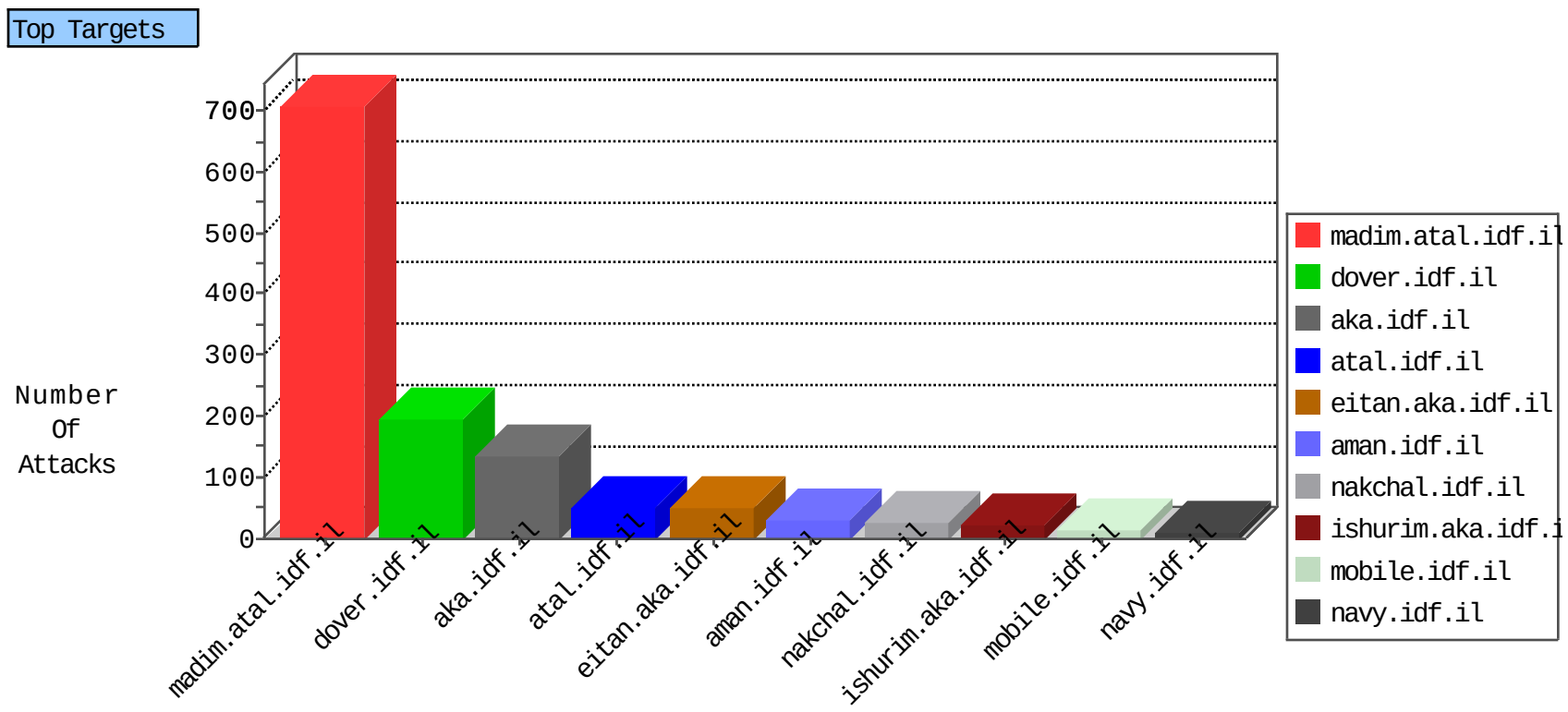
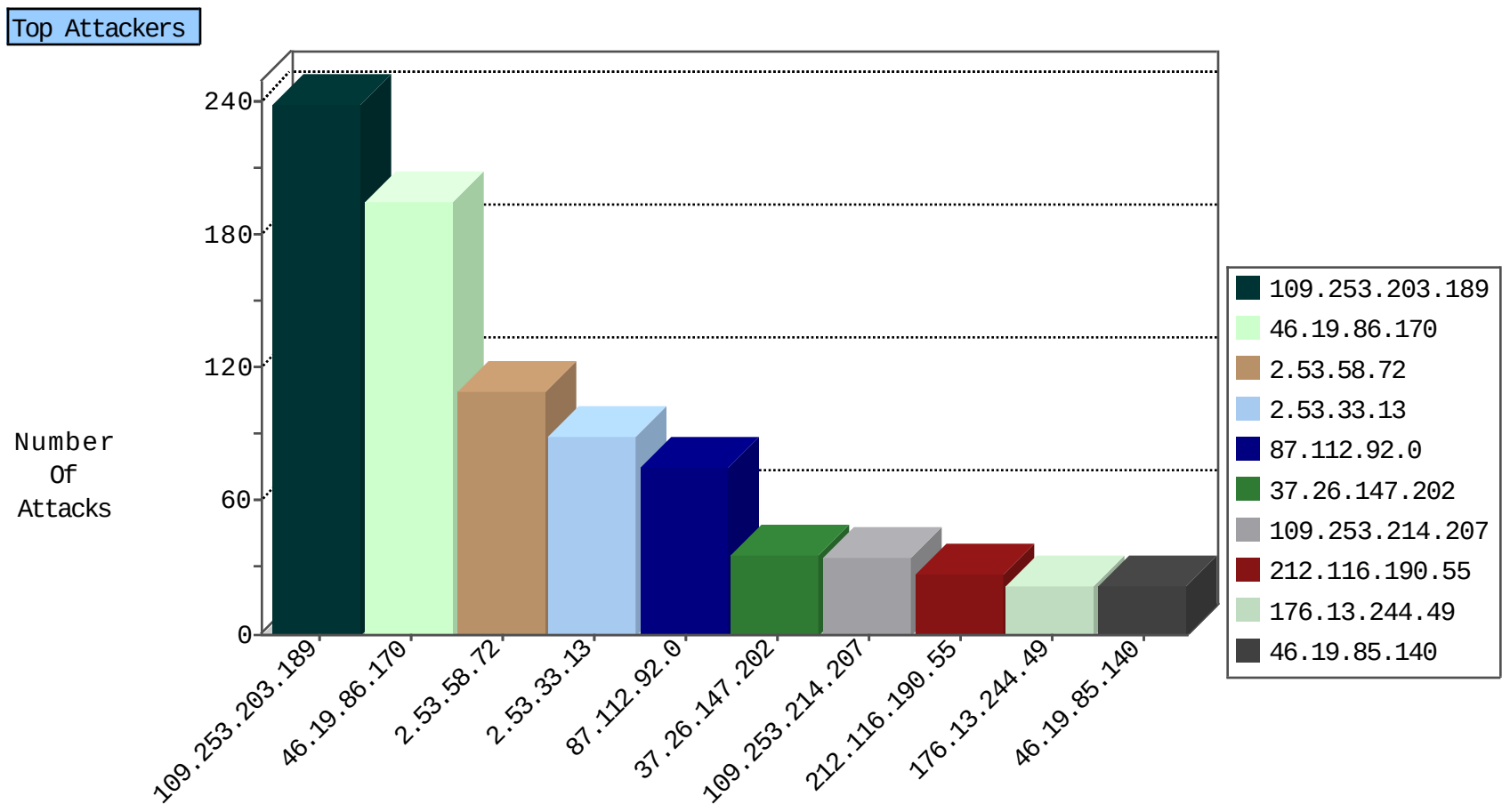
09-19-2016-21:04:08 to 09-19-2016-22:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-19-2016-21:04:08 to 09-19-2016-22:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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
87.181.1.70	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	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
198.82.160.221	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
128.8.126.111	United States	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
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	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
195.113.161.84	Czech Republic	147.237.72.166	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
208.94.63.194	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
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	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
192.33.90.67	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-19-2016-21:04:08 to 09-19-2016-22:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Permit	8
59.108.60.58	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	2
62.210.250.212	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-19-2016-21:04:08 to 09-19-2016-22:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.58	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
123.56.190.151	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
37.26.146.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.232.216.154	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
186.232.216.154	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	1
163.172.177.160	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.131.60	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -f -sS	1
46.4.120.149	147.237.0.200	Germany	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
186.232.216.154	147.237.77.243	Brazil	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
186.232.216.154	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1
180.121.164.175	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.129.15	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

09-19-2016-21:04:08 to 09-19-2016-22:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.112.92.0	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
37.26.147.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.13.244.49	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.116.190.55	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
89.237.107.221	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
80.246.130.58	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.65.120.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
66.249.66.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.72.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.70.132	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.173.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.184	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
80.246.130.58	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.138.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
185.3.147.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.140	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.43.114.86	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.29	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.51.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.3.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
5.22.134.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.181.1.70	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.43.114.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.103.116.130	Greece	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
95.86.90.4	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.37	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.3.147.195	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.53.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.235.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.116.190.55	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.3.147.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.116.190.55	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
212.116.190.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
5.22.134.172	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.15.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.11	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
80.246.137.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.176.146.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.147.157	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-19-2016-21:04:08 to 09-19-2016-22:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.203.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	239
46.19.86.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	195
2.53.58.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
2.53.33.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
109.253.214.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
79.180.16.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
79.180.248.44	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 216.244.66.236	Block	2
72.193.162.44	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.8.215	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
217.69.133.247	Russian Federation	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /english/#012	Block	1
163.172.52.197	United Kingdom	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/admin/i18n/readme.txt	Block	1
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
37.26.149.252	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.176.118.2	Israel	147.237.72.156	aman.idf.il	Illegal Parameter Encoding ctl00$ctl00$cphMain$CPHMainContent$ctl76$ctl07$ctl03$txtField in www.aman.idf.il/modiin/questionnaires.aspx	None	1
213.151.35.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/main/main.asp	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.142.9.104	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
2.53.142.246	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
79.181.122.160	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
77.139.10.88	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
163.172.52.197	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/admin/i18n/readme.txt	Block	1
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
37.26.149.252	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.6.31	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.176.118.2	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17380-he/dover.aspx	Block	1
46.19.85.37	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
109.253.214.207	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** ****	None	1
2.53.173.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.182.88.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.139.92.202	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
180.76.15.18	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	1
94.124.15.138	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
37.46.38.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
79.176.146.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
87.71.15.27	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
5.3.154.76	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	1
77.139.116.210	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim	Block	1
180.76.15.154	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
46.121.213.190	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/homepage/homepage.aspx	Block	1
109.67.96.214	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
37.142.9.28	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
217.69.133.246	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11349-en/dover.aspx	Block	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1

09-19-2016-21:04:08 to 09-19-2016-22:04:08