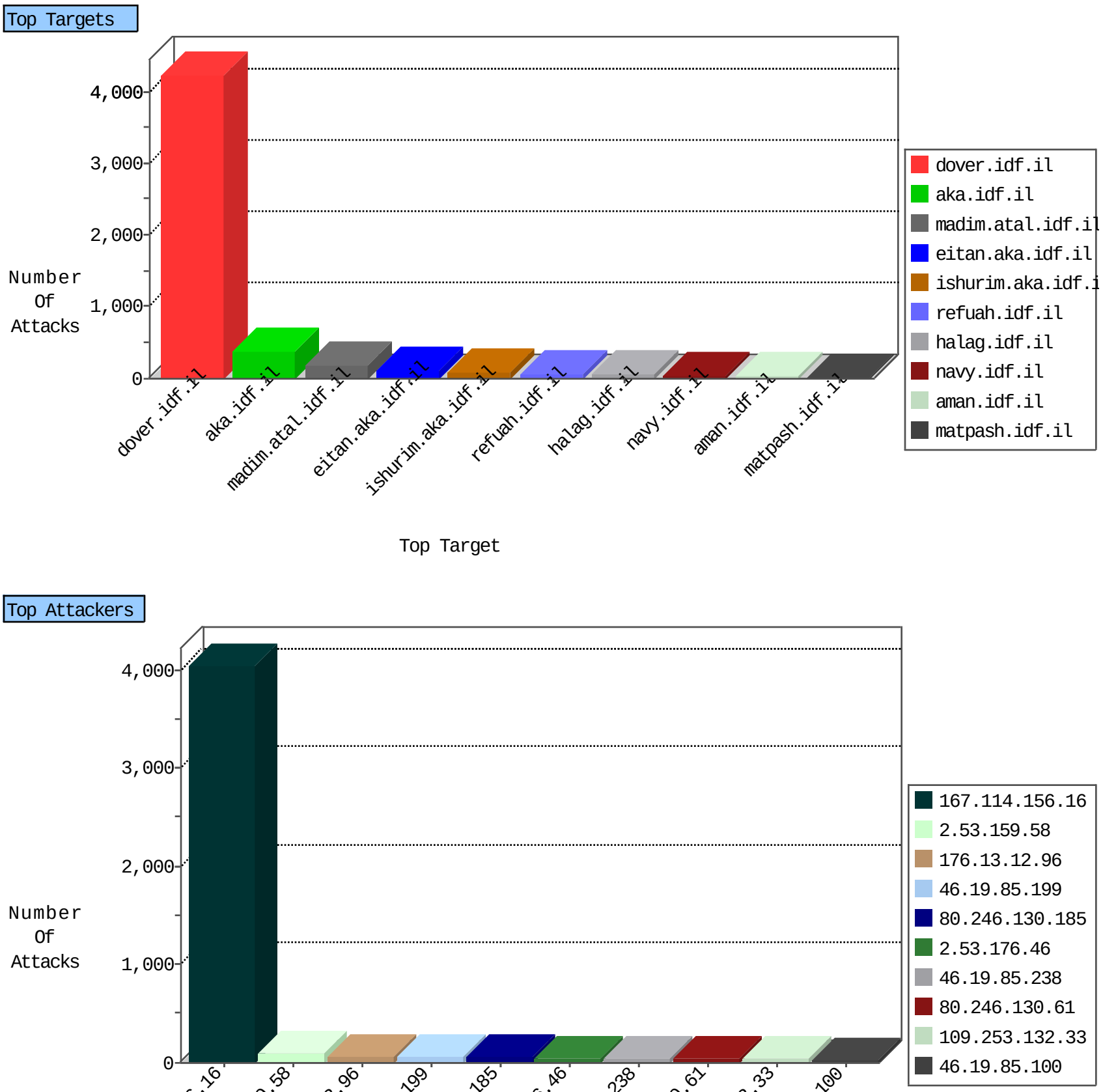
04-19-2016-17:04:07 to 04-19-2016-18:04:07

IDF Under Attack Daily Report



04-19-2016-17:04:07 to 04-19-2016-18:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4043
80.246.137.41	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
80.246.138.215	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
120.132.50.135	China	147.237.72.166	aka.idf.il	block-sp-traf1	forward	4
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
31.168.243.63	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.243.63	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
207.104.161.245	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
71.216.155.117	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
123.30.183.145	Vietnam	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
123.30.183.145	Vietnam	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1

04-19-2016-17:04:07 to 04-19-2016-18:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.103.252.98	Russian Federation	147.237.0.34	tikshuv.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
37.8.10.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	3807: HTTP: SQL Injection Evasion Inline SQL Comment	Block	1
185.103.252.98	Russian Federation	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
185.103.252.98	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
185.103.252.98	Russian Federation	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

04-19-2016-17:04:07 to 04-19-2016-18:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
201.235.215.254	147.237.8.27	Argentina	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
5.102.242.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.131.208.140	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
85.131.208.140	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
187.227.131.40	147.237.76.30	Mexico	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.117.208.243	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.88	147.237.8.46	Lithuania	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
77.124.24.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.106.229.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
65.181.123.161	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
134.228.0.146	147.237.76.34	United States	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.205.69	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
112.218.60.60	147.237.77.227	Korea, Republic of	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.85.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.158.255.194	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.180.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.84.159.128	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
85.250.129.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.235.215.254	147.237.8.27	Argentina	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
85.131.208.140	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.125.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.88	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.103.252.98	147.237.0.19	Russian Federation	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
75.112.247.219	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.226.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
65.181.123.161	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
46.117.206.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.49.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.84.159.128	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
91.208.139.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-19-2016-17:04:07 to 04-19-2016-18:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.159.58	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
80.246.130.185	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
176.13.12.96	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.85.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
80.246.130.61	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.181.213.106	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
46.19.85.61	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
217.132.237.133	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.12.96	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
2.55.37.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.0.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.90.145.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.3.147.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.239.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
196.217.240.204	Morocco	147.237.77.176	matpash.idf.il	drop		drop	7
176.13.12.96	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	6
209.23.209.250	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.150.128.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.253.225.164	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.79.42	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
209.23.209.250	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.55.10.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.65.239.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.139.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
217.132.148.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.65.239.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
65.55.210.19	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
209.37.96.2	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.65.239.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.239.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.246.139.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.118.27.253	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.129.27.45	Greece	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.218.103.137	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.178.98.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.24.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.111.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.128.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
2.53.176.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.253.132.33	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	39
109.253.203.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
80.246.137.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.137.41	Block	18
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
37.8.10.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.86.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
85.65.136.181	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
176.13.12.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.222.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.0.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.93.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
132.66.160.154	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	2
2.55.129.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.241.32.158	United States	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.241.32.158	None	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
80.246.130.185	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
5.102.242.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.241.32.158	United States	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.mag.idf.il/163-7507-en/patzar.aspx	Block	1
80.246.138.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter d in www.aka.idf.il/main/giyus/general.aspx	None	1
79.129.27.45	Greece	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.133.170.97	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.171	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.171	Block	1
87.71.82.227	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
59.37.23.181	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
23.80.148.140	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
120.132.50.135	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.ctrip.com/main/home/default.aspx	Block	1
80.246.138.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter do in www.aka.idf.il/main/giyus/general.aspx	None	1
79.181.98.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
207.46.13.15	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
94.70.168.151	Greece	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.0.192.63	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1
23.106.85.128	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
80.246.137.41	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/giyus/general.aspx	None	1
185.24.76.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2422.jpg	Block	1
80.246.138.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/main/giyus/general.aspx	None	1
80.246.130.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
207.46.13.176	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method	Block	1