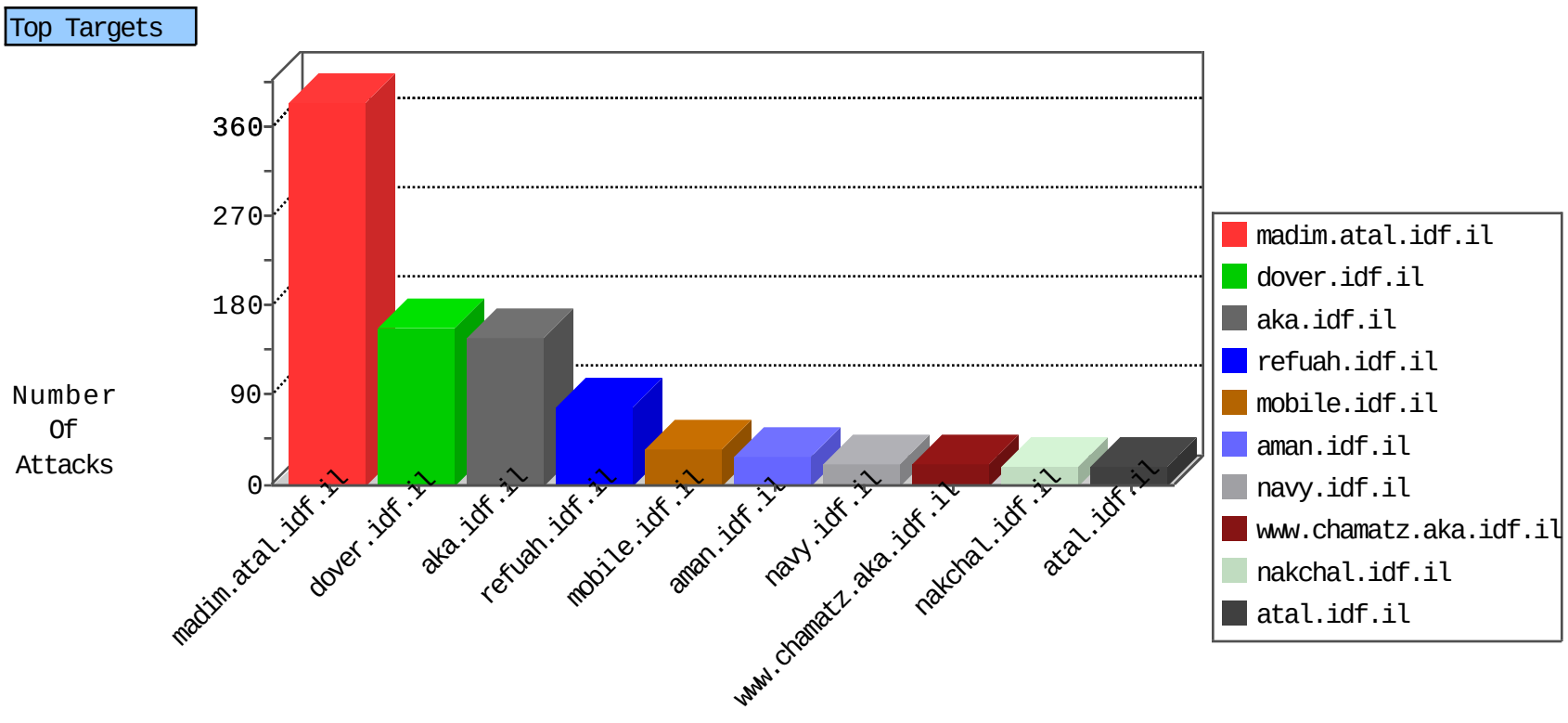
09-18-2016-14:04:01 to 09-18-2016-15:04:01

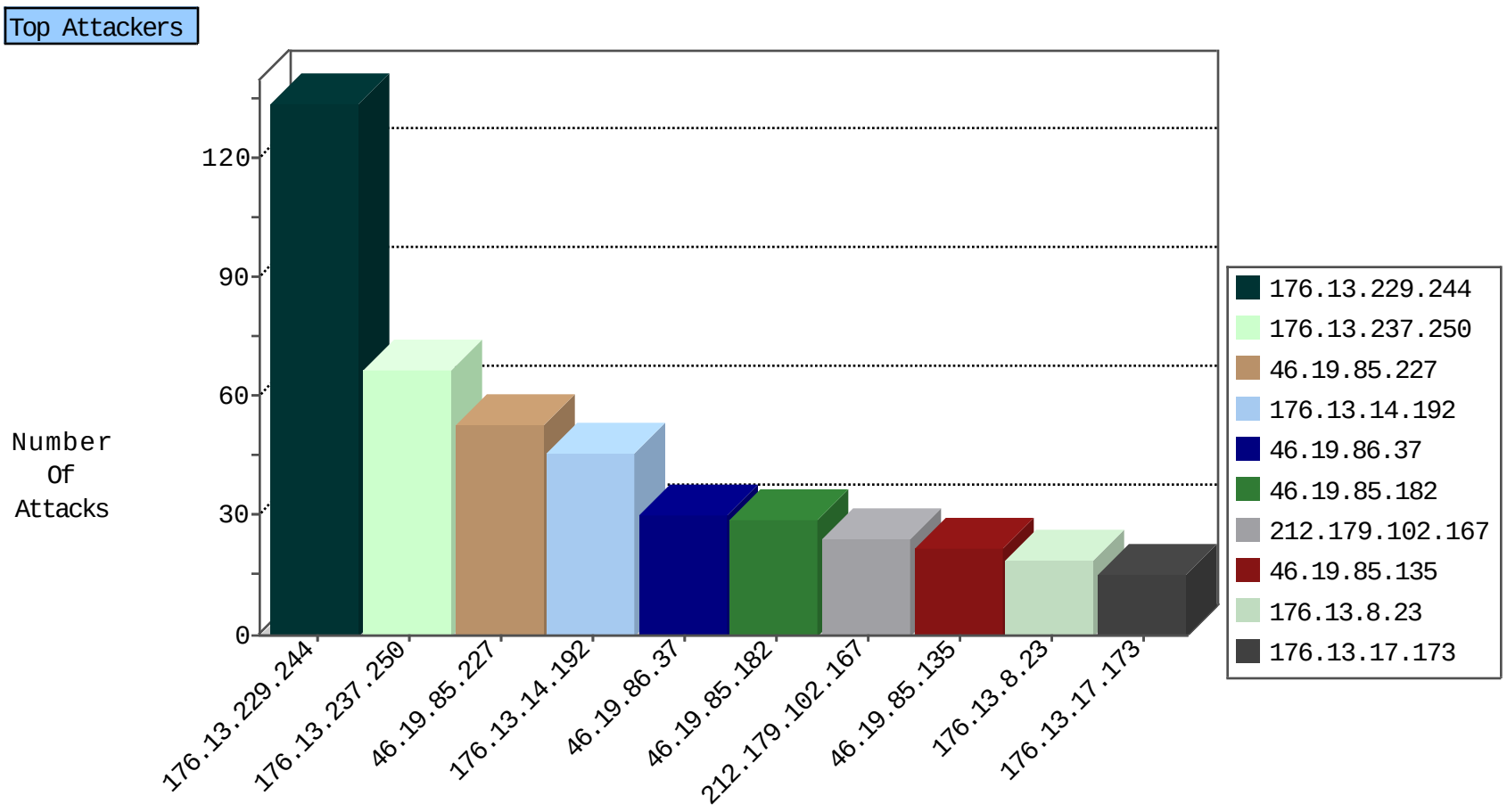
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-18-2016-14:04:01 to 09-18-2016-15:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.31.176	Israel	147.237.77.216	dover.idf.il	Black List	drop	6
82.81.97.181	Israel	147.237.76.42	refuah.idf.il	Black List	drop	3
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.110.84.66	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	1
142.54.174.85	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.197	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.150.114	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-14:04:01 to 09-18-2016-15:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4

09-18-2016-14:04:01 to 09-18-2016-15:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.228.229.138	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.146.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.181.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.214.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.146.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.121.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.70.241	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.217.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.151.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
124.64.215.106	147.237.77.178	China	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.148.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.213.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.233.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.163.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.153.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.211.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.58.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.20.134	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
66.249.93.73	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.117.61.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.128.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-18-2016-14:04:01 to 09-18-2016-15:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.135	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.182	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
77.126.83.231	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.86.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.179.102.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.179.102.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.179.7.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
212.179.102.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
213.57.88.118	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.135	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
213.57.88.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.53.29.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.92.63.229		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.210.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.130.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.196.17	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.53.130.58	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.130.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.0.247.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
147.235.8.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.172.199	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.35	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.55.156.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.170	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.11.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.182	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.8.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.32.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.179.32.87	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
77.126.83.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
192.116.83.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

09-18-2016-14:04:01 to 09-18-2016-15:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.229.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
176.13.237.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
176.13.14.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
176.13.8.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
176.13.17.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
46.19.85.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.247.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
109.67.169.98	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	10
2.55.27.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
212.235.98.139	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	7
212.235.98.139	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.235.98.139	Block	6
2.53.38.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.156.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
185.120.125.181	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
212.179.127.106	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
69.47.161.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	3
209.35.30.20	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.175	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	3
79.183.70.168	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	3
77.139.50.140	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotfaq.aspx	Block	2
93.172.148.107	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.139.109.23	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
37.142.232.39	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
2.55.140.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.179.32.87	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.235	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
84.109.153.62	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
217.132.150.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
109.253.133.125	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
77.138.159.106	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
165.231.90.186	France	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
46.19.85.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.155.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.25.119.193	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.138.239	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
37.142.232.39	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 37.142.232.39	Block	1
212.235.98.139	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
79.183.70.168	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.183.70.168	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main.giyus	Block	1
165.231.90.186	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/wordpress/wp-login.php	Block	1
77.138.194.135	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	1
93.172.148.107	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

09-18-2016-14:04:01 to 09-18-2016-15:04:01