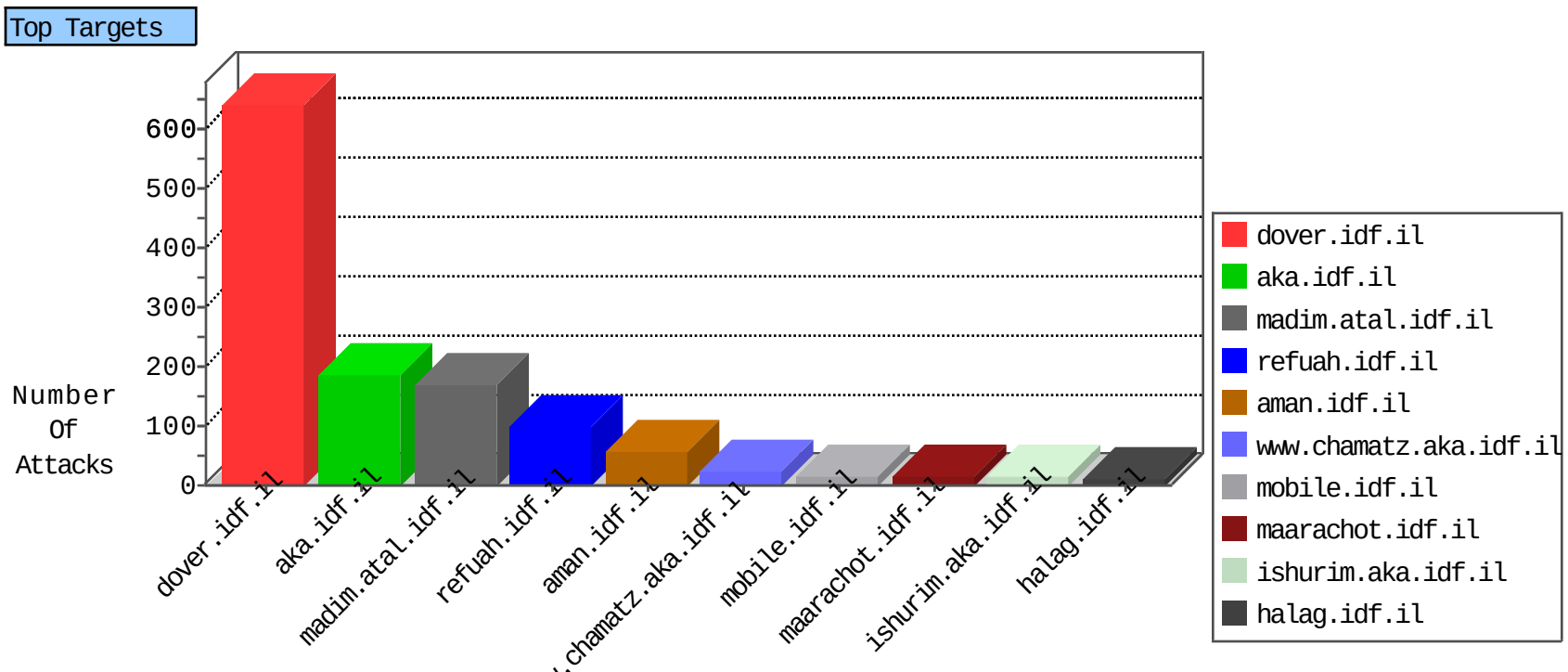
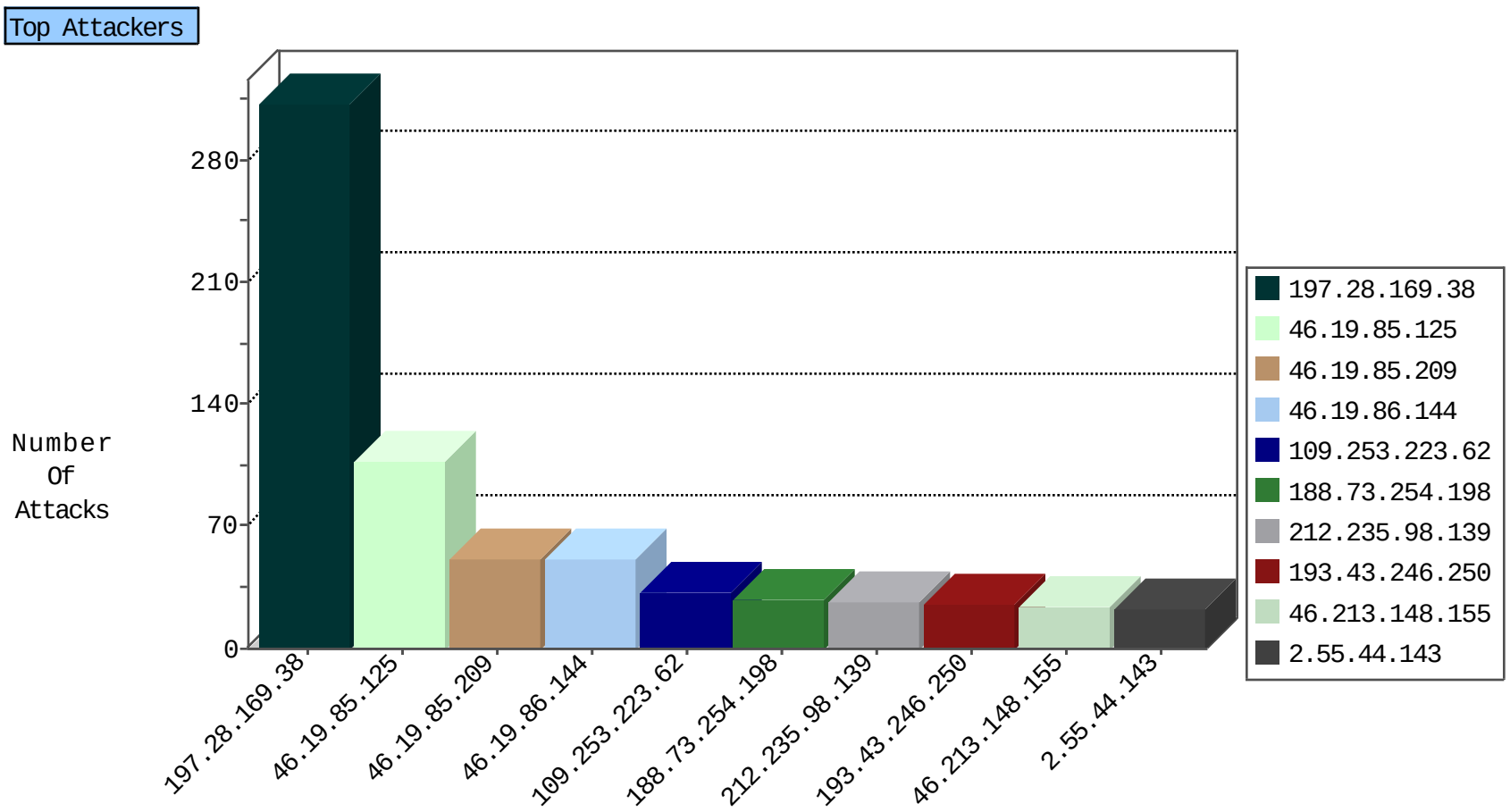
09-13-2016-15:04:08 to 09-13-2016-16:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-13-2016-15:04:08 to 09-13-2016-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.118.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
5.102.220.105	Israel	147.237.72.166	aka.idf.il	Black List	drop	10
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	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	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.186.163.3	Greece	147.237.72.166	aka.idf.il	Black List	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-15:04:08 to 09-13-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.141.46	France	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
136.243.152.18	Germany	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
88.228.43.156	Turkey	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	1
88.228.43.156	Turkey	147.237.72.166	aka.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

09-13-2016-15:04:08 to 09-13-2016-16:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
141.226.218.45	147.237.72.167	Israel	ishurim.aka.idf.i	INDICATOR-SCAN myscan	2
141.226.218.45	147.237.72.167	Israel	ishurim.aka.idf.i	GPL SCAN myscan	2
2.53.185.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.255.20.103	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.68.60.154	147.237.77.216	Israel	dover.idf.il	GPL SCAN superscan echo	1
185.120.125.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.60.154	147.237.77.170	Israel	maarachot.idf.il	GPL SCAN superscan echo	1
82.81.51.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.219.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.187.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.12.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.239.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.96.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
40.121.139.43	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.60.154	147.237.77.234	Israel	halag.idf.il	GPL SCAN superscan echo	1
37.142.202.3	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
87.68.60.154	147.237.77.227	Israel	e.hamaz.idf.il	GPL SCAN superscan echo	1
188.161.35.211	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
87.68.60.154	147.237.77.205	Israel	prisha.idf.il	GPL SCAN superscan echo	1
167.0.168.182	147.237.77.212	Colombia	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.108.164.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.133.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.171.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.92.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.44.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.138.134.26	147.237.77.216	Sweden	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.86.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.60.154	147.237.77.235	Israel	sviva.idf.il	GPL SCAN superscan echo	1
37.142.202.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.60.154	147.237.77.233	Israel	atal.idf.il	GPL SCAN superscan echo	1

09-13-2016-15:04:08 to 09-13-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	304
46.19.86.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
212.235.98.139	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	27
188.73.254.198	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.86.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
212.150.128.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
109.253.223.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
217.132.131.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
46.213.148.155	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.213.148.155	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.223.62	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.229.127.94	Sweden	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
87.69.36.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
96.224.5.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.142.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.244.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.127.10.35	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.85.178	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.69.36.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
178.199.147.77	Switzerland	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.202	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.223.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
93.173.19.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.54.97.123	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
205.197.242.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.124.29.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.202	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.55.49.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
141.226.218.45	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.138.147.13	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
176.13.251.131	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
141.226.218.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

09-13-2016-15:04:08 to 09-13-2016-16:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.53.166.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.55.44.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
46.121.40.183	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.244.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
94.188.162.199	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	5
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.105	Block	4
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.134.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	2
137.54.125.247	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
46.116.42.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.37	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.246.137.37	Block	2
79.177.53.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.26	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	2
80.246.137.37	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
37.26.149.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
94.188.162.199	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 94.188.162.199	Block	2
77.126.25.123	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
217.132.131.182	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
80.246.133.234	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
192.114.1.155	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/113440.pdf	Block	1
85.93.91.84	Germany	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
46.19.85.61	Israel	147.237.76.147	chinuch.aka.idf.il	Malformed URL	Block	1
2.53.3.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl37 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.138.190.78	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
188.73.254.198	Greece	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 188.73.254.198	Block	1
66.102.9.2	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
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.253.207.75	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1411-he/atal.aspx	Block	1
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
139.162.13.205	Singapore	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.61	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown HTTP Request Method 5q25 in URL	Block	1
217.132.24.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
188.73.254.198	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.9	Block	1
109.253.223.62	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
193.186.163.3	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
139.162.13.205	Singapore	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.133.252.195	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
2.53.184.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.44.28	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.44.28	Block	1
79.178.208.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
188.250.203.213	Portugal	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main	Block	1

09-13-2016-15:04:08 to 09-13-2016-16:04:08