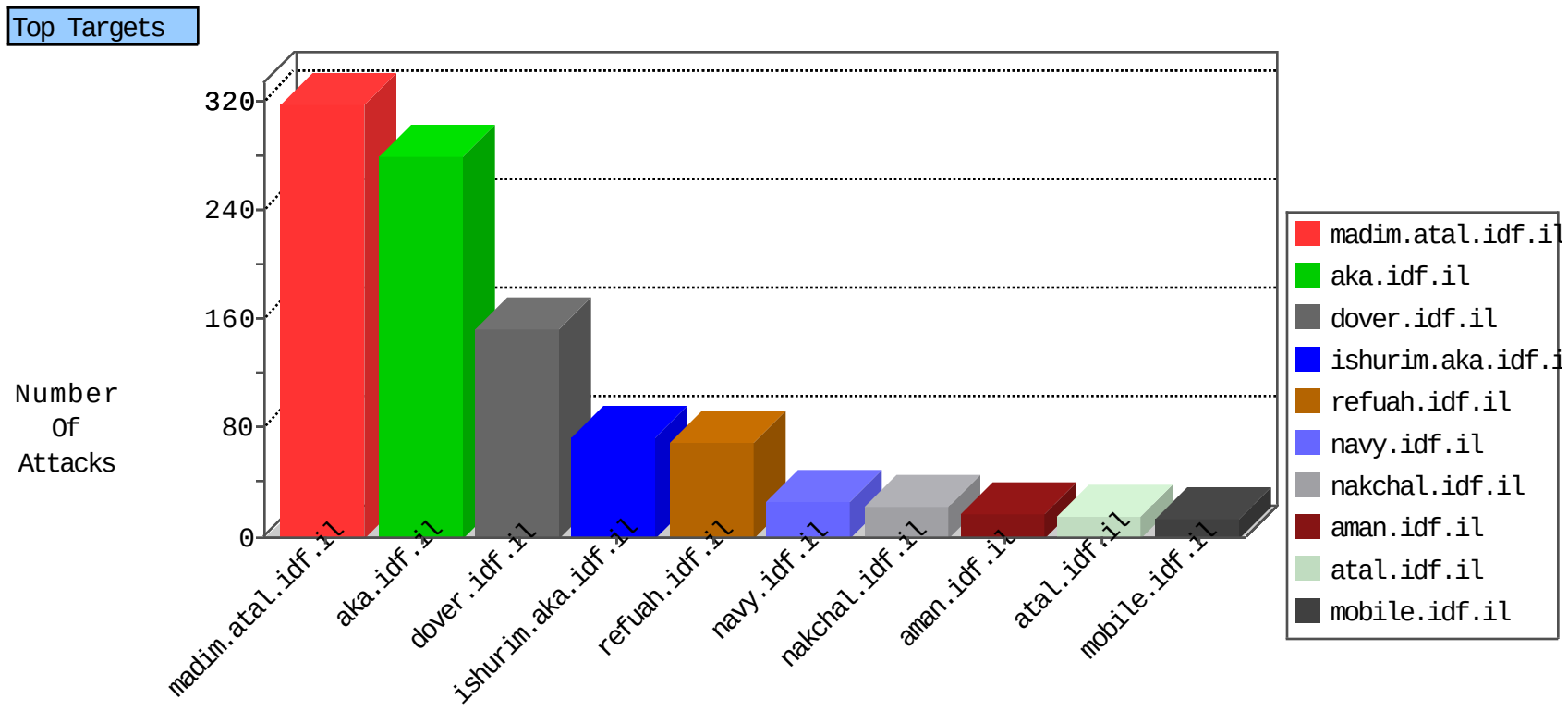
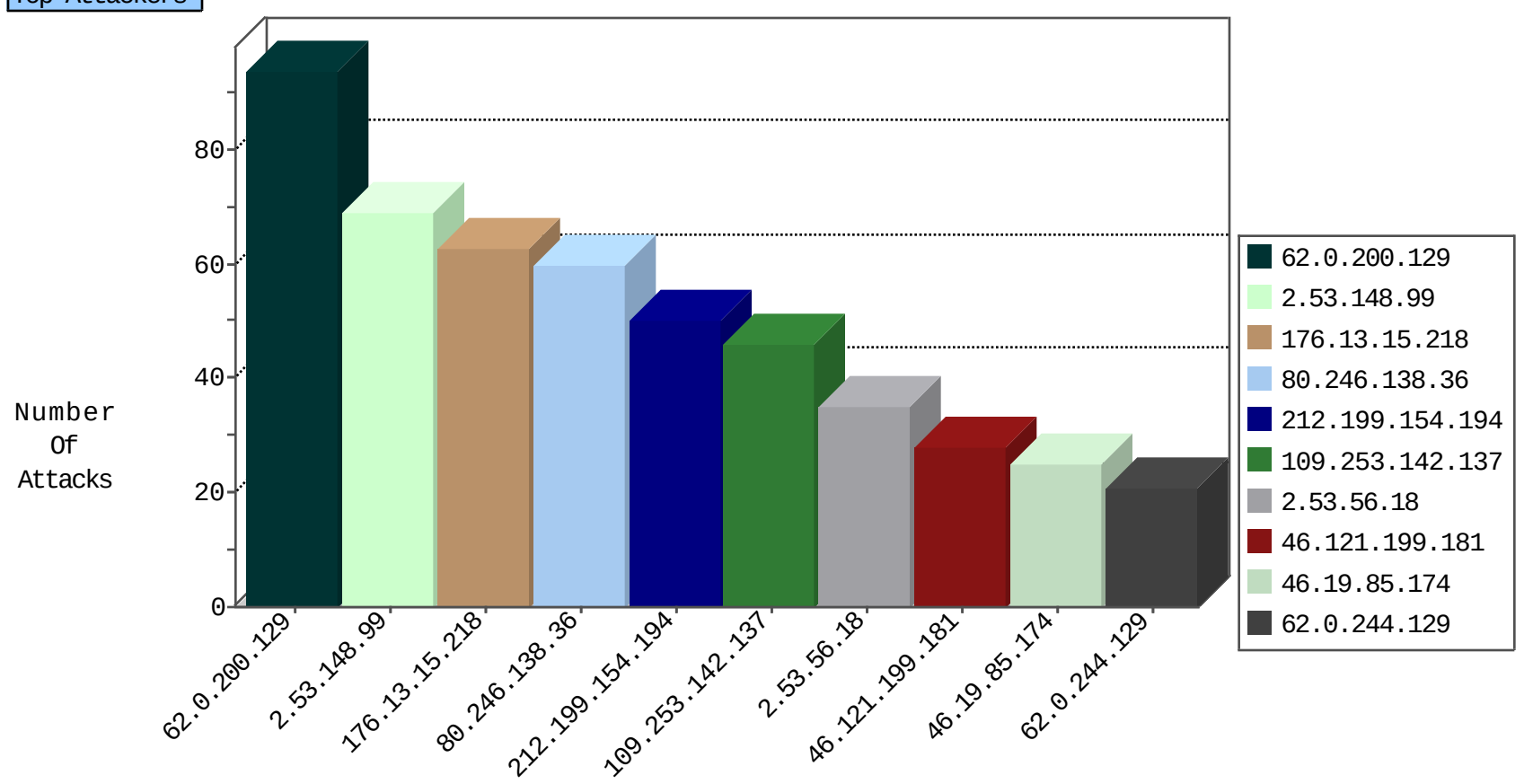
09-14-2016-13:04:02 to 09-14-2016-14:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-14-2016-13:04:02 to 09-14-2016-14:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.226.48.155	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.10.18.52	United States	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
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	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
193.166.167.4	Finland	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
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.14	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-13:04:02 to 09-14-2016-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-14-2016-13:04:02 to 09-14-2016-14:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
2.53.36.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.77.74	Russian Federation	law.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.41.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.114.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.35.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.100.160	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.88.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.39.133.4	147.237.8.14	Iran, Islamic Republic of	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
212.179.223.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.84.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.3.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.226.23.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.7.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.91.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.70.42.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.56.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.184.119.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.39.133.4	147.237.76.200	Iran, Islamic Republic of	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
212.235.27.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.135.236	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.120.106	147.237.76.31	Israel	nakchal.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
162.243.218.193	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.123.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.161.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-14-2016-13:04:02 to 09-14-2016-14:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
62.0.200.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	94
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	42
46.121.199.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
2.53.28.11	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
62.0.212.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
62.0.244.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.174	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.174	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.10.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
31.168.23.59	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
62.0.244.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.69	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
62.0.197.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.153.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
62.0.219.129	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
109.253.203.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.212.120	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.250.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
62.90.169.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.148.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.253.130.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.0.206.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.55.49.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	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
46.19.85.76	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.139.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.146.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.69	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
194.90.119.162	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.19.235	Israel	147.237.72.167	ishurim.aka.idf.i	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	monitor	3
87.70.18.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
80.246.139.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
80.74.103.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.28.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-14-2016-13:04:02 to 09-14-2016-14:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.148.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
176.13.15.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
80.246.138.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
109.253.142.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.53.56.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
176.13.16.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
212.143.120.106	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	9
212.143.120.106	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.143.120.106	Block	6
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
212.143.120.106	Israel	147.237.76.31	nakchal.idf.il	Multiple signatures from 212.143.120.106	Block	4
2.53.166.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.235.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.60.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.117.1	Israel	147.237.72.166	aka.idf.il	Post Request - Missing Content Type from 79.178.117.1	Block	3
37.26.149.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.117.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/authenticationservice.asmx	Block	2
2.53.137.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.148.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.181.117.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.226.48.155	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
79.178.117.1	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/main/giyus/authenticationservice.asmx/authenticate	Block	1
46.121.199.181	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.210.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.226.43.150	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	1
68.180.228.251	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
109.253.136.131	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.55.7.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.20.143.40	Sweden	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
212.143.120.106	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/	Block	1
37.26.149.195	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/	Block	1
84.108.136.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$txtEmail in www.aka.idf.il/main/giyus/faq.aspx	None	1
77.138.24.40	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/drushim/	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for /	Block	1
5.29.129.235	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
109.253.137.96	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
79.179.117.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.142.237.224	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
176.13.10.202	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
87.70.57.206	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
79.178.117.1	Israel	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	1
46.19.86.177	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
109.253.142.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js	Block	1
213.57.138.116	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
89.138.108.127	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1

09-14-2016-13:04:02 to 09-14-2016-14:04:02