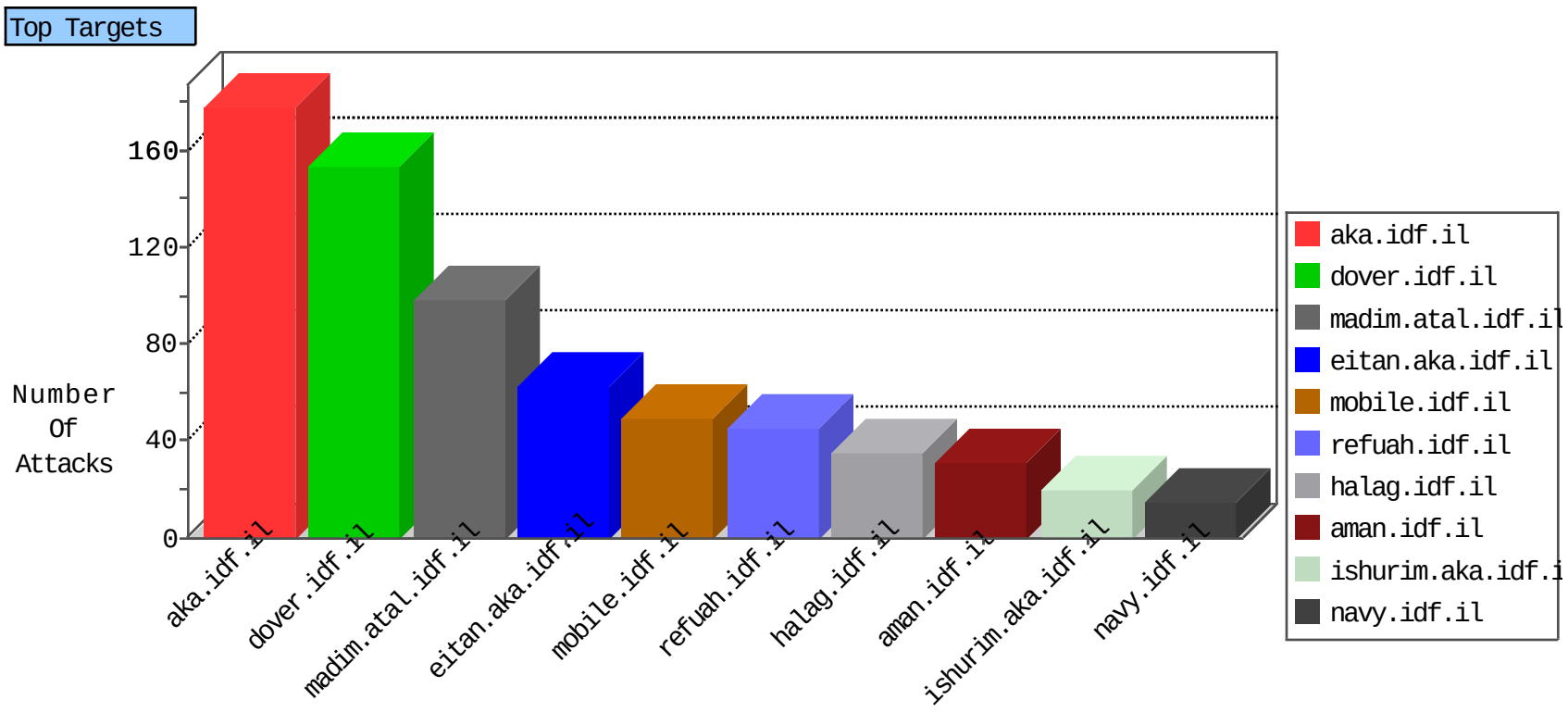
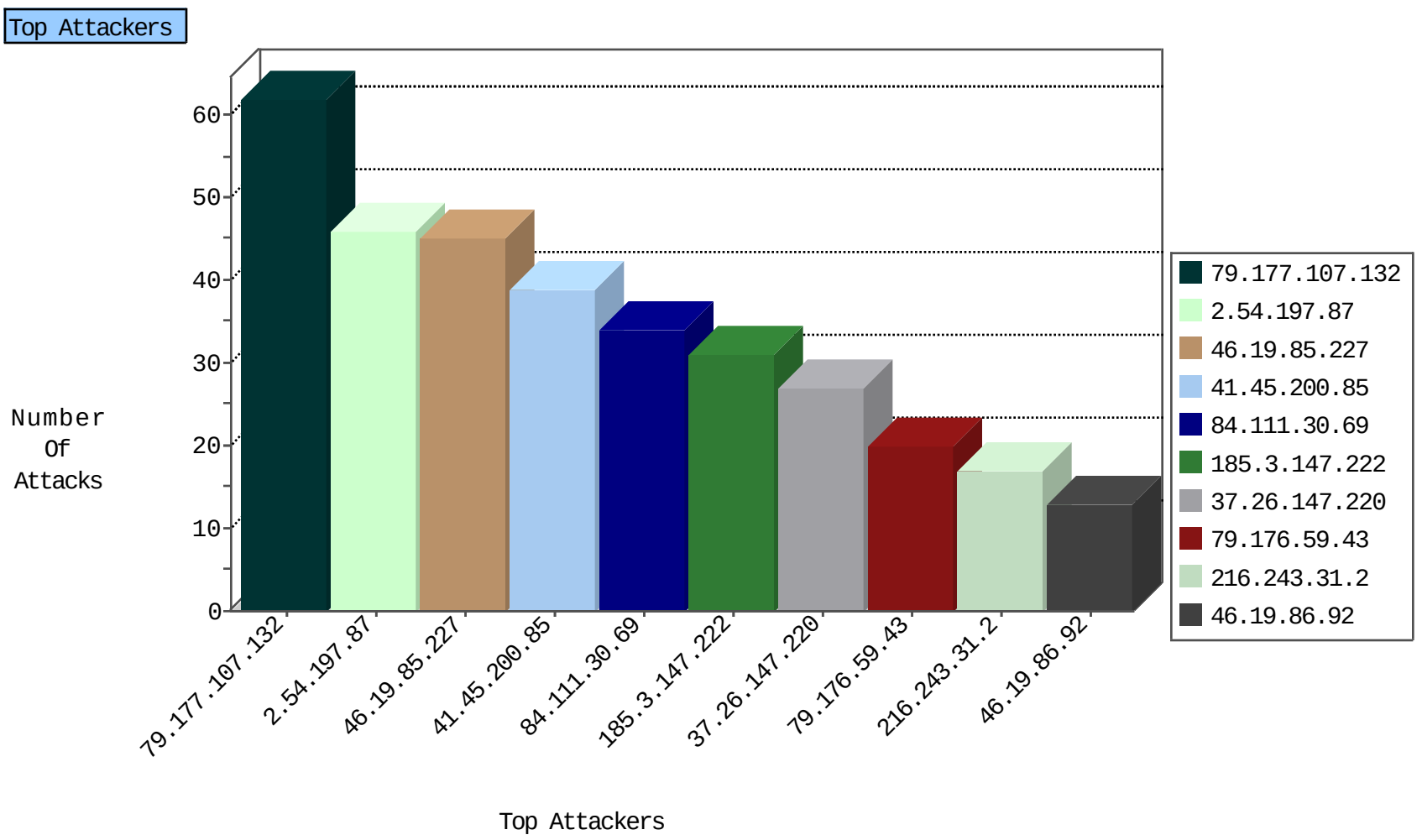
09-20-2016-22:04:08 to 09-20-2016-23:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-22:04:08 to 09-20-2016-23:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.135.131	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
195.62.53.168	Russian Federation	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1

09-20-2016-22:04:08 to 09-20-2016-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-20-2016-22:04:08 to 09-20-2016-23:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
182.255.0.6	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
89.248.171.143	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.255.0.5	147.237.0.15	Indonesia	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.143	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.255.0.4	147.237.77.178	Indonesia	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.243	China	mobile.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
182.255.0.4	147.237.0.16	Indonesia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
220.134.154.29	147.237.77.19	Taiwan	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
138.59.200.75	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.0.16	Latvia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
200.98.129.125	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
118.103.126.194	147.237.76.86	Japan	navy.idf.il	ET SCAN NMAP -sS window 1024	1
182.255.0.5	147.237.76.198	Indonesia	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
182.255.0.5	147.237.76.39	Indonesia	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
92.42.162.161	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
182.255.0.5	147.237.0.17	Indonesia	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.143	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.255.0.4	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.143	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.255.0.4	147.237.77.176	Indonesia	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
172.246.126.103	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
60.249.84.179	147.237.77.216	Taiwan	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
200.98.129.125	147.237.77.234	Brazil	halag.idf.il	ET SCAN Potential SSH Scan	1
125.65.83.162	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
182.255.0.6	147.237.76.176	Indonesia	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Potential SSH Scan	1
182.255.0.5	147.237.77.233	Indonesia	atal.idf.il	ET SCAN Potential SSH Scan	1
116.102.209.128	147.237.76.200	Vietnam	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.255.0.5	147.237.76.147	Indonesia	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.92	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
182.255.0.5	147.237.0.35	Indonesia	akaws.idf.il	ET SCAN Potential SSH Scan	1

09-20-2016-22:04:08 to 09-20-2016-23:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.107.132	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
185.3.147.222	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
37.26.147.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
41.45.200.85	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.176.59.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
2.54.197.87	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
2.54.197.87	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.197.87	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
46.117.128.158	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
213.57.142.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
185.89.217.235	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
41.45.200.85	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
46.19.86.92	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.55.142.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.45.200.85	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
5.22.134.185	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.69.4.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
41.45.200.85	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.247.71	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
84.111.154.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.111.154.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.81.78.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.3.244	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
41.45.200.85	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.55.29.138	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.178.170.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.36	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.111.30.69	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.197.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.197.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.216.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.211.169	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.111.30.69	Israel	147.237.0.19	madim.atal.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	2
2.55.29.138	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
62.82.27.122	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

09-20-2016-22:04:08 to 09-20-2016-23:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
84.111.30.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
37.26.147.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
77.125.69.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	5
37.26.146.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
89.237.99.51	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
77.138.118.58	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	3
89.139.231.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
83.130.83.114	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	3
141.226.164.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.176.12.47	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nakha	Block	1
176.13.21.152	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
89.139.106.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.176.59.43	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.243	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
109.226.48.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
85.64.115.128	Israel	147.237.72.156	aman.idf.il	Unauthorized Request Content Type from 85.64.115.128	Block	1
185.3.147.222	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
89.139.221.167	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.177.227.23	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.92	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.137.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.255.5.49	Ireland	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
85.64.128.9	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	1
195.62.53.168	Russian Federation	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
2.228.119.40	Italy	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
86.245.110.59	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.138.140.248	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
213.57.142.6	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	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
84.109.11.93	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
31.154.81.54	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
141.226.164.54	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
87.69.4.187	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.8.124.41	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1

09-20-2016-22:04:08 to 09-20-2016-23:04:08