
79.183.92.9	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	2
173.208.197.204	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
173.208.197.206	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
69.30.193.251	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
45.32.205.133	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
173.208.150.115	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
84.94.0.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
45.32.196.8	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
142.54.174.82	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
69.30.193.253	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
63.141.242.197	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
45.32.196.8	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
52.53.222.9	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
63.141.242.197	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
45.32.196.8	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-20-2016-17:04:02 to 09-20-2016-18:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-20-2016-17:04:02 to 09-20-2016-18:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.183.92.9	147.237.76.86	Israel	navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	23
109.64.25.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.48.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.246.60	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
195.244.23.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.70.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.16.127.148	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
79.182.95.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.58.37.44	147.237.77.74	Russian Federation	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
62.0.117.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.22.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.67.13	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.67.13	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential SSH Scan	1
5.29.190.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.62.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.170.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.157.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.76.38	Russian Federation	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
1.52.248.240	147.237.77.233	Vietnam	atal.idf.il	ET SCAN NMAP -sS window 3072	1
200.6.65.102	147.237.76.202	Chile	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.155	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
195.16.127.148	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
195.16.127.148	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	1
64.88.214.136	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.148.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.127.12.96	147.237.72.156	Taiwan	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.67.13	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN Potential SSH Scan	1
41.160.222.18	147.237.76.31	South Africa	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.67.13	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.249.158.39	147.237.76.44	Italy	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
139.162.13.205	147.237.8.45	Singapore	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
2.55.51.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.132.76.99	147.237.72.156	Taiwan	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-20-2016-17:04:02 to 09-20-2016-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.162.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.164.25.10	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.96	Israel	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
62.0.244.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
2.55.134.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.55.134.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
2.55.134.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
176.13.240.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
62.0.244.1	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	12
2.53.146.115	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
91.135.102.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
93.192.105.18	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
77.126.240.205	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
91.135.102.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
87.68.32.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.46.41.62	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
85.114.124.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
89.138.125.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.96	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.111.162.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.46.41.62	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.159.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.114.124.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.53.15.170	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
87.68.32.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.240.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.120.208.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.240.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.0.244.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.1.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.240.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
176.13.240.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.53.170.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.111.162.55	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
31.168.108.150	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.240.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.114.124.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.53.42.108	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
109.253.197.124	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4

09-20-2016-17:04:02 to 09-20-2016-18:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
109.253.221.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
185.32.179.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.253.156.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.117.24.100	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.24.100	Block	7
37.26.149.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.120.18.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
68.188.68.66	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 68.188.68.66	Block	5
2.53.31.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.154.81.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.154.81.55	Block	3
2.53.44.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
68.188.68.66	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	3
5.102.253.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.227.23	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.117.24.100	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/pniotfindanswer.aspx	Block	2
77.139.134.243	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
109.253.138.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.30.230	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	2
2.53.17.24	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.139.41.227	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/miluim/templates/inner.asp	Block	2
77.138.86.3	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunpersonalquestionnaire.aspx	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
46.19.86.219	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version deflate	Block	1
77.139.61.220	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
204.79.180.13	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
87.69.64.132	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.157	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.182.61.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.22.226	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$hiddenUpdateEmail in www.aka.idf.il/main/giyus/faq.aspx	None	1
31.154.81.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.86.219	Israel	147.237.76.31	nakchal.idf.il	Malformed URL gzip,	Block	1
46.19.85.6	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
2.53.56.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.99.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/faq.aspx	Block	1
46.19.86.157	Israel	147.237.77.234	halag.idf.il	Unknown HTTP Request Method ku3 in URL	Block	1
79.182.109.86	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.139.22.226	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsList$ctl00$cbEmailSubject in www.aka.idf.il/main/giyus/faq.aspx	None	1
31.168.108.150	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 31.168.108.150 (Open Mode)	None	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
46.19.86.219	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method Accept-Encoding: in URL gzip,	Block	1
46.19.86.157	Israel	147.237.77.234	halag.idf.il	Malformed URL	Block	1
77.139.143.97	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.143.97	Block	1
2.55.146.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.126.89.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-20-2016-17:04:02 to 09-20-2016-18:04:02