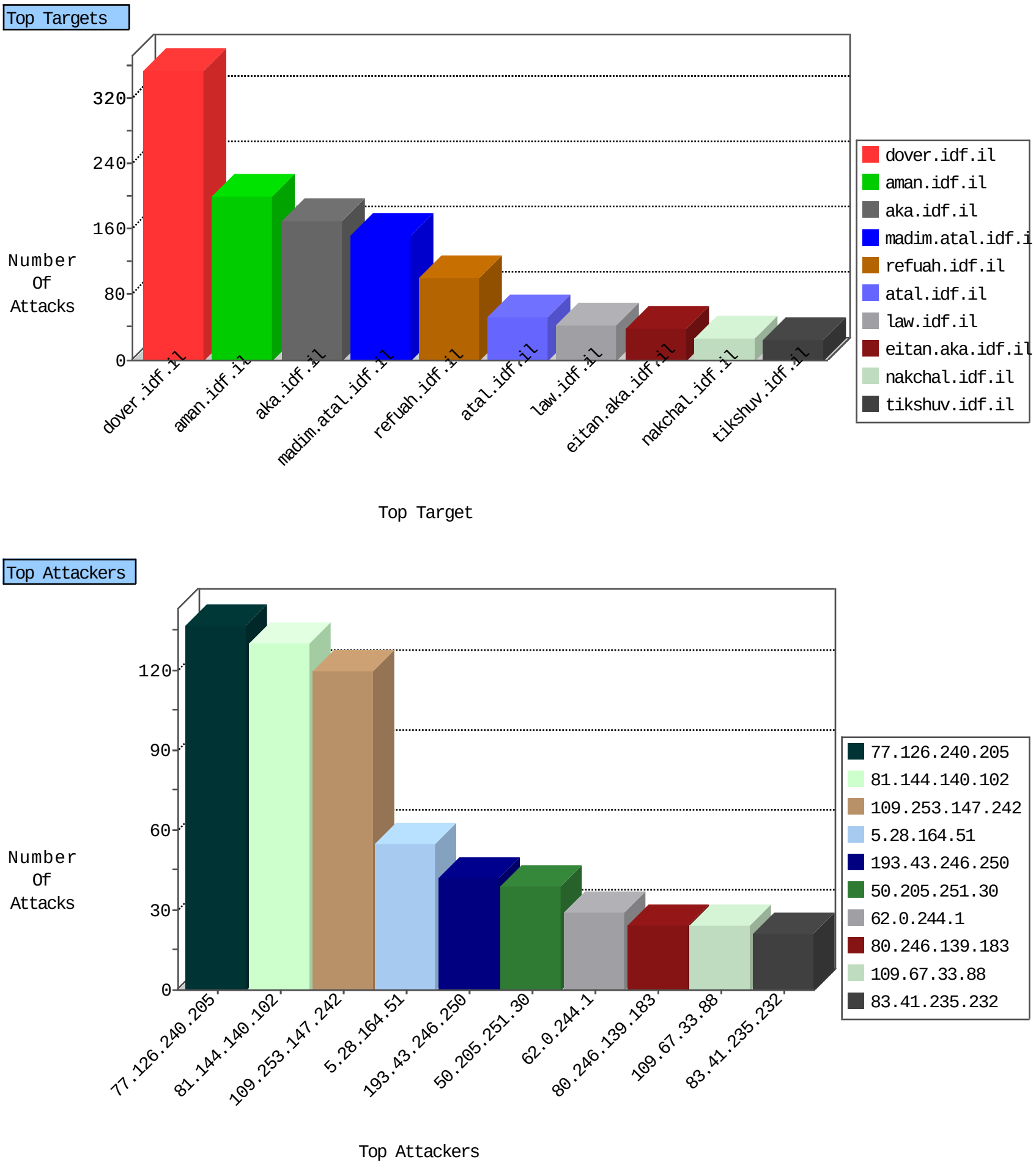
09-20-2016-16:04:00 to 09-20-2016-17:04:00

IDF Under Attack Daily Report



09-20-2016-16:04:00 to 09-20-2016-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.25.74.130	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
45.32.201.228	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
123.151.42.61	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

09-20-2016-16:04:00 to 09-20-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.97.48	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.97.48	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
89.248.172.16	Netherlands	147.237.0.19	madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-20-2016-16:04:00 to 09-20-2016-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
27.24.237.9	147.237.77.234	China	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
220.132.224.48	147.237.8.14	Taiwan	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
58.227.55.118	147.237.0.15	Korea, Republic of	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
46.19.85.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.255.90.133	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
85.65.213.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.185.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.205.254	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
84.108.168.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.35.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.73.143.36	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.106.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.162.13.205	147.237.77.233	Singapore	atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.87.109.253	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.109	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
128.232.110.28	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
46.117.30.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.59.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.91.29	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.237.138.3	147.237.72.166	Poland	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.155	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
217.132.155.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.203.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.132.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.163.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.251.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.86	United States	navy.idf.il	ET DROP Dshield Block Listed Source	1
79.176.77.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
138.59.200.75	147.237.77.121	Brazil	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
125.213.243.10	147.237.77.212	Thailand	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.140.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.219.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-20-2016-16:04:00 to 09-20-2016-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	136
81.144.140.102	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
5.28.164.51	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
193.43.246.250	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	42
109.67.33.88	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.48.40.17	Czech Republic	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
50.205.251.30	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
50.205.251.30	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
62.0.244.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
62.0.244.1	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.89	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
80.179.114.19	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.98.99	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
84.109.202.100	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.85	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.109.202.100	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
176.13.240.254	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.179.104.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
83.41.235.232	Spain	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
77.138.37.189	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.52	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.138.37.189	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.67.253.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.90.91	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.246.139.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
109.67.253.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
50.138.15.23	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
80.246.139.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
141.226.217.111	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
50.138.15.23	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
80.246.139.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.176.49.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.139.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.52	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.139.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.64.77	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-20-2016-16:04:00 to 09-20-2016-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
2.53.31.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.253.221.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.29.242.233	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
37.26.148.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.156.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.203.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
80.246.136.15	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
195.78.246.252	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/news.aspx	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
207.46.13.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
81.218.241.25	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
157.55.39.99	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
66.249.76.71	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
10.161.110.40		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar	Block	1
79.179.106.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
46.19.86.163	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
109.64.143.117	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
139.162.13.205	Singapore	147.237.76.200	eitan.aka.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.116.20.24	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
5.254.65.3	Turkey	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.254.65.3	Block	1
81.218.251.252	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 77.126.240.205 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
37.26.148.223	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.65.182.48	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/piwik.php	Block	1
81.83.158.121	Belgium	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
176.13.232.11	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
139.162.13.205	Singapore	147.237.77.233	atal.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21531-he/idfgdover.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/homepage/div.item	Block	1
5.254.65.3	Turkey	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/drushim	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
77.138.197.23	France	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
40.77.167.73	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
109.253.130.209	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.95.208.20	Israel	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	1
5.28.164.51	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
81.218.37.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1

09-20-2016-16:04:00 to 09-20-2016-17:04:00