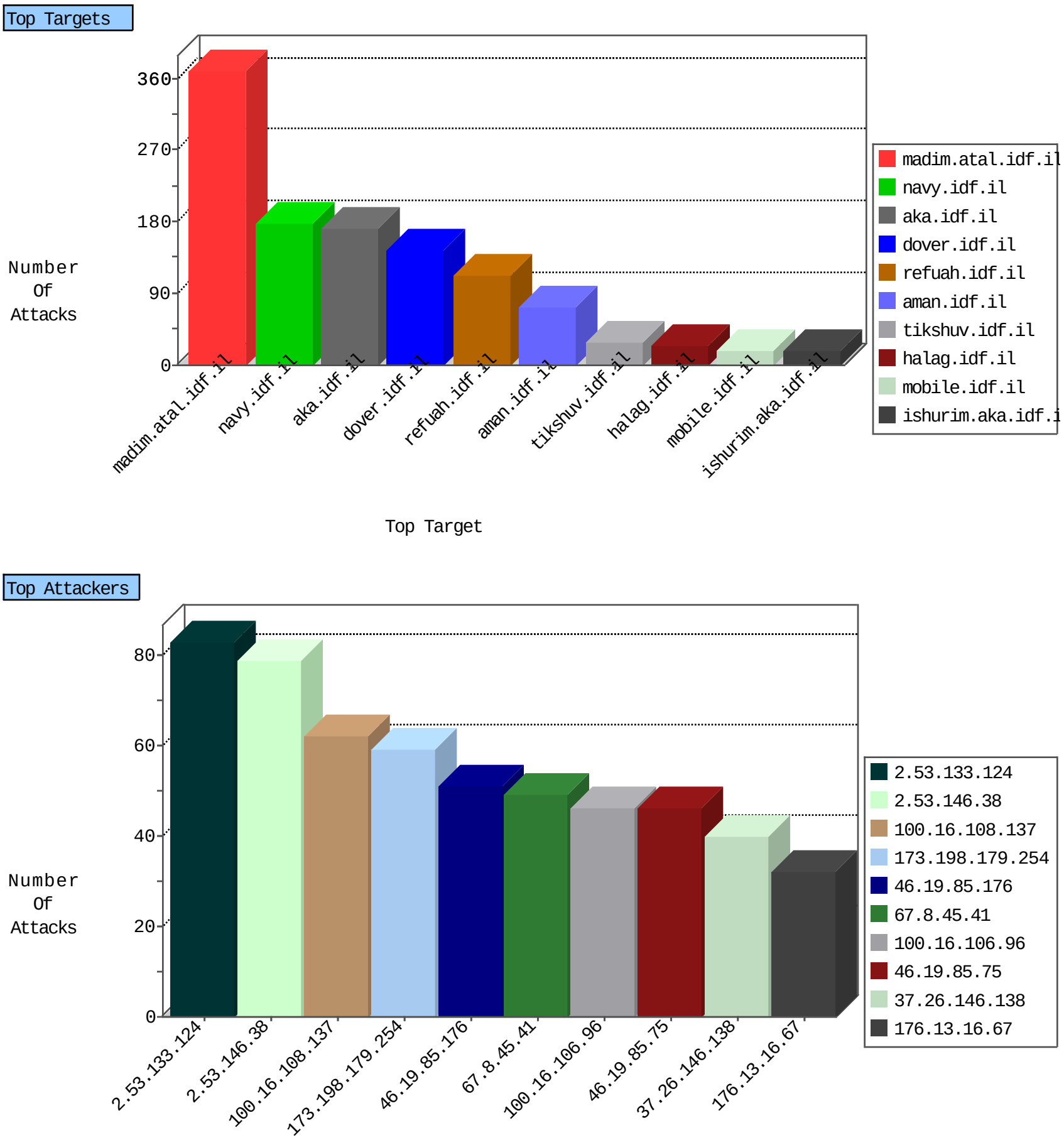
09-11-2016-08:04:09 to 09-11-2016-09:04:09

IDF Under Attack Daily Report



09-11-2016-08:04:09 to 09-11-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.14	Canada	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
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.110.125.52	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.156	aman.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
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1

09-11-2016-08:04:09 to 09-11-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
1.179.134.194	Thailand	147.237.77.216	dover.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
199.87.254.195	United States	147.237.77.74	law.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

09-11-2016-08:04:09 to 09-11-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
173.198.179.254	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
104.148.120.134	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
89.138.109.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.181.50.63	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.129.15	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.253.139.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.38	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.148.120.134	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.81.5.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.152.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.76.122.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.36.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
191.96.249.18	147.237.77.176	Chile	matpash.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.65.106.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-11-2016-08:04:09 to 09-11-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.16.108.137	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	62
67.8.45.41	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	49
100.16.106.96	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	46
173.198.179.254	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
176.13.16.67	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
173.198.179.254	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
88.101.183.181	Czech Republic	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
109.253.195.225	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.148.218	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.246.139.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.55.173.170	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
109.253.206.122	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.70.30.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
87.70.30.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
31.168.164.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.124.61.44	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.233.151	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.252.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.179.9.7	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.115.177.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.234.234	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.198	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.143.80.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.110	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
81.218.66.107	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.148.198	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.230.14	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
173.192.200.77	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.52.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.136	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-11-2016-08:04:09 to 09-11-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.133.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.53.146.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
37.26.146.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
80.246.137.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
79.177.17.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
2.55.173.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.246.137.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.193.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.119.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.51.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.1	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.133.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
176.13.13.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.231	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
176.13.16.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
173.63.18.62	United States	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
77.139.192.160	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
185.27.106.72	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
139.162.13.205	Singapore	147.237.77.234	halag.idf.il	NULL Character in Method [[#0]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]]	Block	1
37.26.148.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.53.61.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.36.20	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
173.180.24.211	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.121.252.215	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
139.162.13.205	Singapore	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Header Name	Block	1
85.65.55.187	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
139.162.13.205	Singapore	147.237.77.234	halag.idf.il	Unknown HTTP Request Method [[#0]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]] in URL	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
109.253.195.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
213.151.52.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
80.246.139.97	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
173.198.179.254	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
54.196.97.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
139.162.13.205	Singapore	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method [[#0]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]]	Block	1
185.32.179.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
144.76.16.162	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
139.162.13.205	Singapore	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.140.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.110	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
139.162.13.205	Singapore	147.237.77.234	halag.idf.il	Malformed URL	Block	1
109.66.53.75	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 109.66.53.75	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
150.70.173.6	Japan	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
2.53.183.71	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
139.162.13.205	Singapore	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
82.80.55.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-11-2016-08:04:09 to 09-11-2016-09:04:09