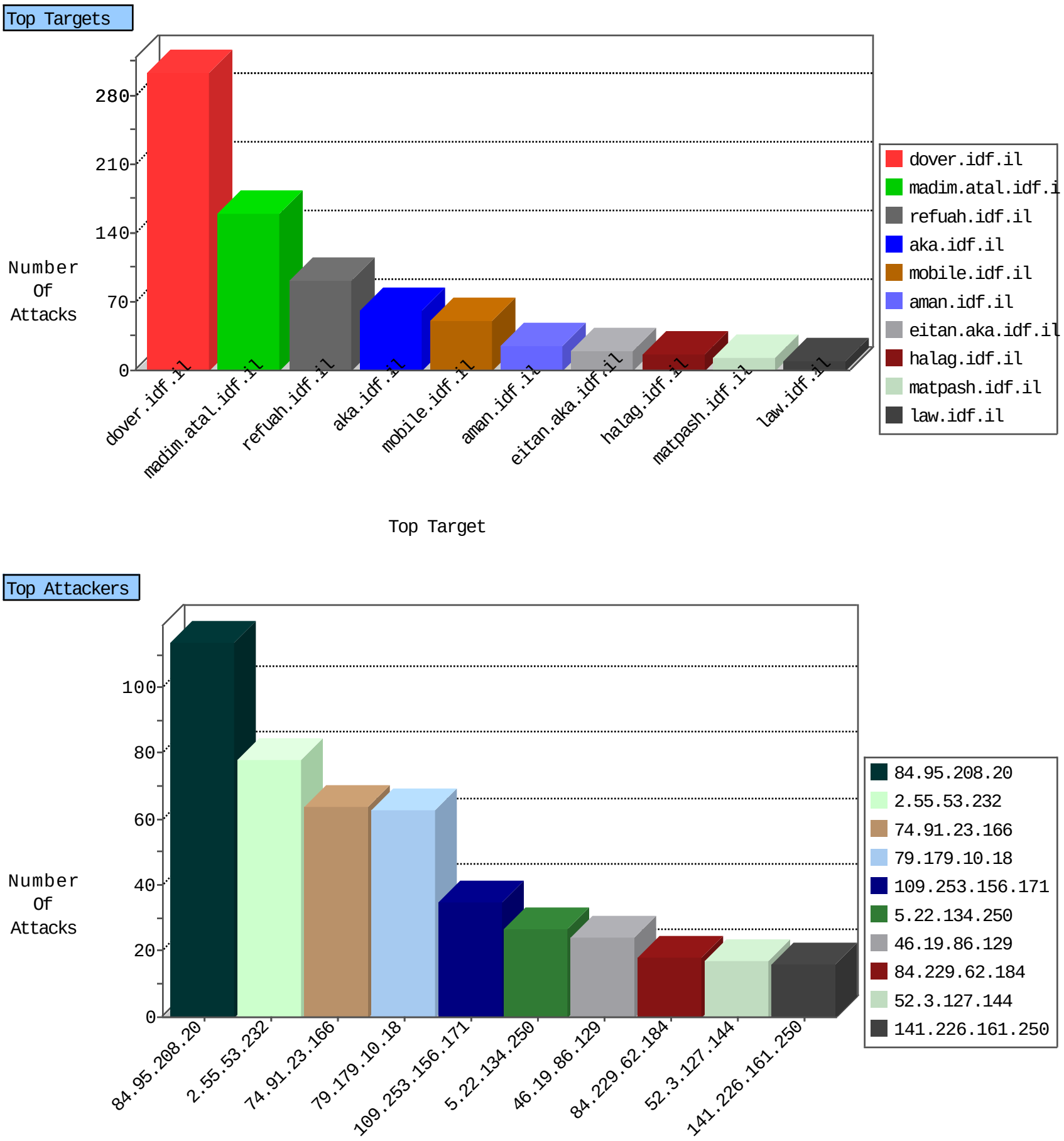
10-02-2016-09:04:03 to 10-02-2016-10:04:03

IDF Under Attack Daily Report



10-02-2016-09:04:03 to 10-02-2016-10:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Black List	drop	5
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Black List	drop	3
79.179.55.62	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
115.146.126.249	Vietnam	147.237.76.196	e.sviva.idf.il	Black List	drop	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

10-02-2016-09:04:03 to 10-02-2016-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-02-2016-09:04:03 to 10-02-2016-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
180.66.11.10	147.237.77.234	Korea, Republic of	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
117.135.131.60	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
117.81.155.211	147.237.8.45	China	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.171	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
188.136.237.251	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
58.218.200.137	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
188.136.237.251	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
182.254.131.170	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.33	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
172.242.41.105	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
46.172.91.21	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
1.162.14.128	147.237.8.45	Taiwan	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.135.131.60	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
211.149.222.5	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
84.229.12.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.128.127.140	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
188.136.237.251	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
186.67.104.75	147.237.8.28	Chile	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.33	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
41.215.36.46	147.237.8.28	Kenya	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

10-02-2016-09:04:03 to 10-02-2016-10:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
74.91.23.166	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
5.22.134.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
212.199.57.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.11.162.171	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.181.130.44	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.86.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
84.108.137.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
141.226.161.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.53.189.231	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
77.138.240.89	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
141.226.161.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
109.253.156.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
88.238.10.165	Turkey	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
84.109.69.105	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.29.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.62.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
141.226.161.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.120.124.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.229.62.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
141.226.161.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.113.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.62.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.22.134.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
173.17.8.254	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
52.3.127.144	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	5
2.53.12.121	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.167.169	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.156.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.102.195.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.26.183.9	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.84	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
196.106.122.81	Kenya	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
109.253.156.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
109.253.156.171	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.156.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.29.191.141	Israel	147.237.77.243	mobile.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	3
24.4.50.221	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
46.19.86.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.156.171	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.85.18	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
196.53.36.119	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.137.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

10-02-2016-09:04:03 to 10-02-2016-10:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.53.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	77
79.179.10.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
212.199.57.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.90.167.68	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ReturnUrl in madim.atal.idf.il/login.aspx	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
77.126.8.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.32.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	2
2.53.55.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
77.138.188.53	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/894-he/dover.aspx	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8819-he/refuah.aspx	Block	1
139.162.13.205	Singapore	147.237.0.34	tikshuv.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
194.90.79.80	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl95 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.230.186	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
52.209.46.233	Ireland	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/web-console/serverinfo.jsp	Block	1
87.68.8.61	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
77.139.86.186	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
139.162.13.205	Singapore	147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8675-he/refuah.aspx	Block	1
5.22.134.250	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
212.25.82.123	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
89.237.67.170	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
213.8.204.65	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsControl$ImageButton1.y in www.cogat.idf.il/901-he/cogat.aspx	Block	1
148.251.192.100	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.75.53	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
23.247.85.14	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
212.25.82.123	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/7/	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
94.180.145.50	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
79.181.130.44	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.100	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.75.137	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
23.247.85.14	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
77.127.94.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
212.143.103.172	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1

10-02-2016-09:04:03 to 10-02-2016-10:04:03