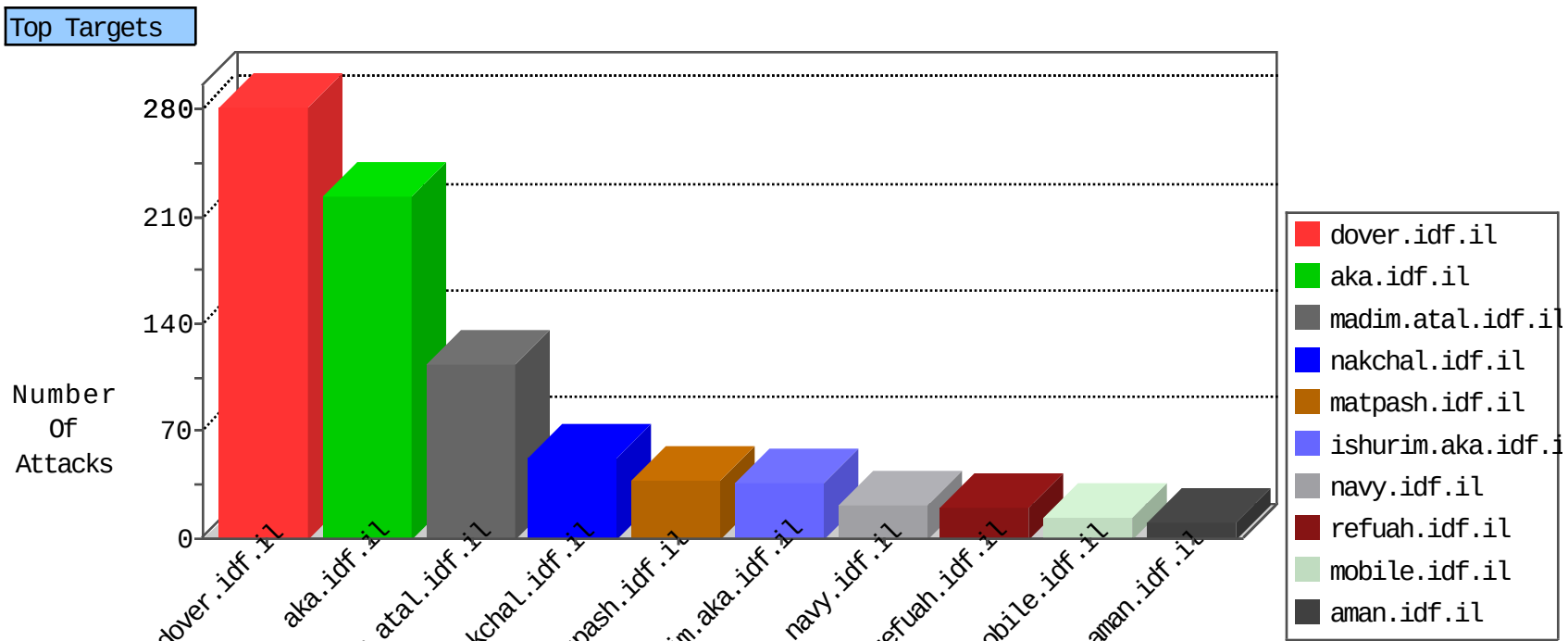
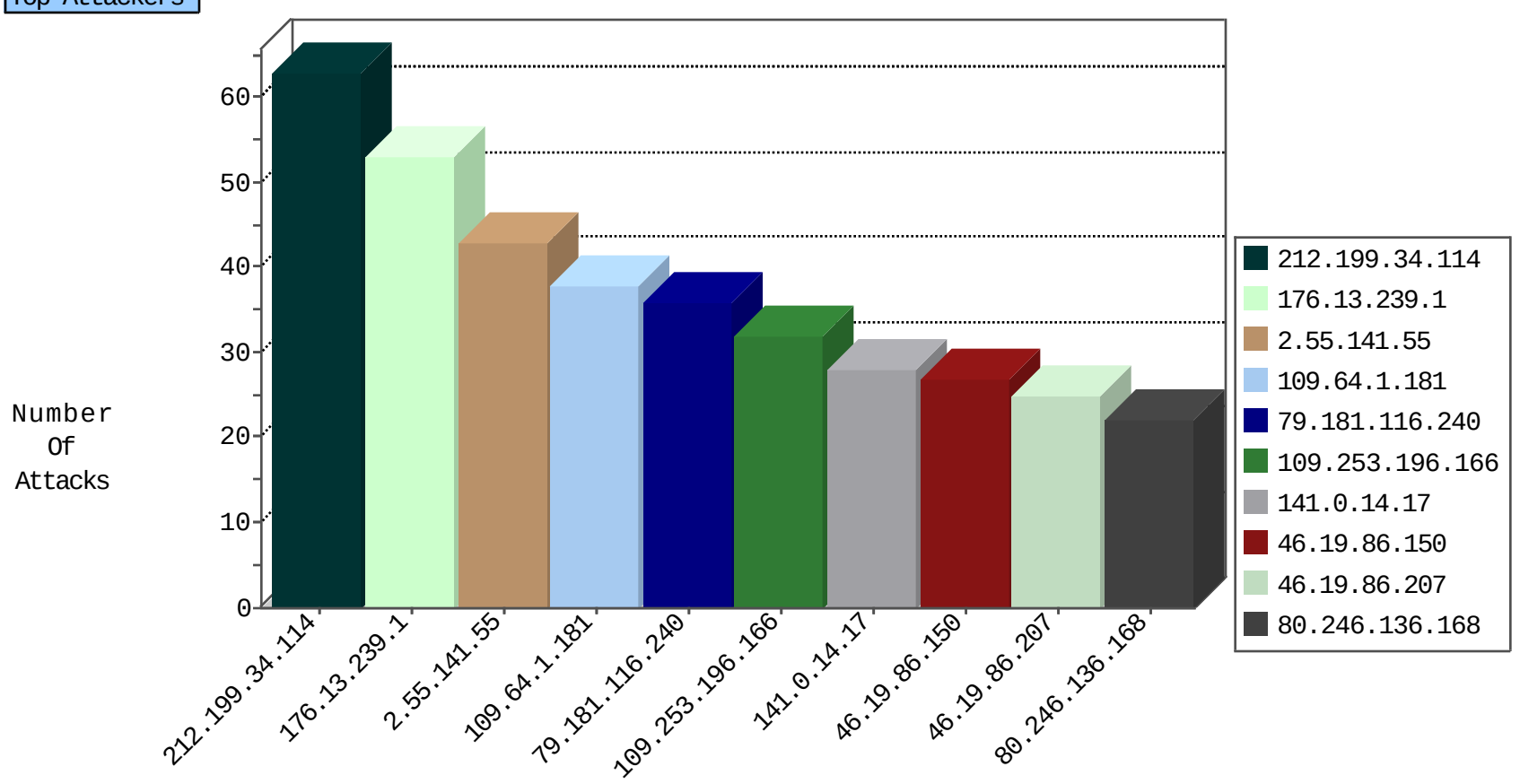
09-15-2016-17:04:05 to 09-15-2016-18:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-15-2016-17:04:05 to 09-15-2016-18:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.234.50	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
176.13.239.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
109.253.157.174	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
84.229.31.74	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
192.91.235.230	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-15-2016-17:04:05 to 09-15-2016-18:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.70.206.108	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-15-2016-17:04:05 to 09-15-2016-18:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.168.144.253	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
191.235.92.192	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
133.208.21.66	147.237.72.167	Japan	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
123.136.27.66	147.237.8.27	Bangladesh	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
109.253.129.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.5.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.212.179.106	147.237.77.121	Canada	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.69.91.149	147.237.0.35	United States	akaws.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
2.53.27.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
191.235.92.192	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
132.74.208.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.146.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.115.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.20.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.132.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.180.8.100	147.237.0.200	South Africa	m4u.idf.il	ET SCAN Potential SSH Scan	1
2.55.140.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-15-2016-17:04:05 to 09-15-2016-18:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.55.141.55	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
141.0.14.17	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	28
176.13.239.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.86.245	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
46.19.85.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
176.13.239.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
212.199.34.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.53.17.203	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.199.34.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.64.1.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
46.19.86.228	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.86.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.178.226.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.55.22.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
176.13.239.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.63	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.64.1.181	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.199.34.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
85.65.22.142	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
80.178.150.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
212.199.34.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
87.69.32.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
109.64.1.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.124.27	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
46.19.86.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.1.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.1.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.64.157.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.231.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.199.34.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.253.157.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.168	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.193.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.7.100.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.7.100.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
85.64.3.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.213.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.60	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.146.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.213.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.28.148.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-15-2016-17:04:05 to 09-15-2016-18:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.116.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
109.253.196.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.19.86.207	Block	24
80.246.136.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
89.138.121.248	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	3
2.53.171.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.124.23.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.230.218.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.34.12.63	Jordan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method 0.1; in URL d6503	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/.well-known/apple-app-site-association	Block	1
95.86.84.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in aka.idf.il/main/sachar/payslips.aspx	None	1
80.230.219.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
181.214.61.149	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to chinuch.aka.idf.il/wp-login.php	Block	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1	Block	1
80.230.219.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.218.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.76.103.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
109.65.98.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
84.108.47.41	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
31.154.81.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.230.219.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.34.12.63	Jordan	147.237.77.176	matpash.idf.il	Abnormally Long Request request version	Block	1
46.116.108.103	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
89.138.188.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in aka.idf.il/main/sachar/payslips.aspx	None	1
80.230.219.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.218.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
109.253.132.252	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
77.138.78.215	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
84.109.115.200	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
80.230.219.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.34.12.63	Jordan	147.237.77.176	matpash.idf.il	Illegal HTTP Version Build/23.5.A.1.291) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.98 Mobile Safari/537.36	Block	1
79.182.113.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.219.243.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
92.126.212.98	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
80.230.219.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.53.3.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.230.218.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
85.65.209.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
41.60.25.38	Zambia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
80.230.219.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.218.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.34.12.63	Jordan	147.237.77.176	matpash.idf.il	Malformed URL d6503	Block	1
66.102.9.5	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
93.172.105.98	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
2.53.44.219	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
80.230.219.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1

09-15-2016-17:04:05 to 09-15-2016-18:04:05