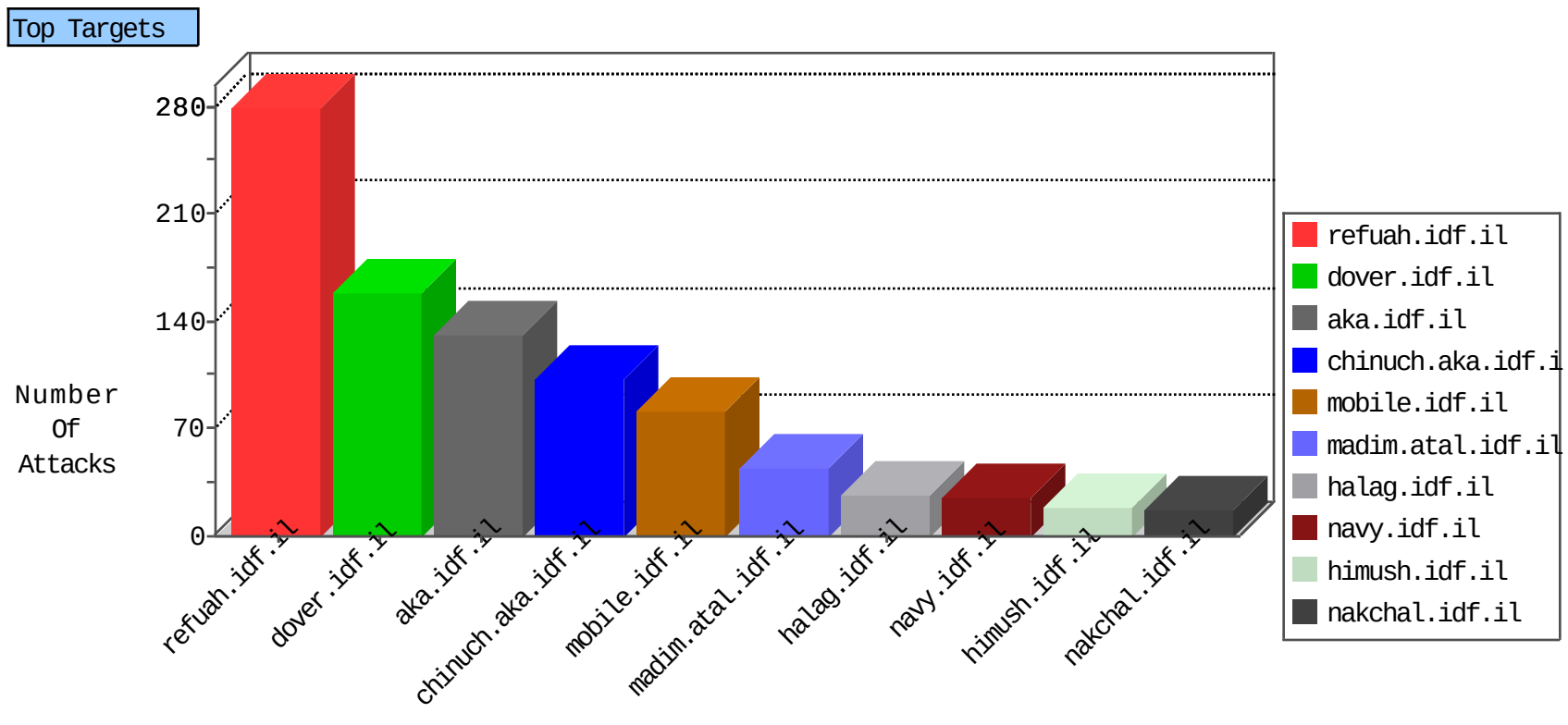
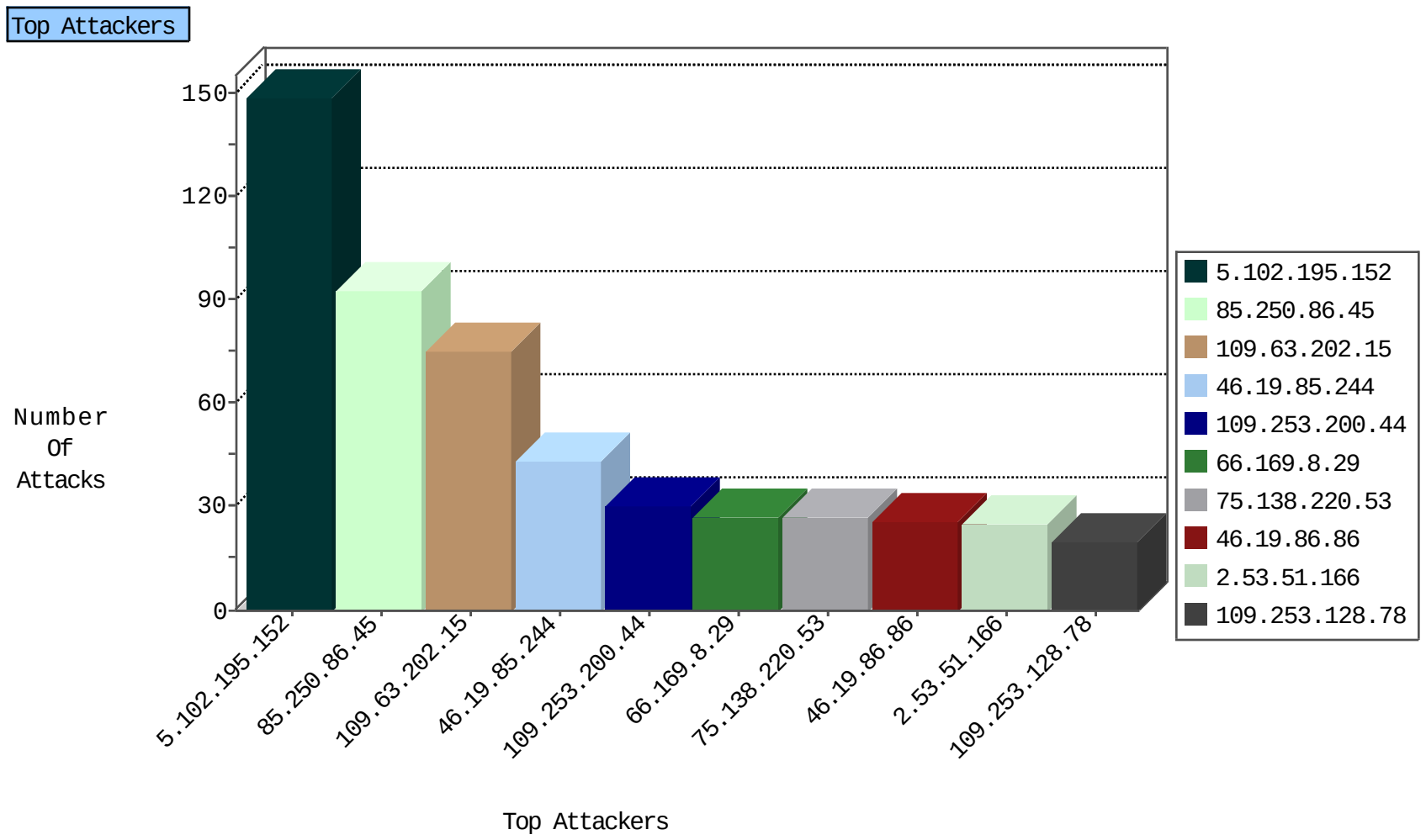
09-26-2016-23:04:07 to 09-27-2016-00:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-26-2016-23:04:07 to 09-27-2016-00:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.126.136.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
89.187.217.75	Lebanon	147.237.0.33	idf.il	L4 Source or Dest Port Zero	drop	1

09-26-2016-23:04:07 to 09-27-2016-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.152.84	France	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

09-26-2016-23:04:07 to 09-27-2016-00:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.69.47.220	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	10
141.226.162.74	147.237.77.226	Israel	www.chamatz.aka.idf.il	GPL SCAN myscan	3
141.226.162.74	147.237.77.226	Israel	www.chamatz.aka.idf.il	INDICATOR-SCAN myscan	3
117.21.173.9	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
117.21.173.9	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.19.86.255	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
117.21.173.9	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
91.121.147.218	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
117.21.173.9	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
95.163.144.203	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.18	147.237.0.33	Switzerland	idf.il	ET SCAN Potential SSH Scan	1
93.174.164.92	147.237.76.198	Romania	e.yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.129.15	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.171.173	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential SSH Scan	1
125.65.82.44	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.106	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
117.21.173.9	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.21.173.9	147.237.72.156	China	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.21.173.9	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
179.43.144.18	147.237.77.216	Switzerland	dover.idf.il	ET SCAN Potential SSH Scan	1
95.163.144.203	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.104.108	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
78.129.171.173	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential SSH Scan	1
125.65.82.44	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.171.173	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.173.9	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

09-26-2016-23:04:07 to 09-27-2016-00:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.195.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	143
85.250.86.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	92
109.63.202.15	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.169.8.29	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
75.138.220.53	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
46.19.85.244	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.85.244	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
109.253.128.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.86	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.86.86	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
213.57.185.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
97.47.64.240	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
97.47.64.240	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.28	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.12	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.12	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.196.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.247.77.238	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
87.70.247.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.65.191.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
95.86.80.164	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.166.186.249	Netherlands	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	6
46.19.86.58	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.191.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.65.132.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.195.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.28	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.139.72.210	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
5.146.249.195	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
67.68.242.88	Canada	147.237.72.166	aka.idf.il	SYN Attack		monitor	4
77.139.72.210	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.77	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.255	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.138.40	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
67.68.242.88	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.222.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.72.87.70	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
80.246.137.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
70.177.107.95	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
31.154.49.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-26-2016-23:04:07 to 09-27-2016-00:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.51.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
148.75.228.41	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 148.75.228.41	Block	15
84.109.162.55	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
109.253.128.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.50.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.185.89	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.139.58.193	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
46.121.198.73	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
70.184.71.29	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	2
77.138.26.223	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	2
37.26.149.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1296-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
85.250.86.45	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
5.102.195.152	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
77.138.245.197	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.66.243	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/081210gaza141.aspx	Block	1
213.241.16.169	Poland	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
40.143.136.38	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/index.php	Block	1
82.81.67.244	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
176.13.1.31	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
5.102.242.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.250.116.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
46.19.85.79	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
157.55.39.111	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.75.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1129-he/dover.aspx	Block	1
176.13.230.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.154.53.182	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
95.86.70.250	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.111.165.17	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
181.167.160.99	Argentina	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.102.6.25	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
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.244	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
85.65.132.81	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.53.167.253	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.64.148	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
109.253.196.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
81.218.65.146	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1

09-26-2016-23:04:07 to 09-27-2016-00:04:07