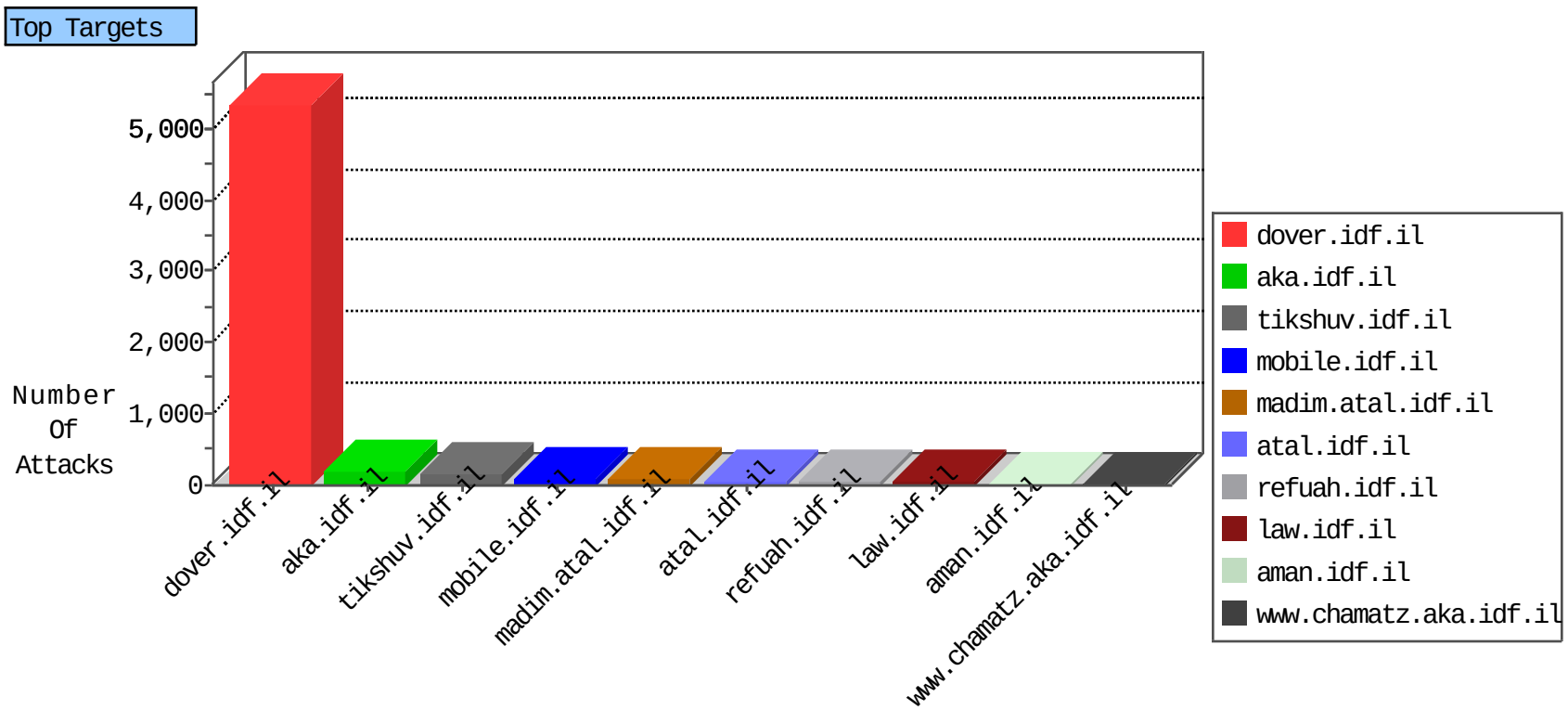
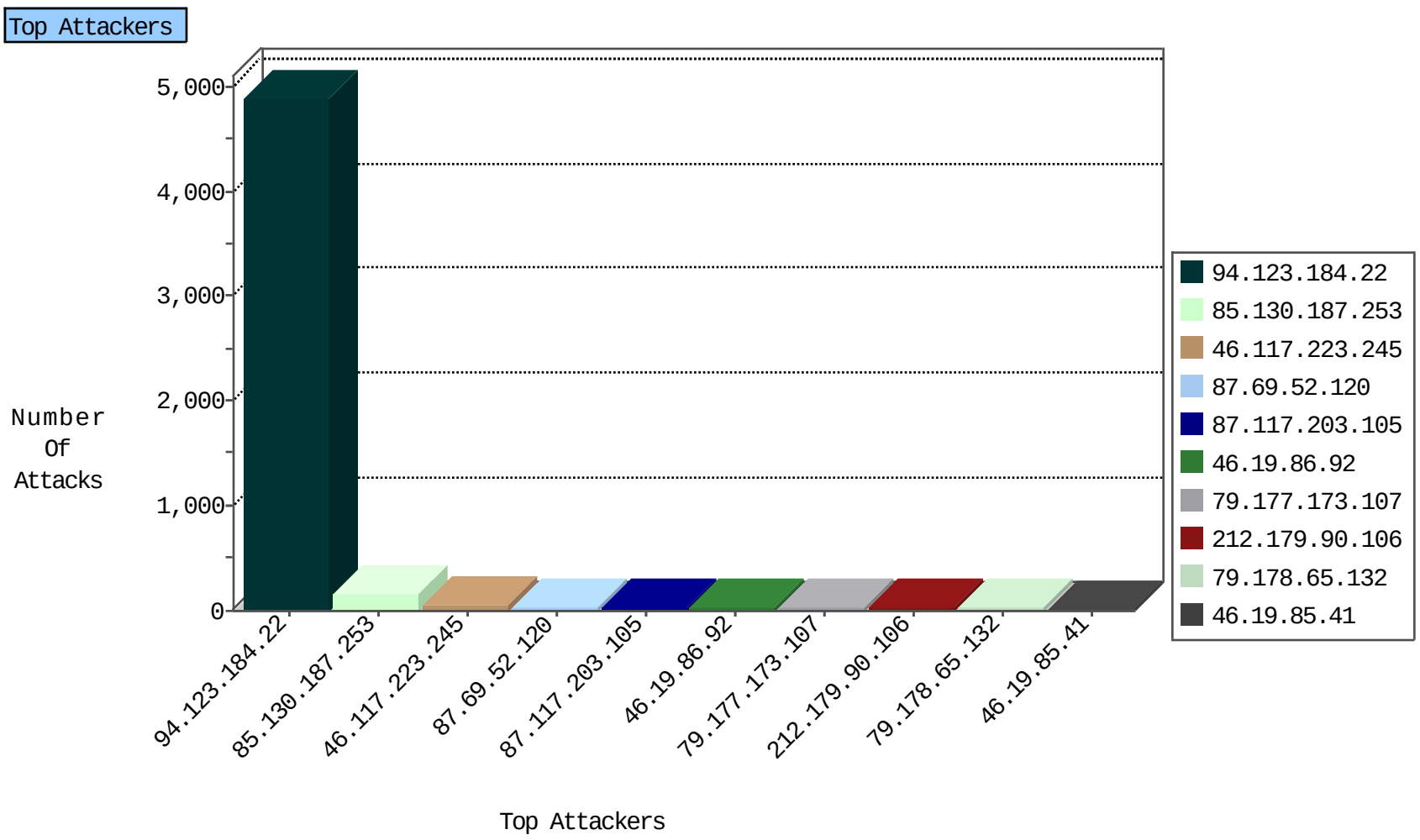
09-18-2016-21:04:01 to 09-18-2016-22:04:01

IDF Under Attack
Daily Report



Top Target



Top Attackers

09-18-2016-21:04:01 to 09-18-2016-22:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.123.184.22	Turkey	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	2710
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
94.123.184.22	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
222.186.34.186	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
63.141.231.195	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
173.208.150.115	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
129.97.74.14	Canada	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
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
63.141.242.196	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
204.12.220.84	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
192.33.90.67	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.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
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
63.141.242.197	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
142.54.174.83	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
2.55.131.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.204.224.235	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.193.251	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-21:04:01 to 09-18-2016-22:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.117.203.105	United Kingdom	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.176.226.68	Russian Federation	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
174.36.80.58	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.117.203.105	United Kingdom	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.96.128.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.229	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
176.9.10.227	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.125.125.31	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-18-2016-21:04:01 to 09-18-2016-22:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.117.203.105	147.237.76.42	United Kingdom	refuah.idf.il	SQL Injection - Select From	20
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
81.176.226.68	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	8
50.63.196.229	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
174.36.80.58	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
123.206.85.139	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.228.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.180.9.40	147.237.0.34	South Africa	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
41.180.9.40	147.237.0.16	South Africa	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.15.49	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.15.49	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
41.180.9.40	147.237.76.30	South Africa	himush.idf.il	ET SCAN NMAP -sS window 1024	1
41.180.9.40	147.237.0.17	South Africa	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.15.49	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
222.254.34.165	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.15.49	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

09-18-2016-21:04:01 to 09-18-2016-22:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
94.123.184.22	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4305
85.130.187.253	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
85.130.187.253	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	49
85.130.187.253	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	39
87.69.52.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	39
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
79.177.173.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
79.178.65.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
50.63.197.204	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
94.123.184.22	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
109.66.138.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.248.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.130.187.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.64.154.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
217.69.133.190	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
217.69.133.247	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.86.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
217.69.133.244	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.147.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
84.94.97.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.29	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
188.120.148.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.179.151.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.8.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.26.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.26.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.124.4.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.178.14.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.10.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
87.69.79.33	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.28.172.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.187.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.166.247.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
85.250.214.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.187.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.109.112.207	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.166.247.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
217.69.133.241	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

09-18-2016-21:04:01 to 09-18-2016-22:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.223.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
46.19.86.92	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.92	Block	27
2.55.36.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.227.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.164.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.22.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.158.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.63.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
104.50.223.12	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
46.19.86.92	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
37.142.217.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.232.101.28	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
213.57.194.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
77.138.85.139	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
46.120.161.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$txtOtherQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
5.102.195.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
79.182.33.184	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.182.33.184 (Unknown SSL Session)	None	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
213.151.37.237	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
87.70.12.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.198.151	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chinuch	Block	1
185.27.105.89	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
79.182.33.184	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.93.69	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
217.69.133.220	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter docId&pageNum in aka.idf.il/tizmoret/faq/default.asp	None	1
89.237.88.206	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
77.139.215.175	France	147.237.72.166	aka.idf.il	Unknown Parameter onepasswdfill in www.aka.idf.il/main/sachar/	None	1
193.86.28.202	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/atudalane.aspx	Block	1
66.249.66.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
109.64.143.17	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.124.34.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/69385.pdf	Block	1
157.55.39.122	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
46.116.61.95	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.55.12.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.215.175	France	147.237.72.166	aka.idf.il	Unknown Parameter onepasswdvault in www.aka.idf.il/main/sachar/	None	1
207.46.13.165	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.76.53	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
109.64.143.17	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
82.81.33.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.225.94	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
94.102.49.190	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
79.180.5.109	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type from 79.180.5.109	Block	1
46.19.86.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.66.51.240	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1

09-18-2016-21:04:01 to 09-18-2016-22:04:01